



Examen - Matemática Discreta 2

27 de julio de 2026

No. de Examen

Nombre y Apellido

Cédula de Identidad

Firma

Puntajes (para uso exclusivo del equipo docente)

E1(A)	E1(B)	E1(C)	E1(D)	E2(A)	E2(B)	E2(C)	E2(D)	E2(E)	E3(A)	E3(B)	E3(C)	E3(D)	E3(E)	Total

EJERCICIO 1.

- (A) Sean m y n enteros positivos tales que $\text{mcd}(m, n) = 1$. Si φ denota la función Phi de Euler, demuestre que

$$\varphi(mn) = \varphi(m) \varphi(n).$$

- (B) Calcular el valor de $\varphi(1950)$.

- (C) Demuestre que $7^{960} \equiv 1 \pmod{1950}$.

- (D) Encuentre el resto de 7^{12} módulo 1950.

Sugerencia: Puede ser de utilidad considerar la descomposición $1950 = 39 \times 50$.



EJERCICIO 2. Dado un grupo $(G, *, e)$, se define su **centro** como el conjunto

$$Z(G) := \{g \in G / g * x = x * g \text{ para todo } x \in G\}.$$

- (A) Demuestre que $Z(G)$ es un subgrupo de G .

- (B) Calcule el centro del grupo $\text{GL}_2(\mathbb{R}) = \{A \in \mathcal{M}_{2 \times 2}(\mathbb{R}) / A \text{ es invertible}\}$.

- (C) Para cada elemento $g \in G$, definimos la función de **conjugación** $\sigma_g: G \rightarrow G$ mediante

$$\sigma_g(x) := g * x * g^{-1}, \text{ para todo } x \in G.$$

Demuestra que σ_g es un automorfismo de G (es decir, un homomorfismo inyectivo de G en sí mismo).

- (D) Si denotamos por $\text{Aut}(G)$ al grupo de automorfismos de G (equipado con la composición y cuyo neutro es el homomorfismo identidad sobre G), considere ahora la función $\Psi: G \rightarrow \text{Aut}(G)$ definida por

$$\Psi(g) := \sigma_g, \text{ para todo } g \in G.$$

Demuestra que Ψ es un homomorfismo de grupos.

- (E) Demuestre que $\text{Ker}(\Psi) = Z(G)$.

EJERCICIO 3.

- (A) Demostrar que $o(26) = 6$ en $U(31)$.
- (B) Hallar la menor raíz primitiva positiva módulo 31.
- (C) Ana y Bernardo acuerdan usar el protocolo Diffie-Hellman para generar una clave común K . Teniendo en cuenta la raíz primitiva hallada en la parte (B), Ana elige $n = 7$, y Bernardo elige $m = 5$. Calcular el mensaje que le envía Ana a Bernardo, y el que le envía Bernardo a Ana, según este protocolo, para que ambos puedan generar la clave común.
- (D) Calcular la clave común K , según Diffie-Hellman, que ambos acuerdan.
- (E) A cada letra del abecedario se le asigna un valor numérico del 0 al 27 según la siguiente tabla de correspondencia:



A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ana utiliza la función de cifrado $E: \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$ dada por

$$E(x) = x + K,$$

y le envía a Bernardo el siguiente mensaje cifrado con E :

FNWYQZJTNYBGQAPCRZYBNQ

Descifrar el mensaje anterior.

Examen - Matemática Discreta 2

27 de julio de 2026



No. de Examen

Nombre y Apellido

Cédula de Identidad

Firma

Soluciones**EJERCICIO 1.**

- (A) Sean m y n enteros positivos tales que $\text{mcd}(m, n) = 1$. Si φ denota la función Phi de Euler, demuestre que

$$\varphi(mn) = \varphi(m) \varphi(n).$$

Solución: Ver teórico.

- (B) Calcular el valor de $\varphi(1950)$.

