

SEGUNDO PARCIAL - 1 DICIEMBRE 2023.

Cédula de identidad	APELLIDO, Nombre	Número de lista

1	2	3	4	5	6

Versión 1.

Ejercicios de respuesta verdadero (V) o falso (F):

(4 puntos, respuesta incorrecta resta 2 puntos)

Ejercicio 1. Usando el método de encriptación Vigenère, con la palabra clave APPA, el mensaje STWENÑTO antes de cifrar es SILENCIO.

Ejercicio 2. Si G es un grupo tal que $o(g) = 2$ (orden de g igual a 2) para todo $g \neq e$ entonces G es abeliano.

Ejercicio 3. Si G es un grupo finito y abeliano, entonces existe un elemento $g \in G$, $g \neq e$, tal que $g = g^{-1}$.

Ejercicio 4. Existe una raíz primitiva módulo $n = 25$.

Ejercicios de respuesta múltiple opción:

(7 puntos, respuesta incorrecta resta 1 punto)

Ejercicio 5. El número de homomorfismos que existen de \mathbb{Z}_9 (los enteros módulo 9) a $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$ (el grupo dihedral de orden 6), es:

- (A) 0. (B) 1. (C) 2. (D) 3.

Ejercicio 6. Determinar exactamente cuáles de los siguientes enteros $\{13, 21, 48, 53\}$ son solución a la ecuación $7^x \equiv 1 \pmod{9}$.

- (A) $x = 21$ y $x = 48$. (C) $x = 21$ y $x = 53$.
(B) $x = 13$ y $x = 48$. (D) $x = 21$, $x = 48$ y $x = 53$.

Preguntas de respuesta por desarrollo escrito:

- **Pregunta 1:** (15 puntos) Si G es un grupo finito y H un subgrupo de G , entonces demostrar que $|H|$ divide a $|G|$.
- **Pregunta 2:** (15 puntos)
 - 1) (5 puntos) Demostrar que si $f : G \rightarrow H$ es un homomorfismo de grupos entonces su kernel es un subgrupo normal de G .
 - 2) (10 puntos) Demostrar que si N es un subgrupo normal de G entonces:
 - a. G/N es un grupo.
 - b. El mapa $\pi : G \rightarrow G/N$, definido $\pi(g) = gN$, es un homomorfismo sobreyectivo.
 - c. El kernel de π es N .

SEGUNDO PARCIAL - 1 DICIEMBRE 2023 - SOLUCIÓN.

Cédula de identidad	APELLIDO, Nombre	Número de lista

1	2	3	4	5	6
F	V	F	V	D	A

Versión 1.

Ejercicios de respuesta verdadero (V) o falso (F):
(4 puntos, respuesta incorrecta resta 2 puntos)

Ejercicio 1. Usando el método de encriptación Vigenère, con la palabra clave APPA, el mensaje STWENÑTO antes de cifrar es SILENCIO.

Solución: FALSA. La segunda letra no se corresponde con el cifrado de la palabra SILENCIO. Si se cifra la palabra SILENCIO correctamente, con el método propuesto, se obtiene: SX ENRXO.

Ejercicio 2. Si G es un grupo tal que $o(g) = 2$ (orden de g igual a 2) para todo $g \neq e$ entonces G es abeliano.

Solución: VERDADERA. Por hipótesis: $(gh)^2 = e$, para todo $g, h \in G$. Es decir: $ghgh = e$. Multiplicando por h a la derecha a ambos lados de la igualdad, y usando que $h^2 = e$, se obtiene: $ghg = h$. Multiplicando por g a la derecha a ambos lados de la igualdad, y usando que $g^2 = e$, se obtiene: $gh = hg$. Esto vale para cualquier par $g, h \in G$, por lo que se concluye que G es abeliano.

Ejercicio 3. Si G es un grupo finito y abeliano, entonces existe un elemento $g \in G$, $g \neq e$, tal que $g = g^{-1}$.

