

EXAMEN DE MATEMÁTICA DISCRETA 2

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

Duración: 3:30 hs. Sin material y sin calculadora.

Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

Ejercicio 1.

- A. Enuncie (y no demuestre) la identidad de Bezout.
- B. Demuestre que si $a, b, c \in \mathbb{Z}$ con $\text{mcd}(a, b) = 1$ y $a|bc$, entonces $a|c$.
- C. Hallar todos los $a, b \in \mathbb{N}$ tales que $a > b$, $a|7b$ y $\text{mcm}(a, b) = 245$.
- D. En un campamento 23 acampantes van a cargar la leña para el asadito. Se encuentran 63 atados de leña con igual cantidad de leños cada uno. Además, encuentran sueltos 7 leños. Si cada acampante no puede cargar más de 50 leños cada uno, y logran repartirse los leños equitativamente, ¿cuántos leños había en cada atado?

Ejercicio 2.

- A. Hallar todos los $x \in \mathbb{Z}$ tales que
$$\begin{cases} x \equiv 8 \pmod{31} \\ x \equiv 11 \pmod{17} \end{cases}$$
- B. Sean p y q dos primos distintos y $n = pq$. Sea $e \in \mathbb{N}$ tal que $\text{mcd}(e, \varphi(n)) = 1$ y $E : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ la función de encriptado utilizada en el sistema RSA con clave (n, e) ; es decir $E(x) = x^e \pmod{n}$.
Probar que si $ed \equiv 1 \pmod{\varphi(n)}$, entonces la función $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dada por $D(y) = y^d \pmod{n}$ descrypta.
- C. Sean $p = 17$, $q = 31$ y $n = pq$ y $e = 107$. Si la clave para RSA es (n, e) ,
 - (i) Hallar la función D de descryptado.
 - (ii) Si E es la función de encriptado y $E(x) = 250$, hallar x (puede resultar útil saber que $255 = 15 \times 17$ y $248 = 8 \times 31$).

Ejercicio 3.

- A. Enuncie (y no demuestre) el Teorema de Lagrange.
- B. Deduzca que si G es un grupo finito con neutro e y $g \in G$, entonces $g^{|G|} = e$.
- C. Pruebe que si $f : G_1 \rightarrow G_2$ es un homomorfismo de grupos finitos, y $g \in G_1$, entonces $o(f(g)) | \text{mcd}(|G_1|, |G_2|)$ (todas las propiedades que se utilicen sobre homomorfismos, deben ser probadas).
- D. Hallar todos los homomorfismos $f : \mathbb{Z}_2 \rightarrow U(8)$.
- E. Hallar p sabiendo que p es primo, y existe un homomorfismo no trivial $f : \mathbb{Z}_{51} \rightarrow \mathbb{Z}_p$ tal que $f(\overline{17}) = \bar{0}$.