

| Nro de prueba | Cédula | Apellido y nombre |
|---------------|--------|-------------------|
|               |        |                   |

### Ejercicios de múltiple opción

| Ejercicio 1 | Ejercicio 2 |
|-------------|-------------|
|             |             |

#### Ejercicio 1 (10 puntos)

Sean  $n = 319$  y  $e = 19$ . Para los datos anteriores sea la función de descifrado  $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

- A.  $D(y) = y^{42} \pmod{n}$                       B.  $D(y) = y^{59} \pmod{n}$   
C.  $D(y) = y^{84} \pmod{n}$                       D.  $D(y) = y^{67} \pmod{n}$

#### Ejercicio 2 (10 puntos)

Sea  $0 \leq m < 325$  tal que  $m \equiv 435^{241} \pmod{325}$ . Indicar cuál de las opciones es correcta:

- A.  $m = 65$ .                                      B.  $m = 110$ .  
C.  $m = 300$ .                                    D.  $m = 175$ .

### Ejercicios de desarrollo

#### Ejercicio 3 (40 puntos)

- a) Dados dos enteros  $m$  y  $n$  tales que  $(m, n) \neq (0, 0)$ , definir el máximo común divisor de  $m$  y  $n$ .  
b) Enunciar y probar el Teorema de Bézout. (Denominado igualdad o identidad de Bézout.)  
c) Probar que la ecuación diofántica  $ax + by = c$  tiene solución si y solo si  $\text{mcd}(a, b) | c$ .  
d) Consideremos la ecuación diofántica  $4x + 80y = 28$ .  
i) Verificar que la ecuación tiene solución.  
ii) Hallar todas sus soluciones.

#### Ejercicio 4 (40 puntos)

- a) Definir:  
i) grupo,  
ii) subgrupo,  
iii) morfismo de grupos.  
b) Enunciar y probar el Teorema de Lagrange.  
c) Hallar el conjunto de los  $m$  tales que existe un morfismo de grupos no trivial  $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_m$

## Solución

### Ejercicio 1 Opción B

### Ejercicio 2 Opción D

- Ejercicio 3**
- a) Ver notas (Definición 1.2.4. página 7).
  - b) Ver notas (Teorema 1.2.8. página 10).
  - c) Ver notas (Teorema 1.5.3. página 18).
  - d)
    - i) Como  $\text{mcd}(4, 80) = 4$  y 4 divide a 28 entonces la ecuación diofántica tiene solución.
    - ii) Primero hallemos una solución particular a la ecuación diofántica. Por ejemplo, si tomamos  $x = 7$  y  $y = 0$  se tiene que  $4 \times 7 + 80 \times 0 = 28$ . Usando la parte b del Teorema 1.5.3. la solución general es de la forma

$$\{(7 + 20k, -k) \mid k \in \mathbb{Z}\}$$

- Ejercicio 4**
- a)
    - i) Ver notas (Definición 3.1.1. página 44).
    - ii) Ver notas (Definición 3.7.1. página 51).
    - iii) Ver notas (Definición 3.9.1. página 56).
  - b) Ver notas (Teorema 3.8.1 página 55).
  - c) Primero hay que notar que para que un morfismo  $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_m$  sea no trivial la imagen por  $f$  del grupo  $\mathbb{Z}_7$  debe verificar  $|\text{Im}(f)| = 7$ . Por lo tanto, usando el Teorema de Lagrange, si 7 no divide a  $m$  no hay ningún morfismo no trivial entre  $\mathbb{Z}_7$  y  $\mathbb{Z}_m$ . Ahora si 7 divide a  $m$ , supongamos que  $m = 7k$  con  $k \in \mathbb{Z}$ , tenemos que el elemento  $\bar{k} \in \mathbb{Z}_m$  tiene orden 7, por lo tanto podemos definir  $f_m : \mathbb{Z}_7 \rightarrow \mathbb{Z}_m$  a partir de  $f(1) = \bar{k}$  utilizando la Proposición 3.9.9. de las notas.