Pràctica 4: EL TEOREMA XINÈS DEL RESIDU

1. Resol el sistema de congruències

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 1 \pmod 5, \\ x \equiv 3 \pmod 7. \end{cases}$$

2. Esbrina el significat de les funcions següents del *Mathematica*: `Product`, `Sum`, `Length`, `Apply`, `PowerMod`.

3. Defineix una funció `TXR` que, donades dues llistes d'enters $a = \{a_1, \ldots, a_k\}$ i $m = \{m_1, \ldots, m_k\}$, on els m_i són positius i relativament primers, retorni l'única solució del sistema de congruències

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

que és positiva i menor que el producte dels mòduls m_i. Aquí tens un possible esquema per a la funció `TXR`:

(a) Defineix $M = m_1 m_2 \cdots m_k$.

(b) Calcula els quocients $r_i = M/m_i$.

(c) Calcula l'invers s_i de r_i mòdul m_i.

(d) Calcula $y = a_1 r_1 s_1 + \cdots + a_k r_k s_k$.

(e) Redueix la solució obtinguda: $x = \text{Mod}[y, M]$.

No utilitzis cap bucle; tingues en compte que cadascun dels passos anteriors es pot fer amb una única instrucció de *Mathematica* per mitjà de les funcions de l'exercici anterior.

4. Utilitza la funció `TXR` de l'exercici anterior per implementar la suma modular.
Es tracta de construir una funció que, donada una llista $m = \{m_1, \ldots, m_k\}$ d'enters positius i relativament primers dos a dos, i donats dos enters positius a, b menors que $m_1 m_2 \cdots m_k/2$, calculi $a + b$ a partir dels residus de a i b mòdul els m_i.
Observació: Pots definir la suma modular en una sola línia.

5. Implementa la multiplicació modular.
Observació: Pots definir la multiplicació modular en una sola línia.