Tarea núm. 4

Para el jueves 18 feb 2010

Algunas definiciones y resultados vistos en clase:

- **Definición**. Sean $a, b, n \in \mathbb{Z}$, $n > 1$. Se dice que b es un *recíproco* de a módulo n si $ab \equiv 1 \bmod n$.
- **Teorema** (visto en clase pero no demostrado todavía). Un entero a tiene recíproco módulo n si y solo si a y n son primos relativos.
- **Teorema**. Todo entero > 1 es un producto de primos.
- **Teorema**. Existe una infinidad de números primos.
  Demostración (de Euclides): si $p_1, p_2, \ldots, p_k$ son primos entonces todo factor primo p de $N := p_1 p_2 \cdots p_k + 1$ es distinto de $p_1, p_2, \ldots, p_k$. Para ver esto, basta ver que $N \equiv 0 \bmod p$, mientras $N \equiv 1 \bmod$ cualquera de los p_i.

Problemas

1. Sea $n \in \mathbb{Z}$, $n > 1$. Sean $A, B \subset \mathbb{Z}$ dos clases de congruencia módulo n y sean $a \in A$, $b \in B$. Demuestra que las siguienetes condiciones son equivalentes: (a) $A \cap B \neq \emptyset$; (b) $A = B$; (c) $a \equiv b \bmod n$.

   Nota: basta demostrar que $a \Longrightarrow b$, $b \Longrightarrow c$, y $c \Longrightarrow a$ (o cualquier otro ciclo de implicaciones).

2. Sea $n \in \mathbb{Z}$, $n > 1$. Demuestra que $[0], [1], \ldots, [n-1]$ es una lista completa, sin repeticiones, de todas las clases de congruencia módulo n. Concluye que $\mathbb{Z}_n$ (el conjunto de las clases de congruencia módulo n, ver las definiciones en la tarea pasada) tiene n elementos.

3. Sea $n \in \mathbb{Z}$, $n > 1$. Sean $a, b \in \mathbb{Z}$ tal que b es un recíproco de a módulo n. Demuestra:
   a) a es un recíproco de b módulo n.
   b) Para todo $b' \in \mathbb{Z}$ tal que $b' \equiv b \bmod n$, tambien b' es un recíproco de a mod n.
   c) Si b' es un recíproco de a mod n entonces $b' \equiv b \bmod n$.
   d) Concluye de los incisos anteriores que el recíproco de una clase de congruencia modulo n es un concepto bien definido, y en caso que existe tal recíproco, es único.
   e) Usando la tabla de multiplicación módulo 12, decide cuales de las clases de congruencia módulo 12 tienen recíproco, y encuentra su recíproco.

4. *a*) Demuestra: existe una infinidad de primos de la forma $4k + 3$.

   Sugerencia: se puede adaptar a este caso la demostración de Euclides (vista en clase) para la infinitud de los primos. Demuestra que si $p_1, p_2, \ldots, p_k$ es una lista de primos, cada uno de ellos $\equiv 3 \bmod 4$, entonces todo factor primo de $N := 4p_1 p_2 \cdots p_k - 1$ es distinto de $p_1, p_2, \ldots, p_k$, y que alguno de estos factores primos de N debe ser $\equiv 3 \bmod 4$. Para el último, demuestra que el producto de números $\equiv 1 \bmod 4$ es del mismo tipo.
   b) Usa esta deomstración para producir 4 primos de la forma $4k + 3$, empezando con el primo $p_1 = 3$.
   c) (Opcional). Reto: demuestra que existe una infinidad de primos de la forma $4k + 1$.

   Sugerencia: dada una lista $p_1, p_2, \ldots, p_k$ de primos de la forma $4k + 1$, define $P = p_1 p_2 \cdots p_k$ y considera el número $N := 4P^2 + 1$. Ahora viene la parte dificil: demostrar que todo primo p que divide a $4P^2 + 1$ es de la forma $4k + 1$. Empezamos: $p | 4P^2 + 1$ implica $4P^2 + 1 \equiv 0 \bmod p$, o $Q^2 \equiv -1 \bmod p$, donde $Q = 2P$. Ahora elevamos ambos lados a la potencia $(p-1)/2$ y obtenemos $Q^{p-1} \equiv (-1)^{(p-1)/2}$ mpd p. Más tarde en el curso aprendemos que si un primo p no divide a un entero Q entonces $Q^{p-1} \equiv 1 \bmod p$ (el "pequeño teorema de Fermat"). Así que $(p-1)/2$ es par y p es de la forma $4k + 1$.

   Nota: estos son dos casos muy particulares de un teorema (nada fácil, demostrado por Dirichlet en 1837) que afirma que si a y b son dos enteros positivos que son *primos relativos*, entonces existen una infinidad de primos de la forma $ak + b$.