Solución: FALSA. Un contra-ejemplo es el grupo $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, con la suma usual de clases de equivalencia. Este grupo es finito y abeliano. Sin embargo, ningún elemento $g \neq \bar{0}$ es el inverso de sí mismo. Los inversos de cada elemento son: $(\bar{1})^{-1} = \bar{2}$ y $(\bar{2})^{-1} = \bar{1}$.

Ejercicio 4. Existe una raíz primitiva módulo $n = 25$.

Solución: VERDADERA. Se puede escribir $n = 25 = 5^2$; siendo 5 un primo impar. Por lo tanto, el Teorema 4.1.15 de las notas del curso garantiza la existencia de una raíz primitiva módulo $n = 5^2$.

Ejercicios de respuesta múltiple opción:
(7 puntos, respuesta incorrecta resta 1 punto)

Ejercicio 5. El número de homomorfismos que existen de \mathbb{Z}_9 (los enteros módulo 9) a $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$ (el grupo dihedral de orden 6), es:

- (A) 0. (B) 1. (C) 2. (D) 3.

Solución: Opción (D). Buscamos homomorfismos $f : \mathbb{Z}_9 \rightarrow D_3$. El grupo de salida es cíclico y finito, y un generador es $g = \bar{1}$. Por lo tanto, por la Observación 3.9.10 de las notas del curso, sabemos que tendremos un homomorfismo (distinto) por cada forma de asignar al generador g un elemento $k \in D_3$, tal que: $o(k) | o(g)$. El orden del generador es: $o(g) = o(\bar{1}) = 9$. Por otro lado, el orden de cada uno de los elementos del grupo D_3 , es:

$$o(id) = 1, \quad o(r_1) = 3, \quad o(r_2) = 3, \quad o(s_1) = 2, \quad o(s_2) = 2, \quad o(s_3) = 2.$$

Por lo tanto, los elementos $k \in D_3$, cuyo orden divide a $o(\bar{1}) = 9$, son: id, r_1 y r_2 . Se concluye entonces que existen 3 homomorfismos distintos $f : \mathbb{Z}_9 \rightarrow D_3$. Estos quedan determinados por su valor en el generador, y son, respectivamente: $f_1(\bar{1}) = id$ (homomorfismo trivial), $f_2(\bar{1}) = r_1$ y $f_3(\bar{1}) = r_2$.

Ejercicio 6. Determinar exactamente cuáles de los siguientes enteros $\{13, 21, 48, 53\}$ son solución a la ecuación $7^x \equiv 1 \pmod{9}$.

- (A) $x = 21$ y $x = 48$. (C) $x = 21$ y $x = 53$.
(B) $x = 13$ y $x = 48$. (D) $x = 21, x = 48$ y $x = 53$.

Solución: Opción (A). Recordemos que si $o(g)$ es finito, se cumple: $g^m = e$ si y sólo si $o(g) | m$ (Proposición 3.7.8 de las notas del curso). Como $\text{mcd}(7, 9) = 1$, sabemos que $\bar{7} \in U(9)$. Veamos cuál es el orden de $\bar{7}$ en $U(9)$. Observemos que:

$$7^2 = 49 \equiv 4 \pmod{9}, \quad 7^3 = 7^2 7 \equiv 28 \pmod{9} \equiv 1 \pmod{9}.$$

Por lo tanto: $o(\bar{7}) = 3$ en $U(9)$. Entonces, por la proposición inicial, se cumple: $(\bar{7})^m = \bar{1}$ si y sólo si $3 | m$. Tenemos que $3 | 21$ y $3 | 48$; mientras que 3 no divide a 13 ni a 53. La opción correcta es: $x = 21$ y $x = 48$.

