PRACTICO 2

Algoritmo de Euclides:

Es un metodo para hallar el mcd (a,b)

El Algoritmo de Euclides Extendido sirve para hallar ademas los coeficientes de Bezout. Es decir $x, y \in \mathbb{Z}$:

$mcd(a,b) = ax + by$

Ecuaciones Diofanticas

Una ec. diofantica lineal en las variables x, y es una ecuación de la forma:

$$\boxed{ax + by = c \quad \text{con } a,b,c \in \mathbb{Z}}$$

En donde el conjunto solución de la ecuación es: $\boxed{S = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : ax+by = c\}}$

Teorema: Sean a, b y c enteros con $(a,b) \neq (0,0)$. Entonces la ec. diofantica

$ax + by = c$

1) Tiene solución $\leftrightarrow mcd(a,b) \mid c$

2) Si tiene solución, entonces tiene infinitas. Es mas si (x_0, y_0) es sol. El conjunto de soluciones es:

$$S = \left\{ \left(x_0 + \frac{b.k}{mcd(a,b)}, \ y_0 - \frac{a.k}{mcd(a,b)} \right) : k \in \mathbb{Z} \right\}$$

$$S = \{ (x_0 + b^* k, \ y_0 - a^* k) : k \in \mathbb{Z} \}$$

$\rightarrow$ con $a = a^* . mcd(a,b)$

$b = b^* . mcd(a,b)$

Propiedades practico: Sea $a \in \mathbb{N}$, $a \geq 2$

- Si $m \mid n \Rightarrow a^m - 1 \mid a^n - 1$
- $mcd(a^n - 1, a^m - 1) = a^{mcd(n,m)} - 1$
- Si r = Resto de dividir n entre m

$\Rightarrow a^r - 1$ = Resto de dividir $a^n - 1$ entre $a^m - 1$

Pasos para calcularlo:

1) Escribimos nuestro dato inicial en una matriz: $B_0 = \begin{pmatrix} a \\ b \end{pmatrix}$

2) Realizamos $a = b.q_1 + r_1$ y escribimos

$$B_1 = \begin{pmatrix} b \\ r_1 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}}_{= M_1} B_0$$

3) Hacemos lo mismo con los nuevos datos: $b = q_2 . r_1 + r_2$

$$B_2 = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}}_{= M_2} B_1 = M_2 . M_1 . B_0$$

4) Repetimos lo mismo con los siguientes datos:

$B_i = \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$ y $r_{i-1} = q_{i+1} . r_i + r_{i+1}$

$$B_{i+1} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} . B_i = M_{i+1} . M_i \ldots M_1 . B$$

5) Al obtener el primer resto nulo $(r_n = 0)$ nos detenemos en el paso anterior

$$B_{n-1} = \begin{pmatrix} r_{n-2} \\ mcd(a,b) \end{pmatrix} = M . B_0 = M . \begin{pmatrix} a \\ b \end{pmatrix}$$

Siendo $M = M_{n-1} \ldots M_1$

6) La ultima fila de $M = \begin{pmatrix} z & w \\ x & y \end{pmatrix}$ nos dice que $mcd(a,b) = x.a + b.y$

Siendo x e y los coeficientes de Bezout

Algunas propiedades

- Sean $a > 1$, $b > 1$ enteros y coprimos

$\Rightarrow \nexists x, y \in \mathbb{Z} : ax + by = ab - a - b$

- Sean a y $b \in \mathbb{Z}^+$ y coprimos

$\Rightarrow$ Si $n \geq ab - a - b$ $\exists x, y \in \mathbb{Z}^+$:

$ax + by = n$

- Si $(x_0, y_0) \in \mathbb{Z}$ son solución de $ax+by=n$ con $a, b, n \in \mathbb{Z}$ y $a, b > 1$ y q y r son el cociente y el resto de dividir y_0 entre $a \Rightarrow x_1 = x_0 + b.q$, $y = r$ también son solución.