DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL

Prácticas Lección 1 y 2 MATEMÁTICA DISCRETA Aritmética entera y modular

---

Práctica 1 Calcula desarrollando e indicando el algoritmo que corresponda, razonadamente y con la ayuda de ArtEM, el $\mathrm{mcd}(25, 115)$ y el $\mathrm{mcm}(25, 115)$. Con ayuda del desarrollo realizado obtén dos enteros s y t tales que $\mathrm{mcd}(25, 115) = 25s + 115t$.

Práctica 2 Resuelve, de forma razonada, la siguiente ecuación diofántica y comprueba luego que el resultado es correcto mediante ArtEM:

$$-45x + 32y = 7,\ x, y \in \mathbb{Z}$$

Práctica 3 Un distribuidor de equipos informáticos efectuó un pedido de entre 1000 y 1500 equipos a un fabricante. Éste se los envió en contenedores completos con capacidad para 68 equipos cada uno. El distribuidor los repartió a los diferentes puntos de venta usando furgonetas con capacidad para 20 equipos, y quedando 32 equipos sin repartir en el almacén. ¿Cuántos equipos pidió el distribuidor a la fábrica? Ayúdate de ArtEM para comprobar que tus cálculos han sido efectuados correctamente.

Práctica 4 Lee atentamente la descripción de los algoritmos de la opción números primos de ArtEM y averigua cuáles de los siguientes números son primos y en caso de que no lo sean haz, razonadamente, su descomposición en números primos.

$$123456,\ 9999,\ 363,\ 8861.$$

Práctica 5 Disponemos de dos tipos de ladrillos de 56 y 21 cm para construir una pared de 7 metros. Explica cuáles son las distintas maneras posibles de llevar a cabo este trabajo. Comprueba las operaciones que sean posibles con ArtEM.

Práctica 6 Determina los enteros que verifican: $z \equiv 7 \pmod{11}$, $z \equiv 4 \pmod{17}$. Comprueba los cálculos que sean posibles con ArtEM.

Práctica 7 Resuelve las siguientes cuestiones sin utilizar ArtEM, y luego comprueba los cálculos que sean posibles con ArtEM:

1. Calcular el valor de la función de Euler en 35, $\varphi(35)$.
2. Calcular $[27]^{\varphi(35)}$ en $\mathbb{Z}_{35}$. Obtener el resultado como representante de clase entre 0 y 34.
3. ¿Cuál es el resto de dividir 2^{99} entre 35?
4. Calcular $[27]^3$ en $\mathbb{Z}_{35}$. Obtener el resultado como representante de clase entre 0 y 34.
5. Se sabe que un determinado planeta tarda en completar su órbita alrededor de una cierta estrella 35 años. Si actualmente se encuentra en la posición A y transcurren 27^{99} años, ¿cuántos años más deben transcurrir para que vuelva a encontrarse en la misma posición A?

Práctica 8 Utilizando el alfabeto de ArtEM que identifica las letras minúsculas del alfabeto (a-z) y el espacio en blanco con $\mathbf{Z}_{28}$ y usando el código clásico dado en clase con $r = 5$ y $s = 4$, codifica la siguiente frase utilizando ArTEM: hola mama. Haz tú dicha codificación a mano y de forma razonada. A continuación explica cuál será la función de decodificación para volver al mensaje original y decodifica el mensaje cifrado obtenido a mano. Comprueba el resultado con ArTEM. Razona además si es posible tomar $r = 7$ en este código clásico con el alfabeto utilizado.

Práctica 9 **(a)** Explica las diferencias entre los sistemas criptográficos de clave privada y de clave pública.
(b) Da las dos funciones de codificación y decodificación del sistema RSA, mostrando que son funciones una inversa de la otra. Explica sobre qué propiedad se basa la seguridad del sistema RSA.
(c) Sean $n = 77$ y $t = 7$ los parámetros de un sistema RSA, encripta de forma razonada la letra "I", representada por la cifra 8.
(d) Calcula la función de decodificación y decodifica el mensaje cifrado obtenido en el apartado anterior.
(e) Comprueba tus resultados con ArtEM.

Nota: No olvidéis detallar y justificar correctamente cada pregunta. Una respuesta no justificada se considerará incorrecta. Horas presenciales: 4 *horas*