Práctico 3: Algoritmo de Euclides - Ecuaciones diofánticas.

Ec. diofánticas son del tipo $ax+by=c \quad a,b,c \in \mathbb{Z}$

Tienen sol. si y sólo si $mcd(a,b) \mid c$, si (x_0, y_0) es sol $\Rightarrow$ todas las sols son

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

$a,b>1 \quad mcd(a,b)=1 \rightsquigarrow$ no existen sol. no negativas a la ecuación

$ax+by = ab-a-b$

Si $n \geq ab-a-b+1 \Rightarrow$ existen sol. positivas a la ec.

$ax+by=n$.

compañía obtuvo una ganancia de $245, ¿cuántas reliquias faltan por vender?

Ejercicio 7. En el cambio de turno de una fábrica de cerámicas, Alex, obrero que finalizaba su trabajo, dejó preparado un embarque de baldosas para un hospital en construcción. Armó una caja de 42 baldosas y dejó escrito: *"Pérez: va esta caja de 42 unidades y el resto son cajas de 50 unidades"*. El Sr. Pérez, luego de subir al camión la de 42, comenzó a colocar las de 50 unidades, cuando se preguntó: ¿cuántas de 50 hay que llevar? Subió a Administración, donde el Sr. Fernández le ayudó a buscar la información y le avisó que el sabía que eran entre 20 y 40 cajas. Lo único que encontraron era un papel que decía: *"Baldosas de cerámica para el Hospital siquiátrico Cristóbal Colón. Salas de 32 baldosas + una sala chica de 20 baldosas"*. ¿Cuántas baldosas precisa el hospital?

1 de 42 baldosas

Resto de 50 baldosas

¿Cuántas de 50 hay que llevar? — Entre 20 y 40

Salas de 32 baldosas + una de 20

llevarán: $42 + x \cdot 50$ baldosas, queremos averiguar x sabiendo $20 \leq x \leq 40$ y

precisan $20 + y \cdot 32$ baldosas.

$$42 + x \cdot 50 = 20 + y \cdot 32$$

$$\boxed{y \cdot 32 - x \cdot 50 = 22}$$

Tiene sol. si y sólo si $mcd(32,50) \mid 22$

$32 = 2^5$

$50 = 5^2 \cdot 2$

$\Rightarrow mcd(32,50) = 2 \mid 22$ ✓

Con el Algoritmo de Euclides podemos hallar x' e y' tales que

$$y' \cdot 32 - x' \cdot 50 = 2$$

Luego $y_0 = y' \cdot 11$ y $x_0 = x' \cdot 11$ son sol a

$$y \cdot 32 - x \cdot 50 = 22$$

$$2 = 11 \cdot 32 - 7 \cdot 50$$

$$\Rightarrow y_0 = 11 \cdot 11 = 121 \qquad x_0 = 7 \cdot 11 = 77$$

Entonces todas las sol. son:

$$ax + by = c$$

en este caso $a = -50$ $\quad b = 32$ $\quad c = 22$

y $(x_0, y_0) = (77, 121)$ es sol. $\Rightarrow$ todas las sols son

$$\{(77 + 16k, 121 + 25k) : k \in \mathbb{Z}\}$$

Queremos una sol con $20 \leq x \leq 40$ y $y \geq 0$

$$20 \leq 77 + 16k \leq 40$$

$$-57 \leq 16k \leq -37$$

$$\frac{-57}{16} \leq k \leq \frac{-37}{16}$$

$$4 > \frac{57}{16} \geq -k \geq \frac{37}{16} > 2 \Rightarrow -k = 3 \Rightarrow k = -3$$

Verifiquemos: $77 - 3 \cdot 16 = 77 - 48 = 29$ ✓

$x = 29$ → Hay que llevar 29 cajas de 50 baldosas.

Ejercicio 9. Sea a un número natural mayor o igual que 2.

a. Probar que si $m|n$ entonces $a^m - 1 | a^n - 1$. [Sug. $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + 1)$]

b. Probar que si $\text{resto}(n, m) = r$ entonces $\text{resto}(a^n - 1, a^m - 1) = a^r - 1$.

c. Probar que $\text{mcd}(a^n - 1, a^m - 1) = a^{\text{mcd}(n,m)} - 1$. [Sug. utilizar el algoritmo de Euclides]

d. Calcular el máximo común divisor de $\underbrace{111\ldots1}_{2010 \text{ unos}}$ y $\underbrace{111\ldots1}_{100 \text{ unos}}$. $= 10^0 + 10^1 + 10^2 \ldots + 10^{99}$

$= (10^{100-1} + 10^{100-2} + \ldots + 1)$

a. $n = m \cdot k$ y $b^k - 1 = (b-1)(b^{k-1} + b^{k-2} + \ldots + 1) \quad \forall b \geq 2$

Si tomamos $b = a^m$:

$$(a^m)^k - 1 = (a^m - 1) \cdot (a^{m(k-1)} + a^{m(k-2)} + \ldots + 1)$$

$$a^n - 1 = (a^m - 1) \cdot C$$

$n = mk + r$

b. Tenemos que ver que $a^n - 1 = (a^m - 1)q + a^r - 1$

Observar que $0 \le a^r - 1 \le a^m - 1$.

$$a^n - 1 = a^{mk+r} - 1 = a^r \cdot a^{mk} - 1$$
$$= (a^r - 1 + 1) \cdot a^{mk} - 1$$
$$= (a^r - 1)a^{mk} + a^{mk} - 1$$

Queremos $(a^r - 1) \cdot 1$

$$= (a^r - 1)(a^{mk} - 1 + 1) + a^{mk} - 1$$
$$= a^r - 1 + (a^r - 1)(a^{mk} - 1) + a^{mk} - 1$$
$$= a^r - 1 + (a^{mk} - 1) \cdot (a^r)$$

por la parte anterior $a^m - 1$ divide $a^{mk} - 1$ q

$$= a^r - 1 + (a^m - 1) \cdot Q.$$

(c) Observar que

Algoritmo de Euclides

$\text{mcd}(n, m) = \text{mcd}(m, r)$ donde $r = \text{resto}(n, m)$

Luego, $\text{mcd}(a^n - 1, a^m - 1) = \text{mcd}(a^m - 1, \text{resto}(a^n - 1, a^m - 1))$

por la parte anterior

$$= \text{mcd}(a^m - 1, a^r - 1)$$
$$\vdots$$
$$= \text{mcd}(a^k - 1, a^{r_k} - 1)$$
$$\vdots$$
$$= \text{mcd}(a^{r'-1} - 1, a^0 - 1) = a^{r'} - 1$$

(d) $\text{mcd}(\underbrace{11 \cdots 11}_{2010 \text{ 1's}}, \underbrace{11 \cdots 11}_{100 \text{ 1's}})$

Obs: $\underbrace{11 \cdots 11}_{100 \text{ unos}} = 1 + 10 + \cdots + 10^{100-1}$

por (a) $= \dfrac{10^{100} - 1}{10 - 1}$

$\underbrace{11 \cdots 11}_{2010} = \dfrac{10^{2010} - 1}{10 - 1}$

$\Rightarrow \text{mcd} = \dfrac{\text{mcd}(10^{100} - 1, 10^{2010} - 1)}{9}$

$$= \frac{10^{\underbrace{\text{mcd}(2010, 100)}_{10}} - 1}{9}$$