

DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN E INTELIGENCIA
ARTIFICIAL
(sesión prácticas)

Problemas Lección 1 MATEMÁTICA DISCRETA Aritmética entera y modular

Ejercicio 1 Resuelve razonadamente las siguientes cuestiones:

- (a) Halla la representación en base 2 del número expresado en base decimal 137.
- (b) Halla la representación usual (en base 10) de $(4165)_7$.
- (c) Obtén mediante el algoritmo de Euclides $d = \text{mcd}(56, 34)$, y con la ayuda de los pasos de dicho algoritmo encuentra dos enteros s y t tales que $d = 56s + 34t$.

Ejercicio 2 Resuelve la siguiente ecuación diofántica:

$$28x - 36y = 44, \quad x, y \in \mathbb{Z}.$$

Problemas Lección 2 MATEMÁTICA DISCRETA Aritmética entera y modular

Ejercicio 3 Calcula el inverso de $[33]$ en \mathbb{Z}_{50} . Expresa el resultado con el representante de clase entre 0 y 49.

Ejercicio 4 Resuelve en \mathbb{Z}_7 el siguiente sistema. Expresa la solución con representantes de clase entre 0 y 6.

$$\left. \begin{array}{rcl} x + [5]y & = & [2] \\ [2]x - y & = & [3] \end{array} \right\}$$

Ejercicio 5 Resuelve la siguiente ecuación cuadrática en \mathbb{Z}_{11} .

$$x^2 + [3]x + [4] = 0, \quad x \in \mathbb{Z}_{11}.$$

Expresa el resultado mediante representantes de clase entre 0 y 10.

Ejercicio 6 Usa el teorema de Fermat para calcular el resto de dividir $3^{25} \cdot 7^{68}$ entre 23.

Nota: No olvidéis detallar y justificar correctamente cada pregunta. Una respuesta no justificada se considerará incorrecta. Horas presenciales: 2 horas

ARITMÉTICA ENTERA Y MODULAR

Problemas lección 1

① a) $137 \div 12$

$$\begin{array}{r}
 137 \\
 12 \overline{) 137} \\
 \underline{120} \\
 17 \\
 12 \overline{) 17} \\
 \underline{12} \\
 5 \\
 12 \overline{) 50} \\
 \underline{48} \\
 2 \\
 12 \overline{) 20} \\
 \underline{12} \\
 8 \\
 12 \overline{) 80} \\
 \underline{72} \\
 8 \\
 12 \overline{) 88} \\
 \underline{84} \\
 4 \\
 12 \overline{) 40} \\
 \underline{36} \\
 4 \\
 12 \overline{) 44} \\
 \underline{36} \\
 8 \\
 12 \overline{) 88} \\
 \underline{84} \\
 4 \\
 12 \overline{) 40} \\
 \underline{36} \\
 4 \\
 12 \overline{) 44} \\
 \underline{36} \\
 8 \\
 12 \overline{) 88} \\
 \underline{84} \\
 4
 \end{array}$$

$$137_{10} = 10001001$$

b) $4165_7 = (4 \cdot 7^3 + 1 \cdot 7^2 + 6 \cdot 7^1 + 5 \cdot 7^0)_{10} = 1468_{10}$

c)

$\text{mcd}(56, 34)$

$$a = qb + r$$

$$d = 56s + 34t$$

$$56 = 34 \times 1 + 22 \checkmark$$

$$12 = 10 \times 1 + 2$$

$$34 = 22 \times 1 + 12 \checkmark$$

$$r = a + q(-b)$$

$$22 = 12 \times 1 + 10 \checkmark$$

$$2 = 12 + 10(-1)$$

$$(-1) \cdot (-1) = 1$$

$$12 = 10 \times 1 + 2 \checkmark$$

$$2 = 12 + [22 + 12(-1)](-1) = 12 + 22(-1) + 12(1) = 12(2) + 22(-1)$$

$$10 = 2 \times 5 + 0$$

$$2 = [34 + 22(-1)](-2) + 22(-1) = 34(-2) + 22(3)$$

$$2 = 34(-2) + [56 + 34(-1)](-3) = 34(-2) + 56(-3) + 34(3) = 34(4) + 56(-3)$$

Ec. diofántica $\rightarrow 2 = 56 \underset{\Delta}{(-3)} + 34 \underset{\overline{\Delta}}{(4)}$

