

Tarea núm. 6

Para el jueves 11 mar. 2010

- Sean $a, b, m, n \in \mathbb{Z}$, donde $m, n > 1$ y $(m, n) = 1$. Demuestra:
 - Existe un $x \in \mathbb{Z}$ tal que $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$.
 - Tal x es único modo mn . O sea, si $y \in \mathbb{Z}$ tal que $y \equiv a \pmod{m}$ y $y \equiv b \pmod{n} \implies x \equiv y \pmod{mn}$.

Sugerencia para inciso (a): las soluciones a la primera ecuación son de la forma $x := a + km$, $k \in \mathbb{Z}$. Ahora busca las k tal que x resuelva la segunda ecuación también. Es útil introducir el recíproco de $m \pmod{n}$.

Sugerencia para inciso (b): define $z := x - y$ y estudia sus propiedades.

- Sean $a_1, \dots, a_k, n_1, \dots, n_k \in \mathbb{Z}$, donde $n_1, \dots, n_k > 1$ y $(n_i, n_j) = 1$ para cada $i \neq j$. Demuestra que existe un x , único mod $n_1 \cdots n_k$, tal que $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_k \pmod{n_k}$ (son k congruencias que el x debe satisfacer.)

Nota: este resultado se llama el "Teorema Chino de Resíduos".

Sugerencia: usar el Problema anterior e inducción sobre k .

- Sean $A, B, m, n \in \mathbb{Z}$, donde $m, n > 1$ y $(m, n) = 1$. Entonces $A \equiv B \pmod{mn}$ si y solo si $A \equiv B \pmod{m}$ y $A \equiv B \pmod{n}$.

Sugerencia: se puede demostrar directamente, o se puede usar el problema 1, con $a = b = 0$, $x = A - B$.

- Sean p, q dos primos distintos, $n = pq$, $f = (p - 1)(q - 1)$, $c \in \mathbb{Z}$ tal que $c > 0$ y $(c, f) = 1$. Sea $d \in \mathbb{Z}$, $d > 0$, un recíproco de $d \pmod{f}$. Demuestra que para todo $M \in \mathbb{Z}$, $(M^c)^d \equiv M \pmod{n}$.

Sugerencia: Según el problema anterior, basta demostrar esta congruencia mod p y mod q . Para esto usa el teorema de Fermat ($x^p \equiv x \pmod{p}$ para todo primo p y entero x).

- Resolver las siguientes congruencias (encontrar todos los valores enteros de x en cada caso):
 - $3x \equiv 2 \pmod{5}$.
 - $3x \equiv 2 \pmod{100}$.
 - $17x \equiv 1 \pmod{100}$.
 - $x \equiv 77^{77} \pmod{100}$.
 - $x \equiv 14 \pmod{15}$ y $x \equiv 16 \pmod{17}$.
 - $29 \equiv x^{87} \pmod{55}$.