Tarea núm. 5

Para el viernes 5 de sept. 2008

1. Sea $n \in \mathbb{Z}$ con $n > 1$. Demuestra que para todo $a, b \in \mathbb{Z}$ con $a \equiv b \mod n$, $(a, n) = 1$ si y solo si $(b, n) = 1$. (O sea, la condición $(a, n) = 1$ depende solamente de la clase de congruencia de a mod n.)

   Nota: "A si y solo si B" significa "A implica B y B implica A" (dos incisos separados).

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

   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 tambien. Es útil usar el problema 1 de la tarea 4.

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

3. Sean $a_1, \ldots, a_k, n_1, \ldots, n_k \in \mathbb{Z}$, donde $n_1, \ldots, n_k > 1$ 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 $x \equiv a_1 \mod n_1$, $\ldots$, $x \equiv a_k \mod n_k$ (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.

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

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

5. Sean p, q dos primos distintos, $n = pq$, $f = (p-1)(q-1)$ y $M, k \in Z$, $k \geq 0$. Demuestra que $M^{1+fk} \equiv M \mod n$.

6. Resolver las siguientes ecuaciones (encontrar todos los valores de x en cada caso):
   a) $3x \equiv 2 \mod 5$.
   b) $3x \equiv 2 \mod 100$.
   c) $17x \equiv 1 \mod 100$.
   d) $x \equiv 77^{77} \mod 100$.
   e) $x \equiv 14 \mod 15$ y $x \equiv 16 \mod 17$.
   f) $29 \equiv x^{87} \mod 55$.