$$(2) \text{ da } 28x - 36y = 44, x, y \in \mathbb{Z}$$

$$(1) \text{ med}(28, 36)$$

$$36 = 28 \times 1 + (8) \checkmark$$

$$28 = 8 \times 3 + (4) \checkmark$$

$$8 = 4 \times 2 + 0$$

$$a = qb + r$$

$$28 = 8 \times 3 + 4$$

$$r = a + q(-b)$$

$$4 = 28 + 8(-3)$$

$$4 = 28 + [36 + 28(-1)](-3) = 28 + 36(-3) + 28(3) = 28(4) + 36(-3)$$

\bar{D}

$$28(4) - 36(3)$$

$S \leftarrow$ Identidad de Bézout $\rightarrow T$

$$(1) \text{ ¿Es divisor de } C?$$

$$C/D = 44/4 \Rightarrow SI \Rightarrow \text{luego tiene solución}$$

$$(3) \text{ Sean } \alpha, \beta \text{ enteros}$$

$$A = \alpha D \Rightarrow 28 = \alpha 4 \Rightarrow \alpha = 28/4 = 7$$

$$B = \beta D \Rightarrow 36 = \beta 4 \Rightarrow \beta = 36/4 = 9$$

$$(2) \text{ Solución particular -}$$

$$d = 4$$

$$dn = 44 \mid n = 44/d = 11$$

$$(x_0, y_0) = (44, 33)$$

$$\begin{matrix} 11 & 11 \\ m & n \end{matrix}$$

$$(4) \text{ Solución general}$$

$$X = x_0 + k\beta = 44 + 9(-k)$$

$$y = y_0 - k\alpha = 33 - 7k \Rightarrow y = 33 + 7(-k)$$

$$(5) \text{ comprobación}$$

$$11A - 11B$$

$$x = 44 + 9 = 53$$

$$y = 33 + 7 = 40$$

$$28(53) - 36(40) = 44$$

Problemas lección 2

③ Hallar $[a]^{-1}$ en $\mathbb{Z}/50$ para $a=33$

$a=33$ $n=50$ $\text{med}(a,n) = \text{med}(33,50) = 1 \Rightarrow [33]^{-1}$ en $\mathbb{Z}/50$

$$50 = 33 \times 1 + 17 \checkmark$$

$$33 = 17 \times 1 + 16 \checkmark$$

$$17 = 16 \times 1 + 1 \checkmark$$

$$16 = 1 \times 16 + 0$$

Backout

$$1 = 17 + 16(-1)$$

$$1 = 17 + [33 + 17(-1)](-1) = 17 + 33(-1) + 17(1) = 33(-1) + 17(2)$$

$$1 = 33(-1) + [50 + 33(-1)](2) = 33(-1) + 50(2) + 33(-2) = 33(-3) + 50(2)$$

$$1 = 33(-3) + 50(2)$$

Si lo vemos en $\mathbb{Z}/50$ \nearrow 0 en $\mathbb{Z}/50$

$$[1] = [33](-3) + [50](2)$$

$$[1] = [33](-3)$$

$$[33]^{-1} = [-3] = [50 - 3] = [47]$$

Ejercicio 4

$$\begin{cases} x + [5]y = [2] \\ [2]x - y = [3] \end{cases} \left\{ \begin{array}{l} \text{Resolven en } \mathbb{Z}_7 \text{ y expresen con representantes de clase entre} \\ 0 \text{ y } 6. \end{array} \right.$$

$$\begin{array}{r} [5]x + [25]y = [10] \\ [2]x - y = [3] \\ \hline [7]x + [24]y = [13] \end{array}$$

↓ En \mathbb{Z}_7

$$[7]x + [13]y = [6]$$

$$y = [6][3]^{-1} = [6] \cdot [-2] = [-12] = [7-12] = [-5] = [7-5] = [2]$$

$$\boxed{[3]^{-1}} \text{ mod } (3, 7) \Rightarrow \text{Algoritmo de Euclides}$$

$$7 = 3 \times 2 + 1 \quad \checkmark$$

$$3 = 2 \times 1 + 0$$

Identidad de Bézout

$$\boxed{d = ax + by}$$

$$a = 7, b = 3$$

→ Esto es para cuando
quieras sacar la Ec. Diophantina

$$\boxed{a = qb + r}$$

$$7 = 3 \times 2 + 1$$

$$\boxed{n = a + q(-b)}$$

$$1 = 7 + 3(-2) \Rightarrow [1] = [7] + [3] \cdot [-2]$$

$$[1] = [3] \cdot [-2]$$

$$[3]^{-1} = [-2]$$

Despejar x

$$x + [5]y = [2]$$

$$x + [5] \cdot [2] = [2]$$

$$x + [10] = [2]$$

$$x = [2] - [10] = [-8] = [7-8] = [-1] = [6]$$