Tarea núm. 6

Para el jueves 11 mar. 2010

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

   ▷ El conjunto de soluciones a la primera congruencia, $x \equiv a \pmod{m}$, es $x = a + km$, $k \in \mathbb{Z}$. Luego, $x \equiv b \pmod{n} \iff x = a + km \equiv b \bmod n \iff km \equiv b - a \bmod n$. Luego, como $(m, n) = 1$, m tiene un recíproco modo n, digamos m', por loq ue la última congruencia es equivalente a $k \equiv m'(b - a) \bmod n$. O sea, existe un $l \in \mathbb{Z}$ tal que $k = m'(b - a) + ln$, así que $x = a + km = a + (m'(b - a) + ln)m = x_0 + l(nm)$, donde $x_0 = a + m'm(b - a)$. El conjunto de soluciones es entonces la clase de congruencia modulo nm de x_0. □

2. 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 $x \equiv a_1 \bmod n_1$, $\ldots$, $x \equiv a_k \bmod n_k$ (son k congruencias que el x debe satisfacer.)

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

   ▷ Usamos inducción en k. Para $k = 1$ no hay nada que demostrar. Suponemos el teorema cierto para un sistema con menos que k congruencias y lo demostramos para k. El conjunto de soluciones a las primeras $k - 1$ congruencias es entonces una clase de congruencia, digamos $[A]$, módulo N, donde $N = n_1 \cdots n_{k-1}$. Así que el sistema de las k congruencias es equivalente al par de congruencias $x \equiv A \bmod N$, $x \equiv n_k \bmod n_k$. Para resolver esto, notamos primero que $(N, n_k) = 1$ (demostración: si p es un primo tal que $p|N, n_k \implies p|N \implies p$ divide alguno de los $n_1, \ldots, n_{k-1}$, por el lema de Euclides), por lo que se aplica el problema anterior para dar una solución, única mod $Nn_k = n_1 \cdots n_k$. □

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

   ▷ Sea $C := A - B$, entonces $A \equiv B \bmod mn \iff C \equiv 0 \bmod mn \iff C \equiv 0 \bmod m$ y $C \equiv 0 \bmod n$ (usando el primer problema) $\iff A \equiv B \bmod m$ y $A \equiv B \bmod n$. □

4. 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 $d \bmod f$. Demuestra que para todo $M \in \mathbb{Z}$, $(M^c)^d \equiv M \bmod n$.

   ▷ Según el problema anterior, basta demostrar esta congruencia mod p y mod q. Como d es un recíproco de $c \bmod f$, $cd = 1 + kf$ para algun $k > 0$. Calculemos primero mod p. Si $M \equiv 0 \bmod p$ entonces $(M^c)^d \equiv M \bmod p$ trivialmente. Si $M \not\equiv 0 \bmod p$, entonces por el teorema de Fermat, $M^{p-1} \equiv 1 \bmod p \implies M^f = M^{(p-1)(q-1)} = (M^{(p-1)})^{(q-1)} \equiv 1 \implies (M^c)^d = M^{cd} = M^{1+kf} = M(M^f)^k \equiv M \bmod p$. De manera similar demostramos $(M^c)^d \equiv M \bmod q$. □

5. Resolver las siguientes congruencias (encontrar todos los valores enteros de x en cada caso):

   a) $3x \equiv 2 \bmod 5$.

   ▷ Multiplicamos ambos lados por $3^{-1} \equiv 2 \bmod 5 \implies x \equiv 2 \cdot 2 = 4 \bmod 5 \implies x = 4 + 5k$, $k \in \mathbb{Z}$. □

   b) $3x \equiv 2 \bmod 100$.

   ▷ Tenemos que $3 \cdot 33 = 99 \equiv -1 \bmod 100 \implies 3 \cdot (-33) \equiv 1 \implies 3^{-1} \equiv -33 \bmod 100 \implies x \equiv 2 \cdot (-33) = -66 \equiv 34 \bmod 100$. □

   c) $17x \equiv 1 \bmod 100$.

   ▷ Usamos problema 3 para reducir esta congruencia al par $17x \equiv 1 \bmod 25$ y $17x \equiv 1 \bmod 4$. El segundo da $x \equiv 1 \bmod 4 \implies x = 4k + 1$, $k \in \mathbb{Z} \implies 17(4k + 1) \equiv 1 \bmod 25 \implies 7k \equiv 16 \bmod 25$. Luego, $7 \cdot 7 = 49 \equiv -1 \bmod 25 \implies 7^{-1} \equiv -7 \bmod 25 \implies k \equiv (-7) \cdot 16 = -112 \equiv -12 \equiv 13 \bmod 25 \implies x \equiv 4k+1 \equiv 4 \cdot 13+1 = 53 \bmod 100$. □

   d) $x \equiv 77^{77} \bmod 100$.

   ▷ Usando problema 3, esto es equivalente a $x \equiv 77^{77} \bmod 25$ y $x \equiv 77^{77} \bmod 4$. Calculemos primero mod 4: $x \equiv 77^{77} \equiv 1^{77} \equiv 1 \bmod 4$. Luego mod 25: $x \equiv 77^{77} \equiv 2^{77} \equiv 2^{80-3} \equiv (2^{20})^4 m^3 \equiv m^3 \bmod 25$, donde $m = 2^{-1} \equiv 13 \bmod 25 \implies x \equiv 13^3 = 169 \cdot 13 \equiv (-8) \cdot 13 - 104 \equiv -4 \equiv 21 \bmod 25$. Como $21 \equiv 1 \bmod 4 \implies x \equiv 21 \bmod 100$. □

   e) $x \equiv 14 \bmod 15$ y $x \equiv 16 \bmod 17$.

   ▷ esto es equivalente a $x \equiv -1 \bmod 15$ y $x \equiv -1 \bmod 17$. Como $x = -1$ es una solución, tenemos, por problema 3, $x \equiv 1 \bmod 16 \cdot 17$. □

   f) $29 \equiv x^{87} \bmod 55$.

   ▷ Sea $f = \phi(55) = 40$. Sea $c = 87$ y $d > 0$ un recíproco de $c \bmod f$. Según problema 4, $x \equiv 29^d \bmod 55$. Buscamos a d: $87d \equiv 7d \equiv 1 \bmod 40$, así que $d = 23$ es una opción. Luego $x \equiv 29^{23} \bmod 55$ es equivalente (problema 3) al par de congruencias $x \equiv 29^{23} \bmod 11$, $x \equiv 29^{23} \bmod 5$. Calculemos primero mod 11: $x \equiv 29^{23} \equiv (-4)^{2 \cdot 10+3} \equiv (-4)^3 = -16 \cdot 4 \equiv -5 \cdot 4 = -20 \equiv 2$. Luego mod 5: $x \equiv 29^{23} \equiv (-1)^{23} = -1 \bmod 5$. Luego, $x \equiv 2 \bmod 11 \implies x = 2 + 11k$, $k \in \mathbb{Z} \implies 2 + 11k \equiv -1 \bmod 5 \implies k \equiv -3 \equiv 2 \bmod 5 \implies x \equiv 2 + 11 \cdot 2 \equiv 24 \bmod 55$. □