Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Curso 2011
Lunes 13 de Febrero de 2012

EXAMEN DE MATEMÁTICA DISCRETA 2

Nombre	C.I.	No. de prueba ....

Duración: 4:00 horas. Sin material y sin calculadora.
Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

Ejercicio 1.

(a) Probar que el siguiente sistema de congruencias no posee solución:

$$\begin{cases} x \equiv 25 \pmod{49} \\ x \equiv 13 \pmod{21} \\ x \equiv 17 \pmod{27} \end{cases}$$

(b) Hallar $a \in \{0, 1, \cdots, 20\}$ para que el siguiente sistema de congruencias posea solución:

$$\begin{cases} x \equiv 25 \pmod{49} \\ x \equiv a \pmod{21} \\ x \equiv 17 \pmod{27} \end{cases}$$

(c) Hallar el resto de dividir 5^{44} entre 1323.
(Sugerencia: Utilice que $1323 = 27 \cdot 49$)

Ejercicio 2. En este ejercicio p será un número primo impar.

(a) Enunciar el Teorema de Lagrange para grupos finitos. (No es necesario demostrar el teorema).

(b) Probar que todo grupo de orden p es cíclico.

(c) Sea G un grupo con neutro e, G_1 y G_2 dos subgrupos de G con orden p y $G_1 \neq G_2$. Hallar $G_1 \cap G_2$.

(d) Consideramos el grupo $\mathbb{Z}_p \times \mathbb{Z}_p$ con la suma coordenada a coordenada. Calcule cuántos subgrupos de G tienen orden p.

Ejercicio 3. Sean p y q dos primos distintos y $n = pq$.

(a) Probar que $\varphi(p) = p - 1$ y que $\varphi(n) = (p-1)(q-1)$. En caso de utilizar propiedades de la función φ, éstas deberán ser demostradas.

(b) Si $p = 13$ y $q = 53$ ($n = 13 \times 53 = 689$), calcule la cantidad de enteros e tal que $(689, e)$ es una clave válida de encriptado con el sistema RSA.

(c) Probar que 2 es raíz primitiva módulo 13 y módulo 53.

(d) Determine si existe algún valor entero e, tal que con la clave $(689, e)$, la función de encriptado $E : \mathbb{Z}_{689} \to \mathbb{Z}_{689}$ verifica $E(4) = 105 \mod 689$.
(Sugerencia: Teorema del Resto chino)