Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería
Instituto de Matemática y Estadística

EXAMEN - 23 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):
(Cada ejercicio vale: 5 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 1. Sean a, m, k y n enteros positivos. Si $m \equiv k \pmod{\varphi(n)}$ entonces $a^m \equiv a^k \pmod{n}$.

Ejercicio 2. Sea G un grupo tal que $|G| = 45$. Existe $g \in G$, $g \neq e$, tal que: $g = g^{-1}$.

Ejercicio 3. El criptosistema de clave pública RSA es muy útil porque una vez que conocemos el valor $\varphi(n)$ no existe un algoritmo que encuentre la función de descifrado (que es equivalente a encontrar el inverso de e módulo $\varphi(n)$).

Ejercicio 4. El conjunto de números enteros que al dividirlos simultáneamente por 2 y 3 me dan resto 1 es exactamente el conjunto $\{x \in \mathbb{Z} : x = 1 + 6k, k \in \mathbb{Z}\}$.

Ejercicios de respuesta múltiple opción:
(Cada ejercicio vale: 15 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 5. Sean a y b enteros positivos. Considere las siguientes proposiciones:

(i) Si m es un número primo divisor de a que no divide a b y n un número primo divisor de b que no divide a a, entonces $\mathrm{mcd}(\frac{a}{m}, b) = \mathrm{mcd}(a, \frac{b}{n})$.

(ii) Si m es un divisor de a que no divide a b y n un divisor de b que no divide a a, entonces $\mathrm{mcd}(\frac{a}{m}, b) = \mathrm{mcd}(a, \frac{b}{n})$.

Entonces elija la opción correcta:

(A) sólo (i) es verdadera

(B) sólo (ii) es verdadera

(C) las dos son verdaderas

(D) las dos son falsas

Ejercicio 6. El resto de dividir 7^{77} entre 200 es:

(A) 0.

(B) 1.

(C) 7.

(D) Ninguna de las anteriores.

Preguntas de respuesta por desarrollo escrito:

- **Pregunta 1:** (25 puntos)

  Sean $n, a \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, n) = 1$, entonces demostrar que $a^{\varphi(n)} \equiv 1 \pmod{n}$. (No se puede demostrar como corolario del teorema de Lagrange).

- **Pregunta 2:** (25 puntos)

  a) Defina homomorfismo de grupos y orden de un elemento.

  b) Pruebe que si G y H son grupos finitos, $g \in G$ y $\varphi : G \to H$ es un homomorfismo de grupos entonces el orden de $\varphi(g)$ divide al orden de g.

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

Matemática Discreta 2

Examen - 23 diciembre 2023 - Solución.

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

Versión 1.

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

(Cada ejercicio vale: 5 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 1. Falso. Un contraejemplo se obtiene con: $n = 8$, $a = 2$, $m = 1$ y $k = 5$. Notar que si se agrega la hipótesis $\mathrm{mcd}(a, n) = 1$, entonces la propiedad es cierta.

Ejercicio 2. Falso. Supongamos por absurdo que la afirmación es verdadera. La condición $g = g^{-1}$ equivale a $g^2 = e$. Como además $g \neq e$, se concluye que $o(g) = 2$. Por lo tanto, el subgrupo generado por g es un subgrupo de G de orden 2. Sin embargo, por el teorema de Lagrange, el orden de cualquier subgrupo de G debe dividir a $|G| = 45$.

Ejercicio 3. Falso. Si conocemos $\varphi(n)$, entonces podemos calcular eficientemente la clave privada d resolviendo la siguiente ecuación diofántica: $ex + \varphi(n)y = 1$ (la clave pública e siempre es conocida). Esta diofántica la podemos resolver eficientemente usando el Algoritmo de Euclides Extendido. Si denotamos una solución particular mediante (x_0, y_0), tenemos que: $d \equiv x_0 \pmod{\varphi(n)}$.

Ejercicio 4. Verdadero. Cararacterizar un entero $x \in \mathbb{Z}$ con esas dos condiciones simultáneas, es equivalente a pedir que verifique: $x \equiv 1 \pmod 2$ y $x \equiv 1 \pmod 3$. Dado que $\mathrm{mcd}(2, 3) = 1$, podemos usar el Teorema Chino del Resto para afirmar que esto equivale a que se cumpla: $x \equiv 1 \pmod 6$.

Ejercicios de respuesta múltiple opción:

(Cada ejercicio vale: 15 puntos, respuesta incorrecta resta 3 puntos.)

