AM PRÁCTICA-7

Nombre y apellidos.....

1.- Se consideran los números $a = 10^{36} + 1{,}072{,}771$ y $b = 10^{36} + 1{,}072{,}773$. Calcula $m.c.d.(a, b)$.
Indicación: Considera $b - a$.

SEA $d = mcd(a,b)$. ASS $d|a$ y $d|b$

LUEGO $a = k_1 d$ y $b = k_2 d$; LUEGO

$b - a = (k_2 - k_1) d \Rightarrow d | b-a = 10^{36} + 1{,}072{,}773 - 10^{36} - 1{,}072{,}771 = 2$

LUEGO $d = 1$ ó 2 ; COMO a y b SON IMPARES $\boxed{d = 1}$

2.- Sea $(\mathbb{Z}_m +, \times)$, con $m \in \mathbb{N}$, considerando la suma y el producto en congruencias.

2_1.- Haz la tabla de la suma y del producto de $\mathbb{Z}_6$.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2_2.- Encuentra -3 y -4. Encuentra el inverso de 5.

$-3 = 3$ YA QUE $3 + 3 = 6 \equiv 0 \mod 6$

$-4 = 2$ YA QUE $4 + 2 = 6 \equiv 0 \mod 6$

$5^{-1} = 5$ YA QUE $5 \cdot 5 = 25 \equiv 1 \mod 6$

2_3.- Encuentra elementos no nulos $a, b \in \mathbb{Z}_6 \setminus \{0\}$ de modo que $ab = 0$.

$a = 2 \neq 0$ y $b = 3 \neq 0$

YA QUE $2 \cdot 3 = 6 \equiv 0 \mod 6$

3.- Encuentra el inverso de 36 en $\mathbf{Z}_{49}$. Usa el Lema de Bezout.

$mcd(36, 49) = 1$ ya que $36 = 2^2 \cdot 3^2$ y $49 = 7^2$ no tienen divisores comunes por lo cual nos dice Bezout

$1 = mcd(36, 49) = r \cdot 36 + s \cdot 49$

$s \cdot 49 \equiv 0 \mod 49$. Luego $r \cdot 36 \equiv 1 \mod 49$

Así r es el inverso de 36 en $\mathbb{Z}_{49}$

Para calcularlo, vamos a usar el algoritmo de Euclides:

i	0	1	2				
r_i	49	36	13	10	3	1	0
q_i		1	2	1	3	3	
x_i	1	0	1	-2	3	-11	
y_i	0	1	-1	3	-4	15	

Luego $1 = (-11) \cdot 49 + 15 \cdot 36$

Así $r = (36)^{-1} = 15$

Comprobación $36 \cdot 15 = 540$

$540 \overline{)49}$
$50 \quad 11$
1

$540 \equiv 1 \mod 49$

4.- Encuentra todos los elementos de $\mathbf{Z}_{49}$ que tiene inverso.
Indicación: ¿Quizás sea más corto indicar cuáles no lo tienen? ¿Por qué?

$49 = 7 \cdot 7$

Las congruencias $7, 14, 21, 28, 35$ y 42 tienen divisores comunes con 49, por tanto cada uno de ellos

$a \cdot 7 \equiv 0 \mod 49$, por ser múltiplos de 49

para dicho $a = 7, 14, 21, 28, 35$ o 42.

Luego si $b \in \mathbb{Z}_{49} \setminus \{0, 7, 14, 21, 28, 35, 42\}$ tienen inverso en $\mathbb{Z}_{49}$ por no tener divisores comunes con 49.. Claro por el Lema de Bezout.

$1 = mcd(b, 49) = r \cdot b + s \cdot 49$

Luego como $s \cdot 49 \equiv 0 \mod 49$

$$\boxed{r \cdot b \equiv 1 \mod 49}$$