Algebra Superior, 21.10.99

Tarea num. 10

Para entregar el 26 de oct. 99

1. (a) Sea p un primo. Demuestra que $\binom{p}{k} \equiv 0 \pmod{p}$, para todo $0 < k < p$.
   (b) Concluye de (a) que
   $$(a+b)^p \equiv a^p + b^p \pmod{p},$$
   para todo $a, b \in \mathbb{N}$, y mas general,
   $$(a_1 + a_2 + \ldots + a_n)^p \equiv a_1^p + a_2^p + \ldots + a_n^p \pmod{p},$$
   para todo $a_1, a_2, \ldots, a_n \in \mathbb{N}$.
   (Sugerencia: usar el binomio de Newton).
   (c) Usa (b) para dar una demostración que $n^p \equiv n$ para todo entero n (el "Pequeño Teorema de Fermat").

2. Demostrar que si p es un primo entonces $(p-1)! \equiv -1 \pmod{p}$.

   (Sugerencia: demuestra que se puede arreglar los $p-3$ resíduos $2, 3, \ldots, p-2$ en $(p-3)/2$ pares $\{x, y\}$ tal que $xy \equiv 1 \pmod{p}$. Para eso vas a tener que demostrar que las únicas soluciónes de $x^2 \equiv 1$ son $x \equiv \pm 1$.)

3. Sea n un entero > 1 y a un entero primo relativo a n.

   (a) Demuestra que existe un entero positivo k tal que $a^k \equiv 1 \pmod{n}$.
   (Sugerencia: en la clase dimos una demostración para el caso de $n = 1000$ y $a = 3$.)
   (b) El mínimo entero positivo e que satisface $a^e \equiv 1 \pmod{n}$ se llama el *orden* de $a \pmod{n}$. Encuentra el orden de 3 modulo 4, 7 y 10.
   (c) Demuestra que si a es de orden e, entonces e divide a todos los $k > 0$ que satisfacen $a^k \equiv 1 \pmod{n}$.
   (Sugerencia: dividir a k entre e con resíduo r y demostrar que $a^r \equiv 1 \pmod{n}$.)

4. (Opcional) Sea p un primo > 2. Un resíduo de orden $p-1$ se llama una raíz primitiva $\pmod{p}$. (Por ejemplo 2 es una raíz primitiva $\pmod{5}$.)

   (a) Encuentra las raízes primitivas $\pmod{11}$.
   (b) (Reto). Demuestra que hay $\phi(p-1)$ raices primitivas $\pmod{p}$.
   (c) Sea g una raíz primitiva $\pmod{p}$. Demuestra que para cualquier a distinto de $0 \pmod{p}$ existe único k, $0 \leq k \leq p-1$, tal que $g^k \equiv a$.

   Llamemos a este k el *indice* de a respeto a $g \pmod{p}$. Notación: $k = \mathrm{ind}_g(a)$.
   (d) Demuestra las siguientes propiedades del indice:
      i. $\mathrm{ind}_g(1) = 0$.
      ii. $\mathrm{ind}_g(ab) = ind_g(a) + ind_g(b)$, para todo a, b distinto de $0 \pmod{p}$.
      iii. $\mathrm{ind}_g(a^k) = k \cdot \mathrm{ind}_g(a)$, para todo a distinto de $0 \pmod{p}$ y $k \in \mathbb{Z}$. (Nota: a^k, para k negativo, denota la inversa de $a^{(-k)}$.)