Problema 3.7.13. *Hallar todas las soluciones de la congruencia* $x^3 + 2x^2 - x + 6 \equiv 0$ *(mód 98).*

Solución:

$98 = 2 \cdot 7^2$, luego tenemos que analizar las siguientes congruencias:

- $x^3 + 2x^2 - x + 6 \equiv 0$ mód 2
- $x^3 + 2x^2 - x + 6 \equiv 0$ mód 7^2

Caso 1:

$$x^3+2x^2-x+6 \equiv 0 \, mod \, 2 \Rightarrow x^3-x \equiv 0 \, mod \, 2 \Rightarrow x(x^2-1) \equiv 0 \, mod \, 2 \Rightarrow \begin{cases} x \equiv 0 \text{ mód } 2 \\ \text{ó} \\ x \equiv 1 \text{ mód } 2 \end{cases}$$

Caso 2:

Sea $f(x) = x^3 + 2x^2 - x + 6$ mód 7 (NOTA: En este caso, $\alpha = 2$, luego $7^{\alpha-1} = 7$). Probando con todos los posibles restos módulo 7, llegamos a que $f(4) = 0$, y sólo lo cumple $x = 4$. Además, $f'(x) = 3x^2 + 4x - 1$ y $f'(4) \equiv 0$ mód 7, luego, por el Teorema visto en clase, tenemos que podemos subir 4 de 7 a 7^2 de 7 formas diferentes, para ello

$$a = 4 + 7q$$

con q $\in \{0, 1, 2, 3, 4, 5, 6\}$, luego

$$a = 4, 11, 18, 25, 32, 39, 46.$$

Por otro Teorema, sabemos que el número de soluciones totales de nuestra congruencia inicial es el producto del número de soluciones en cada uno de los módulos que dividen al módulo inicial, luego en total tenemos $2 \cdot 7 = 14$ soluciones.

Usaremos el Teorema Chino del Resto para calcularlas. Para ello, sabemos que la solución será de la forma

$$x' = M_1 \cdot M_2' \cdot b_1 + M_2 \cdot M_2' \cdot b_2$$

con

$$M_1 = \frac{98}{2} = 49 \; ; \; M_2 = \frac{98}{49} = 2$$

Entonces:

- $M_1' \equiv M_1^{-1}$ mód $2 \Leftrightarrow M_1' \equiv 49^{-1}$ mód 2
  $49 = 24 \cdot 2 + 1 \Rightarrow 1 = 49 - 24 \cdot 2 \Rightarrow 49^{-1} = 1$
- $M_2' \equiv M_2^{-1}$ mód $49 \Leftrightarrow M_2' \equiv 2^{-1}$ mód 49
  $49 = 24 \cdot 2 + 1 \Rightarrow 1 = 49 - 24 \cdot 2 \Rightarrow 2^{-1} = 25$

Luego tenemos

$$x' = 49 \cdot 1 \cdot b_1 + 2 \cdot 25 \cdot b_2$$

con $b_1 \in \{0, 1\}$ y $b_2 \in \{0, 1, 2, 3, 4, 5, 6\}$.

Tomando todas las posibles combinaciones, obtenemos

$$x = 4, 60, 18, 74, 32, 88, 46, 53, 11, 67, 25, 81, 39, 95$$

donde las 7 primeras posibilidades corresponden a tomar $b_1 = 0$ y las 7 últimas a $b_1 = 1$, mientras b_2 toma los valores anteriormente obtenidos para a, y reduciendo todos los resultados módulo 98.

Problema escrito por Loly Soriano.