Teoría de Números 2022

Lista 03

04.agosto.2022

1. a) Dar un ejemplo para mostrar que $a^2 \equiv b^2 \pmod{n}$ no necesariamente implica que $a \equiv b \pmod{n}$.
   b) Mostrar que i $a \equiv b \pmod{n}$, entonces $(a, n) = (b, n)$.

2. Comprobar que
   a) $53^{103} + 103^{53}$ es divisible por 39,
   b) $111^{333} + 333^{111}$ es divisible por 7.

3. Asumiendo que $495 \mid 273x49y5$, encontrar los dígitos x y y.

4. Pruebe que para todo $n > 2$, se cumple que $\displaystyle\sum_{(k,n)=1\ 1\leq k\leq n} k = \frac{n\varphi(n)}{2}$.

5. a) Construya un criterio de divisibilidad entre 59.
   b) Utilice el criterio anterior para verificar si los números 45843, 19641 y 32763 son divisibles entre 59.

6. sea $m \in \mathbb{Z}^+$ un entero positivo, y sean a y b enteros primos relativos a m. Si x y y son eneros tales que

$$a^x \equiv b^x \pmod{m} \quad \text{y} \quad a^y \equiv b^y \pmod{m}$$

   entonces

$$a^{(x,y)} \equiv b^{(x,y)} \pmod{m}.$$

7. Mostrar que:
   a) Si $\{a_1, a_2, \dots, a_n\}$ y $\{b_1, b_2, \dots, b_n\}$ son ambos sistemas completos de residuos módulo n, entonces $\{a_1 + b_1, a_2 + b_2, \dots, a_n + b_n\}$ no es un sistema completo de residuos.
   b) Si $a \in \mathbb{Z}$, entonces $\{a, 2a, 3a, \dots, na\}$ es un sistema completo de residuos módulo n si, y sólo si, $(a, n) = 1$.
   c) Si $S = \{r_1, r_2, \dots, r_n\}$ es un sistema completo de residuos módulo n, y $a, b \in \mathbb{Z}$ son tales que $(a, n) = 1$, entonces

$$T = aS + b = \{ar_1 + b, ar_2 + b, \dots, ar_n + b\}$$

   es también un sistema completo de residuos módulo n.

8. Implementar en Python el algoritmo para el cálculo de potencias módulo n mediante exponenciación binaria (potenciación modular). Usarlo para calcular las siguientes:
   a) $123^{456} \pmod{789}$.
   b) $2022^{1001} \pmod{2202}$,