La ecuación lineal con dos incógnitas

$ax + by = c$ Esta ecuación diofántica solamente tiene solución entera si y sólo si $d = mcd(a,b)$ es un divisor de c.

Soluciones: $x = x_0 + \left(\frac{b}{d}\right)t,\ y = y_0 - \left(\frac{a}{d}\right)t$

Determinación de una solución particular de la ecuación lineal

P1. Determinar x_0 e y_0, tales que: $ax_0 + by_0 = 1$ (Bezout):	P2. Escribir el resultado anterior de la forma:
Para ello, podemos aplicar el Algoritmo de Euclides: $\begin{array}{ccccccc} & c_1 & c_2 & c_3 & \ldots & c_n & c_{n+1} \\ a & b & r_1 & r_2 & \ldots\ldots r_{n-2} & r_{n-1} & r_n \\ r_1 & r_2 & r_3 & \ldots & \ldots & 0 & \end{array}$	$a = b \cdot c_1 + r_1$ $b = r_1 \cdot c_2 + r_2$ $r_1 = r_2 \cdot c_3 + r_3$ $\rightarrow r_{n-2} = r_{n-1} \cdot c_n + r_n$
P3. Escribir 1 como combinación lineal de a y b:	P4. Multiplicaremos la combinación obtenida en P3 por c.
Emplearemos las combinaciones del P2 de forma inversa hasta alcanzar la combinación: $aX_0 + bY_0 = 1$.	$ax_0 + by_0 = c,\ \text{con}\ x_0 = X_0 \cdot c\ \text{e}\ y_0 = Y_0 \cdot c$
P5. Con la solución particular hallada, escribiremos el sistema:	P6. Buscar las soluciones de t que cumplan las restricciones.
$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases},\ t \in Z$	

Congruencias lineales

$$ax \equiv b (\bmod n) \leftrightarrow ax = b + ny, y \in Z \rightarrow\leftrightarrow ax - ny = b \leftrightarrow mcd(a,n) = d \text{ divisor de } b \rightarrow \boxed{x = x_0 + \frac{n}{d}t, t \in Z}$$

Sistema de congruencias lineales:
$$\begin{cases} a_i x \equiv b_i (\bmod m_i) \Leftrightarrow x \equiv c_i (\bmod n_i), \mathrm{i} = 1, \quad \mathrm{k} \\ donde\ c_i = \text{solución particular d ela congruencia} \\ \qquad donde\ \mathrm{n}_i = \dfrac{m_i}{d} \end{cases}$$

Teorema chino de los restos

$$\begin{cases} x \equiv a_1 (\bmod n_1) \\ \\ x \equiv a_k (\bmod n_k) \end{cases} \rightarrow x = x_0 + n_1 n_1 \quad n_k t, t \in Z$$

- Paso 1: $x = n_1 t + a_1$
- Paso 2: Sustituimos en la siguiente congruencia: $n_1 t + a_1 \equiv a_2 (módn_2)$ y despejamos t: $t \equiv a_2' (módn_2)$
- Paso 3: $t = n_2 s + a_2'$
- Paso 4: Reiteramos el proceso hasta haber agotado todas las congruencias y sustituimos en la del Paso 1.
- Paso 5: El mínimo se obtiene con el último parámetro igualado a 0.

La ecuación de Fermat

$x^2 - y^2 = n$ tiene solución entera si y sólo si n se puede factorizar como producto de dos números enteros de la misma paridad, es decir, ambos pare so ambos impares, donde:

$$x = \frac{s+t}{2}, y = \frac{s-t}{2} \text{, donde } n = st \text{ y s y t tienen la misma paridad.}$$

Observaciones

1. Si n es la diferencia de dos cuadrados: n es impar o n es par y, por tanto, múltiplo de cuatro
2. Si n es impar: s y t impares: (s,t) tales que st=n. Si n es par: s ó t pares tales que si n no es múltiplo de 4, no existe solución.

Algunas ecuaciones polinómicas homogéneas

Ecuaciones polinómicas homogéneas (Px,y)=0	Las soluciones enteras de la ecuación P(x,y)=0 tales que $y \neq 0$ son los pares (x,y): $x = pt, y = qt$, donde $\frac{p}{q}$ es cada fracción irreducible solución de P(z,1)=0 .
	P1. P(z,1)=0, donde $z = \lambda_1, \lambda_2, \quad \lambda_k$
Ej.: $2x^3 + 3x^2y - 3xy^2 - 2y^3 = 0$	P2. $\begin{cases} x = \lambda_1 t, \lambda_2 t, \quad \lambda_k t \\ y = t \end{cases}$
	P3. P(x,0)=0
Ecuaciones P(x)=my	Las soluciones de la ecuación P(x)=my son los pares (x,y): $x = x_0 + mt, P(x_0 + mt) = my$, donde $x_0 \in \{0, \quad m-1\}$ es solución particular de $P(x) \equiv 0 (\operatorname{mod} m)$.
	P1. Despejar x's a un lado igualando a my.
Ej.: $x^2 + 5x + 4 + 6y = 0$	P2. $P(x) \equiv 0 (\operatorname{mod} m)$, donde $x = x_{01}, x_{02}, \quad, x_{0k}$.
	P3. $\begin{cases} x = x_{01} + mt, x_{02} + mt \\ y = \text{resultado de sustituir x} \end{cases}$
Ecuaciones P(x)=Q(x)y	Tienen un número finito de soluciones (x,y).
	P1. Despejar y. $y = \frac{P(x)}{Q(x)}$, $P(x) = Q(x) \cdot c(x) + r(x)$
Ej.: $xy = 2x + 2y \rightarrow y(x-2) = 2x$	P2. $my = \frac{Q(x) \cdot C(x) + R(x)}{Q(x)} = C(x) + \frac{R(x)}{Q(x)}, my - C(x) = \frac{R(x)}{Q(x)}$
	P3. Hallamos las soluciones enteras finitas que cumplen esa restricción.
Ecuaciones $\boldsymbol{a^2x^2 + bx + c = y^2}$	Si $a, b, c \in Z$ no son simultáneamente nulos, la ecuación tiene un número finito de soluciones (x,y).
	P1. Cambio de variable: $y = ax + z$.
Ej.: $4x^2 + 3x + 3 = y^2 \rightarrow y = 2x + z$	P2. Resolver la ecuación como P(x)=Q(x)y y resolver.

La ecuación pitagórica

$x^2 + y^2 = z^2, mcd(x, y, z) = 1$, tiene por soluciones: $x = 2kst, y = k(s^2 - t^2), z = k(s^2 + t^2)$, donde $k \in N$ y s y t son dos números naturales de distinta paridad tales que s>t y mcd(s,t)=1.

Triángulos pitagóricos: se llaman así a aquellos cuyos lados tienen longitudes enteras. Con el teorema de la ecuación pitagórica se puede demostrar que el radio de la circunferencia inscrita en cualquier triángulo pitagórico es siempre un número natural.

Último teorema de Fermat

Si $n \in N$ y n>2, la ecuación diofántica $x^n + y^n = z^n$ no tiene soluciones formadas por números naturales.

TRUCOS

- Intentaremos tener siempre dos incógnitas como mucho, poniendo las demás en función de las otras.
- Haremos aparecer los términos y factores que nos propongan los enunciados para ir acercando nuestros resultados a los solicitados.
- Si necesitamos incorporar un nuevo parámetro, podemos hacerlo para facilitar el problema.