Ejercicio 5. Opción correcta: A.

(i) Si m es un primo que no divide a b entonces $\mathrm{mcd}(m, b) = 1$. Por consiguiente: $\mathrm{mcd}(\frac{a}{m}, b) = \mathrm{mcd}(a, b)$. De forma análoga, si n es un primo que no divide a a, entonces: $\mathrm{mcd}(a, \frac{b}{n}) = \mathrm{mcd}(a, b)$. Otra forma de verlo es considerar la factorización en primos de a y b. Por hipótesis, estas son de la forma:

$$a = m^{a_0} p_1^{a_1} \dots p_k^{a_k} n^0, \quad b = m^0 p_1^{b_1} \dots p_k^{b_k} n^{b_0}, \quad p_i \neq m, n, \quad a_0, b_0 \geq 1.$$

Por lo tanto:

$$\mcd\left(\frac{a}{m}, b\right) = p_1^{\text{mín}(a_1,b_1)} \dots p_k^{\text{mín}(a_k,b_k)} = \mcd\left(a, \frac{b}{n}\right).$$

(ii) Si quitamos la hipótesis de que m y n son primos, la afirmación deja de ser válida. Por ejemplo, si tomamos $a = 16$, $b = 18$, $m = 4$ y $n = 6$, vemos que:

$$4|16, \quad 4 \nmid 18, \quad 6|18, \quad 6 \nmid 16, \quad \mcd(\frac{16}{4}, 18) = \mcd(4, 18) = 2 \quad \mcd(16, \frac{18}{6}) = \mcd(16, 3) = 1.$$

Por lo tanto, en este caso no se cumple la afirmación (ii).

Ejercicio 6. Opción correcta: C.

Queremos hallar $r \equiv 7^{77} \pmod{200}$ con $0 \leq r < 200$. La factorización en primos del módulo es: $200 = 2^3 5^2$. Como $\mcd(7, 200) = 1$, y $\varphi(200) = 80$, por el Teorema de Euler: $7^{80} \equiv 1 \pmod{200}$. Es decir: $7^3 7^{77} \equiv 1 \pmod{200}$. Entonces, basta con calcular el inverso de 7^3 módulo 200 para despejar el valor buscado. Notar que este inverso existe pues $\mcd(7^3, 200) = 1$. Por definición, este inverso es cualquier $x \in \mathbb{Z}$, tal que: $7^3 x \equiv 1 \pmod{200}$. Como $7^3 = 49 \times 7 = 343$, esto equivale a resolver la siguiente ecuación diofántica: $343x - 200s = 1$. Para resolverla utilizamos el algoritmo de Euclides extendido:

$$\begin{cases} 343 = 200 \cdot 1 + 143 \\ 200 = 143 \cdot 1 + 57 \\ 143 = 57 \cdot 2 + 29 \\ 57 = 29 \cdot 1 + 28 \\ 29 = 28 \cdot 1 + 1 \end{cases}.$$

Despejando los restos, obtenemos: $7 \cdot 343 - 12 \cdot 200 = 1$. Por lo tanto, las soluciones son de la forma: $x \equiv 7 \pmod{200}$. En particular $(7^3)^{-1} \equiv 7 \pmod{200}$. Recordando la ecuación obtenida al inicio: $7^3 7^{77} \equiv 1 \pmod{200}$, multiplicamos a ambos lados por el inverso de 7^3, y obtenemos: $7^{77} \equiv 7 \pmod{200}$.

Preguntas de respuesta por desarrollo escrito:

- **Pregunta 1:** (25 puntos) Ver notas de teórico: Teorema 2.6.5 (Teorema de Euler).
- **Pregunta 2:** (25 puntos)

  a) Ver notas de teórico: Definición 3.9.1 y Definición 3.7.6.

  b) Ver notas de teórico: Proposición 3.9.3. Reproducimos la prueba a continuación.
  Sabemos que: $g^{o(g)} = e_G$. Aplicando φ de ambos lados, y usando que es un morfismo, se obtiene: $\varphi(g^{o(g)}) = \varphi(e_G) = e_H$. Usando nuevamente que φ es un morfismo, podemos intercambiar la potencia con el morfismo: $e_H = \varphi(g^{o(g)}) = \varphi(g)^{o(g)}$. Esto implica que $o(\varphi(g))|o(g)$.
  Para la última afirmación, utilizamos la siguiente propiedad del orden de un elemento $h \in H$ (Proposición 3.7.8, numeral 4): Si $h^k = e_H$, entonces $o(h)|k$.