Solución: La descomposición en producto de potencias de primos de 1950 es

$$1950 = 2 \cdot 3 \cdot 5^2 \cdot 13.$$

Como los números 2, 3, 5^2 y 13 son coprimos dos a dos, por la propiedad multiplicativa de la función φ se tiene que

$$\varphi(1950) = \varphi(2) \varphi(3) \varphi(5^2) \varphi(13) = 1 \cdot 2 \cdot (25 - 5) \cdot 12 = 480.$$

- (C) Demuestre que $7^{960} \equiv 1 \pmod{1950}$.

Solución: Primero, note que $960 = 2 \cdot 480$. Por otro lado, como 7 es coprimo con 1950, se tiene por el Teorema de Fermat-Euler que

$$7^{480} = 7^{\varphi(1950)} \equiv 1 \pmod{1950}.$$

Luego, por propiedades de la congruencia modular, al elevar al cuadro tenemos

$$7^{960} = (7^{480})^2 \equiv 1 \pmod{1950}.$$

(D) Encuentre el resto de 7^{12} módulo 1950.

Sugerencia: Puede ser de utilidad considerar la descomposición $1950 = 39 \times 50$.

Solución: Sea x dicho resto. Como $1950 = 39 \cdot 50$, y 39 y 50 son coprimos, calcular la congruencia $x \equiv 7^{12} \pmod{1950}$ es equivalente a resolver el sistema

$$\begin{cases} x \equiv 7^{12} \pmod{39}, \\ x \equiv 7^{12} \pmod{50}, \end{cases}$$

el cual tiene solución única módulo 1950 (el valor de x) por el Teorema Chino del Resto. Pasamos ahora a reducir 7^{12} módulo 39 y módulo 50:

$$\begin{aligned} 7^{12} &= (7^2)^6 = 49^6 \equiv 10^6 = 100^3 \equiv 22^3 = 2^3 \cdot 11^3 = 88 \cdot 121 \equiv 10 \cdot 4 = 40 \equiv 1 \pmod{39}, \\ 7^{12} &= 49^6 \equiv (-1)^6 = 1 \pmod{50}. \end{aligned}$$

Luego, el sistema anterior es

$$\begin{cases} x \equiv 1 \pmod{39}, \\ x \equiv 1 \pmod{50}, \end{cases}$$

cuya solución claramente es $x = 1$. Por lo tanto, el resto de 7^{12} módulo 1950 es 1.

EJERCICIO 2. Dado un grupo $(G, *, e)$, se define su **centro** como el conjunto

$$Z(G) := \{g \in G / g * x = x * g \text{ para todo } x \in G\}.$$

(A) Demuestre que $Z(G)$ es un subgrupo de G .

Solución: Claramente, $Z(G) \neq \emptyset$ ya que $e \in Z(G)$. Ahora, verifiquemos que $Z(G)$ es cerrado bajo la operación del grupo y bajo inversos. Sean $g, h \in Z(G)$. Luego, para todo $x \in G$, se tiene lo siguiente:

$$\begin{aligned} (g * h) * x &= g * (h * x) && \text{(propiedad asociativa)} \\ &= g * (x * h) && (h \in Z(G)) \\ &= (g * x) * h && \text{(propiedad asociativa)} \\ &= (x * g) * h && (g \in Z(G)) \\ &= x * (g * h) && \text{(propiedad asociativa),} \\ g^{-1} * x &= g^{-1} * (x^{-1})^{-1} = (x^{-1} * g)^{-1} && \text{(propiedades de los inversos)} \\ &= (g * x^{-1})^{-1} && (g \in Z(G)) \\ &= (x^{-1})^{-1} * g^{-1} = x * g^{-1} && \text{(propiedades de los inversos).} \end{aligned}$$

Por lo tanto, $g * h, g^{-1} \in Z(G)$.



(B) Calcule el centro del grupo $GL_2(\mathbb{R}) = \{A \in M_{2 \times 2}(\mathbb{R}) / A \text{ es invertible}\}$.

Solución: Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(GL_2(\mathbb{R}))$. Luego, en particular para $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$, se tiene que

$$\begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}.$$

Entonces,

$$a+b=a, \quad c+d=a+c \text{ y } d=b+d,$$

de donde $b=0$ y $a=d$, y así $A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix}$.

