

# Examen de Matemática Discreta 2

IMERL/FIng/UdelaR

13 de febrero de 2020

Duración: 3 horas

Número de Examen	Cédula	Nombre y Apellido

## Ejercicios de desarrollo.

- Sean  $a, b \in \mathbb{Z}$ , probar que la ecuación diofántica  $ax + by = c$  tiene solución si y solo si  $\text{mcd}(a, b) | c$ .
  - Hallar el menor par  $x > 199$  que cumpla  $2x + 3 \equiv 4 \pmod{11}$  y  $3x + 4 \equiv 3 \pmod{7}$ .
- Definir la función  $\phi$  de Euler.
  - Enunciar y demostrar el Teorema de Euler
- Dado un número natural  $n$ , definir raíz primitiva módulo  $n$ .
  - Probar que si  $p$  es primo, entonces existen raíces primitivas módulo  $p$ . Enunciar claramente todo resultado a utilizar.
  - Dar un ejemplo de un número natural  $n$  que no tenga raíces primitivas.

## Ejercicio de múltiple opción.

- Sea  $0 \leq m < 99$  tal que  $m \equiv 5^{2579} \pmod{99}$ . Indicar cual de las opciones es correcta:

**A.**  $m = 56$ .      **B.**  $m = 20$ .      **C.**  $m = 86$ .      **D.**  $m = 5$ .

Solución

- Ver notas, Teorema 1.5.3. (página 17)

(b) El número  $x > 199$  tiene que verificar el sistema

$$\begin{cases} x \equiv 0 \pmod{2} \\ 2x + 3 \equiv 4 \pmod{11} \\ 3x + 4 \equiv 3 \pmod{7} \end{cases}$$

Como  $x$  es par, podemos hacer el cambio de variable  $2z = x$  y resolver el sistema

$$\begin{cases} 4z + 3 \equiv 4 \pmod{11} \\ 6z + 4 \equiv 3 \pmod{7} \end{cases}$$

Como  $4 \equiv 3^{-1} \pmod{11}$  y  $6 \equiv -1 \pmod{7}$ , resolver el sistema anterior es equivalente al siguiente

$$\begin{cases} z \equiv 3 \pmod{11} \\ z \equiv 1 \pmod{7} \end{cases}$$

Por la primer ecuación  $z = 3 + 11a$  y por la segunda  $z = 1 + 7b$ . Por lo tanto, para resolver el sistema podemos resolver la ecuación diofántica

$$11a - 7b = -2$$

Como  $(-4, -6)$  es una solución particular de la ecuación diofántica, la solución general resulta  $(-4 - 7k, -6 - 11k)$ . Tenemos  $x = 2z = 2(3 + 11a) = 2(3 + 11(-4 - 7k)) = -82 - 154k$  y por otro lado es el mínimo  $x > 199$ . Por lo tanto  $x = 226$ .

2. (a) Ver notas, Definición 2.6.1. (página 37).  
(b) Ver notas, Teorema 2.6.5. (página 40).
3. (a) Ver notas, Definición 4.1.1. (página 60).  
(b) Ver notas, Teorema 4.1.10. (página 63).  
(c)  $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ . Como  $o(1) = 1$  y  $o(3) = o(5) = o(7) = 2$  el grupo  $\mathbb{Z}_8^*$  no es cíclico y por lo tanto no hay raíces primitivas para  $n = 8$ .
4. Opción correcta: **B**