Matemáticas Discretas II — I Semestre 2023

Parcial # 1 — Profesor: *Rodrigo De Castro K.*

Nombre: _____ *Calificación:* 32/60

No se permite el uso de celulares. No se permite compartir calculadoras.

1. *(12 puntos)* Algoritmo de los Productos y Cuadrados Iterados presentado en clase:

Algoritmo para hallar $b^e \bmod m$
ENTRADA: e, b, m (números naturales)
Expresar e en base 2, $e = (a_k \dots a_1 a_0)_2$
Inicializar
  u := 1
  Potencia := b mod m
Para i desde 0 hasta k,
  REPETIR:
    Si $a_i = 1$ entonces
    u := (u × Potencia) mod m
    Potencia := $(\text{Potencia})^2 \bmod m$
SALIDA: $u \equiv b^e \bmod m$, donde $u < m$.

128 32 16 8 1
1 0 1 1 1 0 0 1

(i) Expresar el número 185 en base 2: 10111001.

(ii) Ejecutar el anterior algoritmo en la siguiente tabla para calcular $6^{185} \bmod 124$.

i		u = u × potencia mod 124		Potencia² mod 124
0	1	1 × 6 = 6	6	$(6)^2 = 36$	36
1	0	~	6	$(36)^2 = 1296$	56
2	0	~	6	$(56)^2 = 3136$	36
3	1	6 × 36 = 216	92	$(36)^2 = 1296$	56
4	1	92 × 56 = 5152	68	$(56)^2 = 3136$	36
5	1	68 × 36 = 2448	92	$(36)^2 = 1296$	56
6	0	~	92	$(56)^2 = 3136$	36
7	1	92 × 36 = 3312	88	~	~

Respuesta = 88

6

2. *(6 puntos)* El número de soluciones de la congruencia $28x \equiv 35 \mod 63$ en $\mathbb{Z}_{63}$ es 7.

Dichas soluciones son: 8, 17, 26, 35, 44, 53, 62

Escribir el procedimiento utilizado para resolver este problema:

$\text{mcd}(28,63) = 7 \rightarrow$ Hay 7 soluciones en $\mathbb{Z}_{63}$

$28x \equiv 35 \mod 63$

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
24, 25, 26, 35, 44, 53, 62

26 — 1,1

50 40 0,94

1,56

8

3. *(10 puntos)* Para los siguientes afirmaciones responder VERDADERO V ✓ o FALSO F ✓.

(i) V ✓ F — En un grupo todo elemento es inverso de algún otro elemento.

X (ii) V — F ✓ Si un grupo G tiene un número par de elementos entonces, según el Teorema de Lagrange, todo subgrupo de G tiene también un número par de elementos.

$f(a \circ b) = f(a)$ y Biyect

(iii) V — F X El grupo $(\mathbb{Z}_p, +)$ es cíclico si y solamente si p es primo.

(iv) V X F — Existen enteros positivos m, n tales que $(\mathbb{Z}_m, +)$ es isomorfo con $(\mathbb{Z}_n^*, \cdot)$.

(v) V — F X Un grupo de orden primo tiene solamente un subgrupo.

0

4. *(7 puntos)* Si la función $f : \mathbb{Z}_{12}^* \to \mathbb{Z}_{10}$ es un homomorfismo entre los grupos $(\mathbb{Z}_{12}^*, \cdot)$ y $(\mathbb{Z}_{10}, +)$ tal que $f(5) = 5$, hallar los siguientes valores:

$f(1) =$ 1. $f(2) =$ 2. $f(7) =$ 8.

$(\mathbb{Z}_7, +)$

{5, 7, 9, 11}

5. *(8 puntos)* Considere las afirmaciones (A) y (B):

(A) Todos los subgrupos del grupo $(\mathbb{Z}_{10}, +)$ son cíclicos.

(B) Todos los subgrupos del grupo $(\mathbb{Z}_{10}^*, \cdot)$ son cíclicos.

cíclico

$(\mathbb{Z}_{10}, +)$

{1, 2, 5, 10}

- {0}
- {0, 5}
- {0, 2, 4, 6, 8}
- $\{\mathbb{Z}_{10}\}$

Elegir una de las siguientes respuestas marcando con ✓.

0

1) ___ Las afirmaciones (A) y (B) son ambas verdaderas. •

2) ___ Las afirmaciones (A) y (B) son ambas falsas.

X 3) ✓ (A) es verdadera y (B) es falsa. •

4) ___ (A) es falsa y (B) es verdadera.

4

6. *(4 puntos)*
El orden de 3 en el grupo $(\mathbb{Z}, +)$ es ∞.
El orden de 3 en el grupo $(\mathbb{Z}_7, +)$ es 7.
El orden de 3 en el grupo $(\mathbb{Z}_8^*, \cdot)$ es 2.

7. *(3 puntos)* Si G es un grupo con 240 elementos, y H y K son subgrupos de G tales que $|H| = 8$ y $|K| = 10$, entonces el número posible de elementos que hay en $H \cap K$ es ~~8~~ 1, 2
(Escribir todos los posibles valores).

8. *(10 puntos)* Sea G un grupo y $f : G \to G$ la función definida por $f(a) = a^{-1}$, para todo $a \in G$.
(i) Demostrar que si G es abeliano, entonces f es un homomorfismo.

Si G es abeliano → f: G → G es un homomorfismo

$f(a) = a^{-1} \quad \forall a, b \in G$
$f(b) = b^{-1}$

$f(a) \circ f(b) \overset{\text{HIPOTESIS}}{=} f(b) \circ f(a)$
$a^{-1} b^{-1} = b^{-1} a^{-1}$

→ Si es abeliano ya que es un grupo conmutativo, por ende es un homomorfismo. □

Hay que demostrar $f(a \cdot b) = f(a) \cdot f(b)$
No lo hizo!

(ii) Demostrar que si f es un homorfosmismo, entonces G es abeliano.

Si f es un homomorfismo → G es abeliano
Si $f(a \circ b) = f(a) \circ f(b) \quad \forall a, b \in G$
$f(a \circ b) = a^{-1} \circ b^{-1}$
$a^{-1} \circ b^{-1} = a^{-1} \circ b^{-1}$
$(ab)^{-1} = (ab)^{-1}$

→ Ya que f es un homomorfismo entonces, G es un grupo Abeliano conmutativo. □

↓ ESPACIO PARA OPERACIONES ↓

Esto no demuestra nada :(= :(