Por otro lado, para $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$, se tiene

$$\begin{pmatrix} a & a \\ c & a+c \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} = \begin{pmatrix} a+c & a \\ c & a \end{pmatrix}.$$

Entonces, $a = a+c$, de donde $c=0$. Por lo tanto, $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, con $a \neq 0$ ya que $A \in GL_2(\mathbb{R})$. Tenemos entonces que el centro de $GL_2(\mathbb{R})$ viene dado por el subgrupo de matrices escalares no nulas:

$$Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \text{ y } a \neq 0 \right\}.$$

(C) Para cada elemento $g \in G$, definimos la función de **conjugación** $\sigma_g: G \rightarrow G$ mediante

$$\sigma_g(x) := g * x * g^{-1}, \text{ para todo } x \in G.$$

Demuestra que σ_g es un automorfismo de G (es decir, un homomorfismo injectivo de G en sí mismo).

Solución: Veamos primero que σ_g es un homomorfismo para cada $g \in G$. Dados $x_1, x_2 \in G$, se tiene lo siguiente:

$$\begin{aligned} \sigma_g(x_1 * x_2) &= g * (x_1 * x_2) * g^{-1} = (g * x_1) * (x_2 * g^{-1}) && \text{(propiedad asociativa)} \\ &= (g * x_1) * e * (x_2 * g^{-1}) && \text{(propiedad del neutro)} \\ &= (g * x_1) * (g^{-1} * g) * (x_2 * g^{-1}) && \text{(propiedad del inverso)} \\ &= (g * x_1 * g^{-1}) * (g * x_2 * g^{-1}) && \text{(propiedad asociativa)} \\ &= \sigma_g(x_1) * \sigma_g(x_2). \end{aligned}$$



Para concluir que σ_g es un automorfismo, damos su inverso. Podemos notar que dicho inverso viene dado por $\sigma_{g^{-1}}$. En efecto, para cada $x \in G$, se tiene que:

$$\begin{aligned}\sigma_{g^{-1}} \circ \sigma_g(x) &= \sigma_{g^{-1}}(g * x * g^{-1}) = g^{-1} * (g * x * g^{-1}) * g = (g^{-1} * g) * x * (g^{-1} * g) \\ &= e * x * e = x.\end{aligned}$$

Luego, $\sigma_{g^{-1}} \circ \sigma_g = \text{id}_G$. De manera similar, $\sigma_g \circ \sigma_{g^{-1}} = \text{id}_G$.

- (D) Si denotamos por $\text{Aut}(G)$ al grupo de automorfismos de G (equipado con la composición y cuyo neutro es el homomorfismo identidad sobre G), considere ahora la función $\Psi: G \rightarrow \text{Aut}(G)$ definida por

$$\Psi(g) := \sigma_g, \text{ para todo } g \in G.$$

Demuestra que Ψ es un homomorfismo de grupos.

Solución: Dados $g, h \in G$, tenemos demostrar que $\Psi(g * h) = \Psi(g) \circ \Psi(h)$. Como debemos verificar una igualdad entre homomorfismos, veamos que valen lo mismo al evaluar en un elemento arbitrario $x \in G$:

$$\begin{aligned}\Psi(g * h)(x) &= \sigma_{g * h}(x) = (g * h) * x * (g * h)^{-1} \\ &= (g * h) * x * (h^{-1} * g^{-1}) && \text{(propiedad de los inversos)} \\ &= g * (h * x * h^{-1}) * g^{-1} && \text{(propiedad asociativa)} \\ &= g * (\sigma_h(x)) * g^{-1} = \sigma_g(\sigma_h(x)) \\ &= \sigma_g \circ \sigma_h(x) = \Psi(g) \circ \Psi(h)(x).\end{aligned}$$

Por lo tanto, $\Psi(g * h) = \Psi(g) \circ \Psi(h)$.

- (E) Demuestre que $\text{Ker}(\Psi) = Z(G)$.

