Examen parcial de Matemática Discreta 2

IMERL/FIng/UdelaR

23 de setiembre de 2019

1. (a) Definir número primo.
   (b) Probar que si $p > 2$ es primo, entonces es de la forma $4k+1$ o $4k-1$, para algún $k \in \mathbb{Z}$.
   (c) Probar que existen infinitos primos de la forma $4k-1$.
2. (a) Enunciar la Igualdad de Bezout.
   (b) Sean a, b y c enteros con $(a, b) \neq (0, 0)$. Probar que la ecuación diofántica
   $$ax + by = c$$
   tiene solución si y solo si $\mathrm{mcd}(a, b) \mid c$.
   (c) Una mujer tiene una caja con manzanas. Haciendo grupos de 3 sobran 2 y haciendo grupos de 4 sobran 3. Hallar el número de manzanas que contiene la caja sabiendo que están entre 100 y 110.
3. (a) i. Definir la función φ de Euler.
   ii. Enunciar el Teorema de Euler.
   iii. Enunciar el Teorema chino del resto.
   (b) Probar que para todo par de naturales m, n coprimos, se cumple $\varphi(mn) = \varphi(m)\varphi(n)$
   (c) Calcular 70^{151} módulo 252.

Solución

1. (a) Ver notas (Definición 1.2.2).
   (b) Si p es primo mayor que 2, p es impar. Todo número entero puede escribirse de manera única de alguna de las siguientes formas: $4k$, $4k+1$, $4k+2$, $4k+3$. Como todo número de la forma $4k$ o $4k+2$ es par, entonces p debe escribirse como $4k+1$ o $4k-1 (= 4k+3)$
   (c) Primero hay que notar que si dos enteros son de la forma $4k+1$ su producto también lo es. Supongamos que hay una cantidad finita de primos de la forma $4k-1$, sea $\{p_1, \ldots, p_n\}$ el conjunto de dichos primos. Si consideramos el entero $4(p_1 \ldots p_n) - 1$, es claro que es

un elemento de la forma $4k-1$. Si hacemos la descomposición en factores primos, por lo primero que observamos, es claro que en su descomposición tiene que aparecer algún primo de la forma $4k-1$. Dicho primo no puede ser ninguno de los primos del conjunto $\{p_1,\ldots,p_n\}$, lo que es absurdo.

2. (a) Ver notas (Teorema 1.2.8).
   (b) Ver notas (Teorema 1.5.3).
   (c) Sea x el número de manzanas. La primer condición nos dice que $x = 3a+2$ y la segunda condición que $x = 4b+3$, por lo tanto debemos resolver la ecuación diofántica:

$$3a - 4b = 1$$

Es fácil ver que $(-1,-1)$ es una solución particular de dicha ecuación, de lo que se deduce que la ecuación tiene como solución general al conjunto $\{(-1-4k,-1-3k) : k \in \mathbb{Z}\}$. Usando lo anterior la solución del problema tiene que verificar $100 \leq 4(-1-3k)+3 \leq 110$ con $k \in \mathbb{Z}$. Por lo tanto la solución es $x = 107$.

3. (a) i. Ver notas (Definición 2.6.1).
   ii. Ver notas (Teorema 2.6.5).
   iii. Ver notas (Teorema 2.5.1).
   (b) Ver notas (Teorema 2.6.3).
   (c) Para calcular $70^{151} \pmod{252}$ debemos calcular la solución del sistema

$$\begin{cases} x & \equiv 70^{151} \pmod{28} \\ x & \equiv 70^{151} \pmod{9} \end{cases}$$

Como $70^2 \equiv 0 \pmod{28}$, claramente la primer ecuación es equivalente a $x \equiv 0 \pmod{28}$. Como $\mathrm{mcd}(70,9) = 1$ y $\varphi(9) = 6$, para la segunda ecuación podemos aplicar el Teorema de Euler a la segunda ecuación de la siguiente forma $x \equiv 70^{151} \equiv 70^{6\times 25+1} \equiv 70^1 \equiv 7 \pmod{9}$. Por lo tanto el problema queda reducido a resolver el siguiente sistema

$$\begin{cases} x & \equiv 0 \pmod{28} \\ x & \equiv 7 \pmod{9} \end{cases}$$

Utilizando el Teorema chino del resto llegamos a que $70^{151} \equiv 196 \pmod{252}$.