

EXAMEN - 20 DE JULIO DE 2016. ESQUEMA DE SOLUCIÓN

Ejercicio 1. Encontrar todos los n naturales tales que

$$\text{mcd}(n, 143)^2 = n + 65.$$

Solución: Sea $d = \text{mcd}(n, 143)$, como $143 = 11 \cdot 13$ tenemos que $d \in \{1, 11, 13, 143\}$. Vemos para que d hay algún n solución.

- Si $d = 1$ entonces $1 = n + 65$ y $n = 1 - 65 = -64 \notin \mathbb{N}$. Por lo que $d = 1$ queda descartado.
- Si $d = 11$ entonces $121 = n + 65$ y $n = 56 = 7 \cdot 8$, pero $\text{mcd}(65, 143) = 1$ por lo que $d = 11$ queda descartado.
- Si $d = 13$ entonces $169 = n + 65$ y $n = 104 = 8 \cdot 13$ y $\text{mcd}(104, 143) = 13$ por lo que $n = 104$ es solución.
- Si $d = 143$ entonces $143^2 = n + 65$ y $n = 143^2 - 65$. Como $11 \nmid 65$ entonces $11 \nmid n$ y queda descartado $d = 143$.

En resumen la única solución es $n = 104$.

Ejercicio 2. Calcular $0 \leq x < 245$ tal que

$$x \equiv 20^{465} \pmod{245}.$$

Solución: Como $245 = 5 \cdot 49$ la congruencia es equivalente a $\begin{cases} x \equiv 20^{465} \pmod{5} \\ x \equiv 20^{465} \pmod{49} \end{cases}$, por el Teorema Chino del Resto. Ahora, la primer congruencia del sistema es claramente equivalente a $x \equiv 0 \pmod{5}$ ya que $5 \mid 20$. Para la segunda podemos utilizar el Teorema de Euler. Primero vemos que $\varphi(49) = 7 \cdot 6 = 42$, y $465 = 42 \cdot 11 + 3$ por lo que $x \equiv 20^3 \pmod{49} \equiv 400 \cdot 20 \pmod{49} \equiv 8 \cdot 20 \pmod{49} \equiv 160 \pmod{49} \equiv 13 \pmod{49}$. Concluimos que el sistema original es equivalente a:

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 13 \pmod{49} \end{cases}.$$

La solución al sistema anterior es 160, por lo que $x \equiv 160 \pmod{245}$.

Ejercicio 3. Para los siguientes sistemas investigar si tienen solución, y en caso afirmativo, hallar todas las soluciones en \mathbb{Z} .

$$\text{a. } \begin{cases} x \equiv 23 \pmod{77} \\ x \equiv 67 \pmod{88} \\ x \equiv 2 \pmod{49} \\ x \equiv 23 \pmod{28} \end{cases} \quad \text{b. } \begin{cases} x \equiv 29 \pmod{77} \\ x \equiv 7 \pmod{88} \\ x \equiv 40 \pmod{49} \\ x \equiv 23 \pmod{28} \end{cases}.$$

Solución:

- a. Separando los módulos de las congruencias en producto de coprimos vemos que el sistema es equivalente a

$$\begin{cases} x \equiv 23 \pmod{7} \\ x \equiv 23 \pmod{11} \\ x \equiv 67 \pmod{8} \\ x \equiv 67 \pmod{11} \\ x \equiv 2 \pmod{49} \\ x \equiv 23 \pmod{4} \\ x \equiv 23 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{8} \\ x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{49} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{7} \end{cases}.$$

Eliminando las repeticiones y las implicancias de potencias de los módulos llegamos al sistema equivalente:

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{49} \end{cases}.$$

Utilizando el método de resolución de sistemas vemos que tiene solución $x \equiv 2795 \pmod{8 \cdot 11 \cdot 49}$, y todas las soluciones son $x = 2795 + 4312 \cdot k$ con $k \in \mathbb{Z}$.

b. De igual manera al sistema anterior, obtenemos que el sistema es equivalente a:

$$\begin{cases} x \equiv 29 \pmod{7} \\ x \equiv 29 \pmod{11} \\ x \equiv 7 \pmod{8} \\ x \equiv 7 \pmod{11} \\ x \equiv 40 \pmod{49} \\ x \equiv 23 \pmod{4} \\ x \equiv 23 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 7 \pmod{11} \\ x \equiv 7 \pmod{8} \\ x \equiv 7 \pmod{11} \\ x \equiv 40 \pmod{49} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{7} \end{cases}.$$

El sistema anterior no tiene solución ya que si $x \equiv 40 \pmod{49}$ entonces $x \equiv 5 \pmod{7}$ que es incongruente con la primer congruencia $x \equiv 1 \pmod{7}$.

Ejercicio 4.

- Sea $n > 1$ entero, probar que existe un primo p tal que $p \mid n$.
- Probar que existen infinitos primos.
- Enunciar y demostrar el Lema de Euclides.

Solución: Ver teórico.

Ejercicio 5.

- Enunciar y demostrar el Teorema de Lagrange.

Solución: Ver teórico.

- Sea el grupo $G = \mathbb{Z}_{14}$.

- Listar los elementos de G junto a sus ordenes.

Solución:

g	$o(g)$
0	1
1	14
2	7
3	14
4	7
5	14
6	7
7	2
8	7
9	14
10	7
11	14
12	7
13	14

Observar que el orden se puede calcular usando la fórmula $o(g^n) = \frac{o(g)}{\gcd(n, o(g))}$, y tomando $g = 1$ obtenemos que $o(n) = \frac{14}{\gcd(14, n)}$.

- Listar todos los subgrupos de G .

Solución: Observamos que G es cíclico, y por lo tanto cualquier subgrupo de G es cíclico. Vemos entonces que los subgrupos H de G tienen que ser:

- $H = \{0\} = \langle 0 \rangle$.
- $H = G = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 9 \rangle = \langle 11 \rangle$.
- $H = \{0, 2, 4, 6, 8, 10, 12\} = \langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle$.
- $H = \{0, 7\} = \langle 7 \rangle$.
- $H = \{0, 13\} = \langle 13 \rangle$.