Solución: Sea $g \in \text{Ker}(\Psi)$. Luego, $\Psi(g)$ es el neutro del grupo $\text{Aut}(G)$, es decir, $\Psi(g) = \text{id}_G$. Luego, para todo $x \in G$, se tiene que

$$g * x * g^{-1} = \sigma_g(x) = \Psi(g)(x) = \text{id}_G(x) = x.$$

Al multiplicar la igualdad $g * x * g^{-1}$ por g a la derecha, obtenemos

$$g * x = (g * x) * e = (g * x) * (g^{-1} * g) = (g * x * g^{-1}) * g = x * g.$$

Entonces, como $g * x = x * g$ para todo $x \in G$, se tiene que $g \in Z(G)$.



Ahora, sea $g \in Z(G)$. Luego, $g * x = x * g$ para todo $x \in G$. Por el argumento anterior, $g * x = x * g$ es equivalente a $g * x * g^{-1} = x$, donde $g * x * g^{-1} = \Psi(g)(x)$. Al ser $x \in G$ arbitrario, se tiene que $\Psi(g) = \text{id}_G$, es decir, $g \in \text{Ker}(\Psi)$.

EJERCICIO 3.

(A) Demostrar que $o(26) = 6$ en $U(31)$.

Solución: Al ser 31 primo, note que $U(31) = \{1, 2, 3, \dots, 29, 30\}$. Como $|U(31)| = \varphi(31) = 30$, el orden de 26 es un divisor de 30 por el Teorema de Lagrange. Luego, $o(26) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$. Claramente, $o(26) \neq 1$. Por otro lado, tenemos las siguientes congruencias:

$$\begin{aligned} 26 &\equiv -5 \pmod{31} \\ 26^2 &\equiv 25 \equiv -6 \pmod{31} \\ 26^3 &= 26^2 \cdot 26 \equiv (-6) \cdot (-5) = 30 \equiv (-1) \pmod{31}, \\ 26^5 &= 26^3 \cdot 26^2 \equiv (-1) \cdot (-6) = 6 \pmod{31}, \\ 26^6 &= 26^3 \cdot 26^3 \equiv (-1) \cdot (-1) = 1 \pmod{31}. \end{aligned}$$

Por lo tanto, $o(26) = 6$.

(B) Hallar la menor raíz primitiva positiva módulo 31.

Solución: Claramente 1 no puede ser raíz primitiva módulo 31. También se puede notar rápidamente que 2 no es raíz primitiva módulo 31, ya que

$$2^5 = 32 \equiv 1 \pmod{31}.$$

Probemos ahora con 3. Por un lado, $\varphi(31) = 30 = 2 \cdot 3 \cdot 5$. Entonces, por un resultado visto en el teórico, para que 3 sea raíz primitiva módulo 31, debe cumplirse que

$$3^{\varphi(31)/5} \not\equiv 1 \pmod{31}, \quad 3^{\varphi(31)/3} \not\equiv 1 \pmod{31} \quad \text{y} \quad 3^{\varphi(31)/2} \not\equiv 1 \pmod{31}.$$

Verifiquemos esas congruencias en el orden sugerido:

$$\begin{aligned} 3^{\varphi(31)/5} &= 3^{30/5} = 3^6 = (3^3)^2 = 27^2 \equiv (-4)^2 = 16 \not\equiv 1 \pmod{31}, \\ 3^{\varphi(31)/3} &= 3^{10} = 3^6 \cdot 3^3 \equiv 16 \cdot (-4) \cdot 3 = 32 \cdot (-6) \equiv 1 \cdot (-6) \equiv 25 \pmod{31}, \\ 3^{\varphi(31)/2} &= 3^{15} = 3^{10} \cdot 3^3 \cdot 3^2 \equiv (-6) \cdot (-4) \cdot 9 = 24 \cdot 9 \equiv (-7) \cdot 9 = (-21) \cdot 3 \equiv 10 \cdot 3 = 30 \not\equiv 1 \pmod{31}. \end{aligned}$$

Por lo tanto, 3 es menor raíz primitiva positiva módulo 31.



- (C) Ana y Bernardo acuerdan usar el protocolo Diffie-Hellman para generar una clave común K . Teniendo en cuenta la raíz primitiva hallada en la parte (B), Ana elige $n = 7$, y Bernardo elige $m = 5$. Calcular el mensaje que le envía Ana a Bernardo, y el que le envía Bernardo a Ana, según este protocolo, para que ambos puedan generar la clave común.

