PRACTICO 5:

Teorema Chino del Resto:

Sean $m_1, m_2, \dots, m_k \in \mathbb{Z}$ coprimos dos a dos y $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Entonces el sistema

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases} \rightarrow$$

tiene solución y hay una única sol. módulo $m_1 \dots m_k$

Es decir si x_0 es solución

$\Rightarrow$ todas las soluciones son $x \equiv x_0 \pmod{m_1 \dots m_k}$

Obs: Si x_0 es solución del sist $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$ la afirmación de que el sist equivale a $x \equiv x_0 \bmod m_1 m_2$ vale solo si m_1 y m_2 son coprimos

Obs 2: Si los módulos NO son coprimos y existe una solución al sistema $\Rightarrow$ si x_0 es solución, todas las soluciones son de la forma:

$x \equiv x_0 \pmod{\text{mcm}(m_1, \dots, m_k)}$

¿Como hacer ejercicios de TCR?

Tengo el sistema: $\begin{cases} x \equiv a_1 \bmod m_1 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$

1) Si los módulos no son coprimos, los separo hasta llevar el sistema a las hipótesis del TCR

2) Despejo x: $x = a_1 + k_1 \cdot m_1$, y lo sustituyo en la siguiente ecuación $a_1 + k_1 m_1 \equiv a_2 \bmod m_2$ y busco k_1 que resuelva la ecuación y encuentro x_0: $x \equiv x_0 \bmod (m_1 \cdot m_2)$

Obs: Puedo encontrar el inverso de $m_1 \bmod m_2$ ya que $\text{mcd}(m_1, m_2) = 1$

3) Hago lo mismo que en el paso anterior pero ahora con m_3 y $m_1 \cdot m_2$, es decir busco x:

$$\begin{cases} x \equiv x_0 \bmod m_1 m_2 \\ x \equiv a_3 \bmod m_3 \end{cases}$$

4) Repito el procedimiento hasta llegar a una solución y_0:

$x \equiv y_0 \bmod (m_1 \dots m_k)$

Propiedades Practico:

- Si m_1 y m_2 son coprimos y $b_1, b_2 \in \mathbb{Z}$:

  $b_1 \cdot m_2 \equiv 1 \bmod m_1$ y $b_2 \cdot m_1 \equiv 1 \bmod m_2$

  $\Rightarrow \forall a_1, a_2 \in \mathbb{Z}$, el entero $x = a_1 \cdot b_1 \cdot m_2 + a_2 \cdot b_2 m_1$ es solución del sist. $\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$

- Sean $m_1, \dots, m_k$ enteros coprimos 2 a 2 con $M_i = \frac{m_1 \dots m_k}{m_i}$ y $b_1, \dots, b_k \in \mathbb{Z}$

  Entonces:

  1) $b_i \cdot M_i \equiv 1 \pmod{m_i}$ $\forall i = 1, \dots, k$

  2) $\forall a_1, \dots, a_k \in \mathbb{Z}$, $x = a_1 \cdot b_1 \cdot M_1 + \dots + a_k \cdot b_k \cdot M_k$ es solución del sist.

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

Exponenciación:

Función de Euler: $\varphi: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ dada por

$\varphi(n) = \#\{a \in \{1, \dots, n\} : \text{mcd}(a, n) = 1\}$

Propiedades

- Si p es primo $\Rightarrow \varphi(p) = p - 1$
- Si p es primo $\Rightarrow \varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$
- Si $\text{mcd}(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$ (Euler)

Teorema: Si $\text{mcd}(m, n) = 1$ $\Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Corolario: (Pequeño teo. de Fermat)

$a^p \equiv a \bmod p$. / $a^{p-1} \equiv 1 \bmod p$ (a coprimo con p)