# AM PRÁCTICA-8

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

**1.-** Resuelve el sistema en congruencias: $\left.\begin{array}{rl} x \equiv 1 & \text{mod } 3 \\ 2x \equiv 5 & \text{mod } 11 \\ x \equiv 3 & \text{mod } 7 \end{array}\right\} \iff$ $2 \times 6 \equiv 1 \text{ mod } 11$

$x \equiv 1 \text{ mod } 3$
$x \equiv 5 \times 6 \equiv 7 \text{ mod } 11$
$x \equiv 3 \text{ mod } 7$

**Indicación:** Teorema Chino del Resto.

$x = 1 \times 77 \times 2 + 7 \times 21 \times 10 + 3 \times 33 \times 3 = 154 + 1470 + 297 =$

$77 \equiv 2 \text{ mod } 3$ ; $2 \times 2 \equiv 1 \text{ mod } 3$

$21 \equiv 10 \text{ mod } 11$ ; $10 \times 10 \equiv 1 \text{ mod } 11$

$33 \equiv 5 \text{ mod } 7$ ; $5 \times 3 \equiv 1 \text{ mod } 7$

$= 1921 \text{ mod } 231$ LUEGO

1921 | 231
073 | 8

$x \equiv 73 \text{ mod } 231$

COMPROBACIÓN

73 | 3
13 | 24
1

73 | 11
7 | 6

73 | 7
03 | 1

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

SI $f(x) = ([2]_4, [3]_5, [4]_7) \iff$ $x \equiv 2 \text{ mod } 4$, $x \equiv 3 \text{ mod } 5$, $x \equiv 4 \text{ mod } 7$

DONDE 4, 5 y 7 SON PRIMOS ENTRE SÍ.

POR EL TEOREMA CHINO DEL RESTO

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

$35 \equiv 3 \text{ mod } 4$ ; $28 \equiv 3 \text{ mod } 5$ ; $20 \equiv 6 \text{ mod } 7$

$= 858 \text{ mod } 140$ LUEGO

858 | 140
018 | 6

$x \equiv 58 \text{ mod } 140$

COMPROBACIÓN

18 | 4
2 | 4

18 | 5
3 | 3

18 | 7
4 | 2

**3.-** Determina las últimas dos cifras del número $18^{2019}$.
**Indicación:** Usa el problema anterior junto con el Teorema de Euler. $\phi$

LA SOLUCIÓN ES $x \equiv 18^{2019} \text{ mod } 100$

SEA $f: \mathbb{Z}_{100} \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_{25}$
$[a]_{100} \longrightarrow ([a]_4, [a]_{25})$

SI $a = 18^{2019} = 2^{2019} \times 9^{2019}$ LUEGO $a$ ES MÚLTIPLO DE 4 y $a \equiv 0 \text{ mod } 4$

$\text{mcd}(18, 25) = 1$ ; $\phi(25) = 25(1 - \frac{1}{5}) = 20$ ; POR EL TEOREMA DE EULER $\longrightarrow$

$18^{20} \equiv 1 \mod 25$ $\quad 18^{2019} = 18^{20\times 100+19} = 18^{19} \equiv (-7)^{19} \mod 25$

$\equiv (49)^9(-7) \equiv (-1)^9(-7) \equiv 7 \mod 25$

Así $f(18^{2019}) = ([0]_4, [7]_{\mathrm{mod}\ 25})$

(Continuación 3).

Buscamos $x \equiv 0 \mod 4$

$x \equiv 7 \mod 25$ por el teorema chino del resto

$\boxed{x \equiv 32 \mod 100.}$

4.- Encuentra $x$ que satisfaga $25x \ mod\ 65 = 5 \cdot 27^{8042} \ mod\ 10$.

¿$27^{8042} \mod 10$? Como $\mathrm{mcd}(27,10)=1$ y la función de Euler

$\phi(10) = \phi(2)\phi(5) = 1\cdot 4 = 4$ y $8042 = 4\cdot 2010 + 2$ $\quad 27^{8042} = 27^{4\times 2010} \times 27^2 \equiv$

$1 \times 7^2 \equiv 49 \equiv 9 \mod 10$ $\quad$ Así $5\times 9 \equiv 45 \equiv 5 \mod 10$

Los elementos de $\mathbb{Z}_{65}$ iguales a $5 \mod 10$ son $5, 15, 25, 35, 45, 55$.

Así $25x \equiv k \mod 65$ con $k = 5, 15, 25, 35, 45, 55$

$\iff 25x = k + k'65$ donde $k' \in \mathbb{Z}$.

$\iff 5x = k/5 + k'13$ " $k' \in \mathbb{Z}$ $\quad k/5 = 1, 3, 5, 7, 9$ y $11$

Es decir $5x \equiv k/5 \mod 13$ $\quad 5^{-1} \equiv 8 \mod 13$

Luego $x \equiv 8\, k/5 \mod 13$ Así

$x \equiv 8 \mod 13$; $k/5 = 1$ / $x \equiv 24 \equiv 11 \mod 13$; $k/5 = 3$ / $x \equiv 40 \equiv 1 \mod 13$; $k/5 = 5$ / $x \equiv 56 \equiv 4 \mod 13$; $k/5 = 7$ / $x \equiv 72 \equiv 7 \mod 13$; $k/5 = 9$ / $x \equiv 88 \equiv 10 \mod 13$. $k/5 = 11$

5.- En el siglo XXIII la población mundial se cuenta por billones de personal. El problema de la vivienda se pudo resolver en el siglo XXII. No así él del juego. Tu tatara....nieto juega el número $4^{51}3^{18}$ del sorteo de Navidad de dentro de dos siglos, cuyo primer premio será el 1.000.788.824 (un número bajito). Si los números terminados en 24 reciben un premio de 1000 eurodolares ¿Le tocará el premio a tu tatara...nieto?

Queremos calcular $x \equiv 4^{51}3^{18} \mod 100$ $\qquad \mathbb{Z}_{100} \xrightarrow{f} \mathbb{Z}_4 \times \mathbb{Z}_{25}$

$a \longrightarrow f(a) = ([a]_4, [a]_{25})$

$[4^{51}3^{18}]_4 = [0]_4$; $\quad \mathrm{mcd}(4,5) = 1$, $\mathrm{mcd}(3,5) = 1$ $\quad \phi(25) = 20$

Luego $[4^{2\times 20+11}]_{25} = [4^{11}]_{25} = [16^5 \times 4]_{25} = [(-9)^5 \times 4]_{25} = [6^2(-9)\times 4]_{25} = [-36^2]_{25} =$

$[3^{18}]_{25} = [27^6]_{25} = [2^6]_{25} = [64]_{25} = [14]_{25}$ $\qquad = [-11^2]_{25} = [-121]_{25} = [-21]_{25} = [4]_{25}$

Luego $[4^{51}\cdot 3^{18}]_{25} = [14 \times 4]_{25} = [56]_{25} = [6]_{25}$

Buscamos $a \equiv 0 \mod 4$

$a \equiv 6 \mod 25$ por el teorema chino del resto

$a = 6 \times 4 \times 19 = 456 \mod 100$ $\quad$ luego $a \equiv 56 \mod 100$

$4 \times 19 \equiv 1 \mod 25$

¡No tocó el premio!