Solución: Según el protocolo Diffie-Hellman, Ana le envía a Bernardo el mensaje (g, p, A) , donde g es una raíz primitiva módulo p , y $A \equiv g^n \pmod{p}$, donde n es el entero privado de Ana. En nuestro caso, $p = 31$ y $g = 3$ de la parte anterior, y $n = 7$. Luego,

$$A = 3^7 = 3^3 \cdot 3^3 \cdot 3 \equiv (-4) \cdot (-4) \cdot 3 = 16 \cdot 3 = 48 \equiv 17 \pmod{31}.$$

Por lo tanto, Ana envía el mensaje $(3, 31, 17)$.

Al recibir Bernardo dicho mensaje, él le envía a Ana el mensaje $B \equiv g^m$, donde m es su entero privado. En nuestro caso, $m = 5$. Luego,

$$B = 3^5 = 3^3 \cdot 3^2 \equiv (-4) \cdot 9 = -36 = -5 \equiv 26 \pmod{31}.$$

- (D) Calcular la clave común K , según Diffie-Hellman, que ambos acuerdan.

Solución: Según Diffie-Hellman, la clave viene dada por $K \equiv g^{mn}$. Teniendo en cuenta la parte (A) y los resultados anteriores, conviene hacer el cálculo de K de la siguiente manera:

$$K = g^{mn} = (g^m)^n = B^n = 26^7 = 26^6 \cdot 26 \equiv 1 \cdot 26 = 26 \pmod{31},$$

ya que $\phi(26) = 6$. Por lo tanto, el valor de la clave de cifrado es $K = 26$.



- (E) A cada letra del abecedario se le asigna un valor numérico del 0 al 27 según la siguiente tabla de correspondencia:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Ana utiliza la función de cifrado $E: \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$ dada por

$$E(x) = x + K,$$

y le envía a Bernardo el siguiente mensaje cifrado con E :

FNWYQZJTNYBGQAPCRZYBNQ

Descifrar el mensaje anterior.

Solución: Debemos usar la función de descifrado, es decir, la inversa de E . Como $E(x) = x + K = x + 26$, la función de descifrado $D: \mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$ viene dada por

$$D(y) = y - K = y - 26 = y + 2.$$

Pasamos a descifrar el mensaje letra por letra:



$D(F)$	$=$	$D(5) = 5 + 2 = 7$	$=$	H
$D(N)$	$=$	$D(13) = 13 + 2 = 15$	$=$	O
$D(W)$	$=$	$D(23) = 23 + 2 = 25$	$=$	Y
$D(Y)$	$=$	$D(25) = 25 + 2 = 27$	$=$	-
$D(Q)$	$=$	$D(17) = 17 + 2 = 19$	$=$	S
$D(Z)$	$=$	$D(26) = 26 + 2 = 28 = 0$	$=$	A
$D(J)$	$=$	$D(9) = 9 + 2 = 11$	$=$	L
$D(T)$	$=$	$D(20) = 20 + 2 = 22$	$=$	V
$D(N)$	$=$	...	$=$	O
$D(Y)$	$=$	...	$=$	-
$D(B)$	$=$	$D(1) = 1 + 2 = 3$	$=$	D
$D(G)$	$=$	$D(6) = 6 + 2 = 8$	$=$	I
$D(Q)$	$=$	...	$=$	S
$D(A)$	$=$	$D(0) = 0 + 2 = 2$	$=$	C
$D(P)$	$=$	$D(16) = 16 + 2 = 18$	$=$	R
$D(C)$	$=$	$D(2) = 2 + 2 = 4$	$=$	E
$D(R)$	$=$	$D(18) = 18 + 2 = 20$	$=$	T
$D(Z)$	$=$	...	$=$	A
$D(Y)$	$=$	...	$=$	-
$D(B)$	$=$	...	$=$	D
$D(N)$	$=$	...	$=$	O
$D(Q)$	$=$	...	$=$	S

Por lo tanto, el mensaje descifrado es:

HOY_SALVO_DISCRETA_DOS

9/9