

TEST: Tets de la lecc. 2 de Aritmética Entera y Modular

1.- Indica cuál de las siguientes afirmaciones es correcta:

- ☐ La relación de congruencia es una relación de equivalencia en \mathbb{Z} .
- ☐ La relación de congruencia cumple las propiedades reflexiva, antisimétrica y transitiva.
- ☐ La relación de congruencia es compatible con la suma en \mathbb{Z} pero no con el producto.
- ☐ La relación de congruencia cumple las propiedades reflexiva, simétrica, antisimétrica y transitiva.

2.- Indica cuál de las siguientes afirmaciones es correcta:

- ☐ 53 es congruente con 17 módulo 9.
- ☐ 53 es congruente con 17 módulo 5.
- ☐ 53 es congruente con 17 módulo 7.
- ☐ 53 es congruente con 17 módulo 10.

3.- Indica cuál de las siguientes afirmaciones es correcta:

- ☐ El inverso de [18] en el conjunto de los enteros congruentes módulo 29 es [22].
- ☐ El inverso de [8] en el conjunto de los enteros congruentes módulo 29 es [11].
- ☐ El inverso de [-21] en el conjunto de los enteros congruentes módulo 29 es [18].
- ☐ El inverso de [8] en el conjunto de los enteros congruentes módulo 29 es [10].

4.- Resuelve el siguiente sistema de ecuaciones lineales en el conjunto de los enteros congruentes módulo 11 (\mathbb{Z}_{11}): $[5]x + [9]y = [8]$, $[2]x + [7]y = [3]$. Una vez resuelto indica cuál de las siguientes afirmaciones es cierta:

- ☐ El sistema no tiene solución en \mathbb{Z}_{11} .
- ☐ La solución de este sistema es $x=[6]$, $y=[7]$.
- ☐ El sistema tiene múltiples soluciones.
- ☐ La solución de este sistema es única y es $x=[3]$, $y=[9]$.

5.- Indica cuál de las siguientes afirmaciones es cierta:

- ☐ La función de euler sobre 100 es 50.
- ☐ La función de euler sobre 29 es 23.
- ☐ La función de euler sobre 27 es 3.
- ☐ La función de euler sobre 80 es 32.

6.- Indica cuál de las siguientes afirmaciones es correcta:

- ☐ La función de euler calculada sobre un número primo p es $p+1$.
- ☐ La función de euler calculada sobre un producto de dos números primos p, q es $(p-1)(q-1)$.
- ☐ La función de euler calculada sobre un producto de dos números primos p, q es $(p+1)(q+1)$.
- ☐ La función de euler calculada sobre cualquier número primo es 1.

7.- Deseamos cifrar con el código de clave privada dado en clase (cifrado afín) e identificando las letras minúsculas del alfabeto con el conjunto de los enteros módulo 28 (se incluye el espacio en blanco; a:0, b:1, c:2,..., z:26, espacio_en_blanco:27) la frase: "hola que tal". Indica cuál de las siguientes afirmaciones es cierta, si se ha elegido $r=7$ y $s=4$.

- ☐ La frase cifrada mediante este código antes de identificar cada número con su letra es 122404050006262500210504.
- ☐ La clave r no es válida ya que $\text{mcd}(r, 28)$ ha de ser 1.
- ☐ La clave s no es válida ya que $\text{mcd}(s, 28)$ ha de ser 1.
- ☐ No podemos usar el conjunto de los enteros módulo 28, ya que 28 no es un producto de dos números primos.

8.- Se ha cifrado mediante el criptosistema de clave privada dado en clase e identificando las letras mayúsculas del alfabeto con los enteros módulo 28 (incluyendo el espacio en blanco; A:0, B:1, C:2,..., Z:26, espacio_en_blanco:27) una palabra y el mensaje cifrado ha resultado ser MATF. Si $s=5$ y $r=9$, indica qué afirmación es correcta:

- ☐ La palabra descifrada es HOLA.
- ☐ La palabra descifrada es BIEN.
- ☐ No podemos usar el conjunto de los enteros módulo 28, ya que 28 no es un producto de dos números primos.
- ☐ Las claves no son válidas.

9.- Un cometa tiene una órbita alrededor de la Tierra de 28 años. Si está situado en una posición A y transcurren $3^{40} \cdot 7^{85}$ años, ¿cuántos años faltan para que el cometa vuelva a estar situado, por primera vez, en la posición A?

- ☐ 7 años.
- ☐ 21 años.
- ☐ 25 años.
- ☐ 175 años.

10.- Sean $n=221$ y $t=11$ los parámetros de un sistema RSA, encripta la letra E representada por la cifra 4 e indica cuál de las siguientes afirmaciones es cierta:

- ☐ La función de cifrado es $C([m])=[m]^{221}$.
- ☐ Para obtener la función de descifrado necesito calcular el valor de s que en este caso es 192.
- ☐ Cuando cifremos la letra E con este código obtenemos la clase de 166 en el conjunto Z_{221} .
- ☐ El valor de $t=11$ no cumple las condiciones del sistema RSA.