Tarea núm. 4

Para el viernes 29 de agosto 2008

Algunas definiciones y resultados vistos en clase:

- **Definición**. Un entero $d \neq 0$ *divide* a otro entero a (o es un *divisor* de a) si existe un entero m tal que $a = md$. Notación: $d|a$. El *máximo comun divisor* de dos enteros m, n se denota por (m, n).
- **Definición**. Un entero p es primo si (1) $p > 1$ (2) sus únicos divisores positivos son 1 y p.
- **Teorema**. Todo entero $n > 1$ es el producto de primos, de manera única (salvo el orden de los factores).
- **Teorema**. Hay una infinidad de primos.
- **Definición**. Dos enteros a, b son *congruentes modulo* n, donde n es un entero > 1, si $n|a-b$. Notación: $a \equiv b \mod n$. La clase de congruencia modulo n de un entero es el conjunto $[a] = \{b \in \mathbb{Z} | a \equiv b \mod n\}$. El conjunto de las clases de congruencia mod n se denota por $\mathbb{Z}_n$ y consiste en los n elementos $[0], [1], \ldots, [n-1]$.
- **Definición**. Se define en $\mathbb{Z}_n$ el producto y la suma mediante $[a][b] = [ab]$, $[a] + [b] = [a + b]$. (Se verifica que estas operaciones estan bien definidas, i.e. no dependen de los representantes de las clases de congruencia que se toma).
- **Definición**. Dados dos elementos $[a], [b] \in \mathbb{Z}_n$, se dice que $[b]$ es el recíproco de $[a]$ si $[a][b] = [1]$ (mismo que $ab \equiv 1 \mod n$). El conjunto de clases de congruencia $[a] \in \mathbb{Z}_n$ que tienen un recíproco ("invertibles") se denota por $\mathbb{Z}_n^*$. El número de elementos (=cardinalidad) de $\mathbb{Z}_n^*$ se denota por $\phi(n)$ (la "función de Euler").

Problemas

1. Demuestra el siguiente teorema:
   Teorema. Para todo $a, n \in \mathbb{Z}$, donde $n > 1$, las siguientes 3 condiciones so equivalentes:
   a) $[a] \in \mathbb{Z}_n$ tiene un recíproco, i.e. existe un $[b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$.
   b) $(a, n) = 1$ (a y n son primos relativos).
   c) Existe un par de enteros x, y tal que $ax + ny = 1$.

   Sugerencia: basta demostrar que $(a) \Longrightarrow (b) \Longrightarrow (c) \Longrightarrow (a)$. Para $(a) \Longrightarrow (b)$, la relación $ab \equiv 1 \mod n$ implica que $ab + kn = 1$ para algun k, así que todo d que divide a a y n divide a 1. Para $(b) \Longrightarrow (c)$, si $(a, n) = 1$ puedes suponer que $0 < a < n$ y usas inducción sobre a. Divides n entre a y te da $n = ka + r$ con $0 < r < a$ y $(n, a) = (r, a) = 1$. Usando la inducción, $ax_1 + ry_1 = 1$ para algunos x_1, y_1. Ahora usas esto para resolver la ecuación $ax + ny = 1$. $(c) \Longrightarrow (a)$ es muy fácil.

2. Calcula $\phi(p^k)$ para p primo y $k > 0$. (Por ejemplo, hemos visto en clase que $\phi(p) = p - 1$.)

3. Si $n, m > 1$ y $(n, m) = 1$ entonces $\phi(mn) = \phi(m)\phi(n)$.

   Sugerencia: estableces una biyección $f : \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Para cada clase de congruencia $[x] \in \mathbb{Z}_{mn}^*$ defines $f([x]) = (c_1, c_2)$ donde c_1 es la clase de congruencia de x mod m y c_2 es la clase de congruencia de x mod n. Tienes que verificar primero que f está *bien definida*, o sea que $c_1 \in \mathbb{Z}_m^*$ y $c_2 \in \mathbb{Z}_n^*$ y que $f([x]) = f([y])$ si $x \equiv y \mod mn$. Luego demuestras que f es *inyectiva* y *sobre*. Tambien tienes que usar el hecho que para dos conjuntos finitos A, B, $\#(A \times B) = (\#A) \cdot (\#B)$.

4. Sea $n = p_1^{\alpha_1} p_2^{\alpha_1} p_2 \cdots p_m^{\alpha_m}$ la descomposición de un entero $n > 1$ en producto de primos, donde $p_1, \ldots, p_m$ son primos distintos. Demuestra que
$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$
   Sugerencia: usar los dos problemas anteriores.