# AM PRÁCTICA-8

**Nombre y apellidos**.................................................................

**1.-** Resuelve el sistema en congruencias: $\left.\begin{array}{rl} x \equiv 1 & \text{mod } 3 \\ 2x \equiv 5 & \text{mod } 11 \\ x \equiv 3 & \text{mod } 7 \end{array}\right\}$

**Indicación:** Teorema Chino del Resto.

COMO $2^{-1}$ mod 11 ES 6 $\left\{\begin{array}{l} x \equiv 1 \text{ mod } 3 \\ 2x \equiv 5 \text{ mod } 11 \\ x \equiv 3 \text{ mod } 7 \end{array}\right.$ $\iff$ $\begin{array}{l} x \equiv 1 \text{ mod } 3 \\ x \equiv 30 \equiv 8 \text{ mod } 11 \\ x \equiv 3 \text{ mod } 7 \end{array}$

APLICANDO EL TEOREMA CHINO DEL RESTO

$x \equiv 1 \times 77 \times 2 + 8 \times 21 \times 10 + 3 \times 33 \times 3 = 154 + 1680 + 297 = 2131$

$77 \equiv 2$ mod 3, $2^{-1} = 2$ $\quad$ $21 \equiv 10$ mod 11, $10^{-1} = 10$ $\quad$ $33 \equiv 5$ mod 7, $5^{-1} = 3$

$x \equiv 2131 \text{ mod}(3 \times 11 \times 7) \iff \boxed{x \equiv 52 \text{ mod } 231}$

COMPROBACIÓN

$52 = 3 \cdot 17 + 1$ $\quad$ $52 = 11 \cdot 4 + 8$ $\quad$ $52 = 7 \cdot 7 + 3$

**2.-** Dado el isomorfismo: $\begin{array}{rccc} f & : & \mathbb{Z}_{140} & \rightarrow & \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \\ & & [a]_{140} & \rightarrow & ([a]_4, [a]_5, [a]_7) \end{array}$ Encuentra la preimagen de $([2]_4, [3]_5, [4]_7)$.

$f^{-1}([2]_4, [3]_5, [4]_7) = x$ y $\begin{array}{l} x \equiv 2 \text{ mod } 4 \\ x \equiv 3 \text{ mod } 5 \\ x \equiv 4 \text{ mod } 7 \end{array}$

USANDO EL TEOREMA CHINO DEL RESTO

$x = 2 \times 35 \times 3 + 3 \times 28 \times 2 + 4 \times 20 \times 6 = 210 + 168 + 480 =$

$35 \equiv 3$ mod 4, $3^{-1} = 3$ $\quad$ $28 \equiv 3$ mod 5, $3^{-1} = 2$ $\quad$ $20 \equiv 6$ mod 7, $6^{-1} = 6$

$= 858 \text{ mod}(140) \iff \boxed{x \equiv 18 \text{ mod } (140)}$

COMPROBACIÓN:

$18 = 4 \cdot 4 + 2$ $\quad$ $18 = 5 \cdot 3 + 3$ $\quad$ $18 = 7 \cdot 2 + 4$

**3.-** Determina la última cifra del número $18^{2019}$.
**Indicación:** Usa el problema anterior junto con el Teorema de Euler.

QUEREMOS CALCULAR $18^{2019} \equiv x$ mod 10.

SEA $f \quad \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$

$x = 18^{2019} \longrightarrow ([18^{2019}]_2, [18^{2019}]_5) = (0, [18^{2019}]_5)$

$2 \mid 18$

AHORA mcd$(18,5) = 1$, $\phi(5) = 4$

Y ASÍ COMO $2019 = 4 \cdot 504 + 3$

$18^{2019} = 18^{4 \times 504 + 3} \equiv 1 \times 18^3 \text{ mod } 5,$ $\quad$ $18 \equiv 3$ mod 5, $18^3 \equiv 27 \equiv 2$ mod 5.

TEOREMA DE EULER

$(0,2) \in \mathbb{Z}_2 \times \mathbb{Z}_5$ ; ¿ $f^{-1}((0,3)) = x$ ?

$x \equiv 0 \mod 2$
$x \equiv 2 \mod 5$ $\iff$ $x \equiv 2 \mod 10$. LUEGO LA ÚLTIMA CIFRA DE $18^{2019}$ ES 2

(Continuación 3).

**4.-** Dado el grupo $(G, +)$ donde $G = \mathbb{Z}_{12} \times \mathbb{Z}_{28} \times \mathbb{Z}_{56}$ ¿Cuál es el orden máximo de los elementos del grupo? Encuenta el orden del elemento $([9]_{12}, [16]_{28}, [14]_{56})$. Justifica tu respuesta.

$mcm(12, 28, 56) = 2^3 \times 7 \times 3 = 8 \times 21 = \boxed{168}$ ORDEN MÁXIMO DE ALGÚN ELEMENTO

$12 = 2^2 \times 3$
$28 = 2^2 \times 7$
$56 = 2^3 \times 7$

ord 9 EN $\mathbb{Z}_{12}$ ES $mcm(9,12) = 36$ $\quad 36/9 = 4$
ord 9 EN $\mathbb{Z}_{12}$ ES 4

ord 16 EN $\mathbb{Z}_{28}$ ES $mcm(16, 28) = 16 \times 7 = 112$ $\quad 112/16 = 7$
ord 9 EN $\mathbb{Z}_{28}$ ES 7

ord 14 EN $\mathbb{Z}_{56}$ ES $mcm(14, 56) = 56$ $\quad 56/14 = 4$
ord 14 EN $\mathbb{Z}_{56}$ ES 4

LUEGO $ord([9]_{12}, [16]_{28}, [14]_{56})$ EN $\mathbb{Z}_{12} \times \mathbb{Z}_{28} \times \mathbb{Z}_{56}$ ES $mcm(4, 7, 4) = 28$.

**$5_1$.-** Se considera el subconjunto $G = \{1, -1, \imath, -\imath\} \subset \mathbb{C}$, donde $\imath = \sqrt{-1}$. ¿Es $G$ con el producto un grupo? ¿Es cíclico? Encuentra un generador $g$ ¿Cuál es el orden de $g^2$?

| × | 1 | -1 | $i$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | -1 | $i$ | $-i$ |
| -1 | -1 | 1 | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | -1 | 1 |
| $-i$ | $-i$ | $i$ | 1 | -1 |

LA TABLA PRUEBA QUE G ES UN GRUPO CONMUTATIVO

$G = \{ i, i^2 = -1, i^3 = -i, i^4 = 1 \}$ LUEGO G ES CÍCLICO

y $g = i$ ES UN GENERADOR

$g^2 = (i^2) = -1$ EL $ord(-1) = 2$ YA QUE $(-1)^2 = 1$.

**$5_2$.-** En general, si $g$ es un generador de un grupo $G = \{g, g^2, \ldots, g^{n-1}, g^n = 1\}$, ¿cuál es el orden de $g^k$, $k < n$?

$ord(g^k) = \min\{ r : (g^k)^r = 1 = g^{kn} \}$.

LUEGO SI $s = mcm(k, n)$, ENTONCES $\boxed{r = \frac{s}{k} = \frac{mcm(k,n)}{k}}$