Tarea num. 12

Para entregar el 11 de nov. 99

1. (a) Sea $n = pq$ donde p y q son dos primos distintos. Demuestra que $a^{t+1} \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$, donde $t = (p-1)(q-1)$.
   (Sugerencia: escribe $a = da_1$ donde $(a_1, n) = 1$ y $d = (a, n)$. Puedes dividir en 4 casos segun $d = 1, p, q$ o pq. Para el primer caso usa el teorema de Euler. Para el segundo caso demuestra que $A \equiv B \pmod{q} \Longrightarrow pA \equiv pB \pmod{pq}$. De aqui sigue que $p^{t+1} \equiv p \pmod{n}$. Luego aplica el teorema de Euler para demostrar que $a_1^{t+1} \equiv a_1 \pmod{n}$.)
   (b) **Terminologia:** un entero positivo n es “libre de cuadrado” (*square-free*, en ingles) si no es divisible por ningun cuadrado $m^2 > 1$. Definición equivalente: en la factorización prima de n cada primo aparece con multiplicidad 1. Por ejemplo, 100 no es libre de cuadrado (porque 4 lo divide) pero $102 = 2 \cdot 3 \cdot 17$ lo es. Demuestra que las dos definiciones son equivalentes.
   (c) Demuestra que si n es libre de cuadrado entonces $a^{t+1} \equiv a \pmod{n}$, donde $t = \phi(n)$.
   (Sugerencia: escribe $a = da_1$ donde $(a_1, n) = 1$ y $d = (a, n) = p_1 p_2 \ldots p_k$.)
   (d) * (Reto, opcional, no se como hacerlo). Encuentra la generalización del teorema de Euler para n y a general.

2. Sean $a, b, n \in \mathbb{Z}$, $n > 1$. Demuestra los siguientes incisos:
   (a) La congruencia $ax \equiv b \pmod{n}$ tiene solución si y solo si $(a, n) | b$.
   (b) Si $(a, n) | b$, la congruencia $ax \equiv b \pmod{n}$ tiene exactamente (a, n) soluciones distintas $\pmod{n}$.

3. (El “Teorema Chino de los Residuos”.) Sean $m_1, \ldots, m_k$ enteros > 1 tales que $(m_i, m_j) = 1$ si $i \neq j$.
   (a) Demuestra que para todos enteros $b_1, \ldots, b_k$ existe un entero x, único módulo $m_1 m_2 \cdots m_k$, tal que $x \equiv b_i \pmod{m_i}$, $1 \leq i \leq k$.
   (Sugerencia: Sea $n = m_1 m_2 \cdots m_k$, $n_i = n/m_i$. Demuestra que existe un x_i tal que $n_i x_i \equiv b_i \pmod{m_i}$. Toma $x = \sum_i n_i x_i$. No se te olvide la unicidad.)
   (b) * (Opcional). Formular y demostrar un resultado similar acerca de las soluciones de un sistema de congruencias de la forma $a_i x \equiv b_i \pmod{m_i}$, $1 \leq i \leq k$.

4. Sea n un entero > 1, sean $d_1, d_2, \ldots, d_r$ sus divisores positivos y $p_1, p_2, \ldots, p_s$ sus divisores primos.
   (a) Demuestra que $n = \phi(d_1) + \phi(d_2) + \ldots + \phi(d_r)$.
   Por ejemplo: $15 = \phi(15) + \phi(5) + \phi(3) + \phi(1) = 8 + 4 + 2 + 1$.
   (b) Demuestra que $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$.
   Por ejemplo: $8 = \phi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$.

5. * (Opcional). Un entero positivo se llama *perfecto* si es igual a la suma de sus divisores positivos menores que el. Por ejemplo, $6 = 3 + 2 + 1$ es perfecto.
   (a) Verfique que 28 y 496 son perfectos.
   (b) Demuestra que un número par es perfecto si y solo si es de la forma $2^{p-1}(2^p - 1)$, donde p y $2^p - 1$ son primos. (Nota: aun no se sabe si existe un número perfecto impar).
   (c) Demuestra que 2,096,128 no es perfecto pero 33,550,336 lo es.