Otra forma de resolver el ejercicio consiste en calcular la potencia para cada exponente $x \in \{12, 21, 48, 53\}$, con la ayuda de Euler. Como $\text{mcd}(7, 9) = 1$, el Teorema de Euler garantiza que: $7^{\varphi(9)} \equiv 1 \pmod{9}$. Es decir: $7^6 \equiv 1 \pmod{9}$. Por lo tanto:

$$7^{13} = (7^6)^2 7^1 \equiv 7 \pmod{9}; \quad 7^{21} = (7^6)^3 7^3 \equiv 7^3 \pmod{9} \equiv 1 \pmod{9};$$

$$7^{48} = (7^6)^8 \equiv 1 \pmod{9};$$

$$7^{53} = (7^6)^8 7^5 \equiv 7^5 \pmod{9} \equiv 7^3 7^2 \pmod{9} \equiv 7^2 \pmod{9} \equiv 4 \pmod{9}.$$

Preguntas de respuesta por desarrollo escrito:

- **Pregunta 1:** (15 puntos) Si G es un grupo finito y H un subgrupo de G , entonces demostrar que $|H|$ divide a $|G|$.

Respuesta: Ver notas Pereira-Qureshi-Rama Teorema 3.8.1 (Teorema de Lagrange).

- **Pregunta 2:** (15 puntos)

- 1) (5 puntos) Demostrar que si $f : G \rightarrow H$ es un homomorfismo de grupos entonces su kernel es un subgrupo normal de G .

Respuesta: Ya sabemos que $\ker(f)$ es un subgrupo de G (cerrado por producto, inverso y contiene a la unidad). Vamos a probar que es un subgrupo normal. Esto equivale a probar que $g\ker(f)g^{-1} \subseteq \ker(f)$, para todo $g \in G$. Es decir, probar que: $ghg^{-1} \in \ker(f)$, para todo $h \in \ker(f)$, y todo $g \in G$. Sean entonces $h \in \ker(f)$ y $g \in G$ cualesquiera. Como f es un homomorfismo, se cumple:

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(h)f(g)^{-1} = f(g)e_Hf(g)^{-1} = e_H.$$

Por lo tanto, por definición de núcleo, se concluye que $ghg^{-1} \in \ker(f)$.

- 2) (10 puntos) Demostrar que si N es un subgrupo normal de G entonces:

a. G/N es un grupo. **Respuesta:**

- En el conjunto cociente G/N , definimos el siguiente producto: $(aN)(bN) = (ab)N$.
- Veamos primero que este producto está "bien definido", es decir, que no depende del representante de cada clase lateral. Supongamos que $aN = a'N$ y $bN = b'N$. Queremos probar que $(ab)N = (a'b')N$.

Por definición de la relación de equivalencia, existen $n, m \in N$, tales que: $a = a'n$ y $b = b'm$. Por lo tanto: $ab = a'nb'm$. Por otro lado, como N es subgrupo normal, se cumple: $Nb' = b'N$. Esto último implica que para el elemento $n \in N$, existe $t \in N$, tal que: $nb' = b't$. Juntando ambas igualdades, se obtiene: $ab = a'nb'm = a'b'tm$. Como $tm \in N$, y por definición de la relación de equivalencia, concluimos que $abN = a'b'N$.

- Veamos ahora que G/N con este producto forma un grupo. Es decir: se cumple la propiedad asociativa, existencia de neutro, y existencia de inverso.
 - ◇ La unidad es eN , ya que se verifica: $(aN)(eN) = (ae)N = aN$.
 - ◇ El inverso de aN es: $(aN)^{-1} = a^{-1}N$. En efecto: $(aN)(a^{-1}N) = (aa^{-1})N = eN$.
 - ◇ Finalmente, usando la propiedad asociativa de la operación del grupo G , se tiene:

$$(aNbN)(cN) = ((ab)N)(cN) = ((ab)c)N = (a(bc))N = (aN)((bc)N) = (aN)(bNcN).$$

- b. El mapa $\pi : G \rightarrow G/N$, definido $\pi(g) = gN$, es un homomorfismo sobreyectivo.

Respuesta: Claramente es sobreyectivo porque para cada $aN \in G/N$ tomo $a \in G$ y cumple $\pi(a) = aN$. Además es un homomorfismo dado que: $\pi(ab) = (ab)N = aNbN = \pi(a)\pi(b)$.

- c. El kernel de π es N .

Respuesta:

$$\ker(\pi) = \{g \in G : \pi(g) = eN\} = \{g \in G : gN = N\} = \{g \in G : g \in N\} = N.$$