Tema 1: Preliminares y Teoría de números

1. Números enteros

- Elemento neutro ⟹ Suma el número 0

  ⟹ Producto el número 1

- Elemento opuesto ⟹ $a + a' = 0$; $a = -a'$

- Elemento inverso ⟹ $a \cdot a' = 1$; $a' = \frac{1}{a}$ si $a \neq 0$

2. Aritmética entera

- División euclídea ⟹ $\begin{array}{l|l} n & m \\ \cline{2-2} r & q \end{array}$ $n = m \cdot q + r$ $0 \leq r < |m|$

¡ojo!

$n = -17$ $m = -3$ ⟹ $\begin{array}{l|l} -17 & -3 \\ \cline{2-2} -2 & 5 \end{array}$

$-17 = (-3) \cdot 5 - 2$

$-17 = (-3) \cdot 5 \underline{-2+3}-3$

Sumar y restar el divisor ⟶ $-17 = (-3) \cdot 5 + 1 - 3$

$-17 = (-3)(5+1) + 1$

$$\boxed{-17 = (-3) \cdot 6 + 1}$$

- Sistemas de numeración posicionales

¡ojo!

$n = 3785$ $b = 7$ (base)

$\begin{array}{l|l} 3785 & 7 \\ \cline{2-2} 28 & 540 \\ 05 & \end{array}$ $\begin{array}{l|l} 540 & 7 \\ \cline{2-2} 50 & 77 \\ 1 & \end{array}$ $\begin{array}{l|l} 77 & 7 \\ \cline{2-2} 0 & 11 \end{array}$ $\begin{array}{l|l} 11 & 7 \\ \cline{2-2} 4 & 1 \end{array}$

Sol. ⇒ $\boxed{3785 = 14015_{(7}}$

- Divisibilidad y números enteros $\Longrightarrow$ $\boxed{m|n \;,\quad n = m \cdot q \quad q \in \mathbb{Z}}$

+ Propiedades de la divisibilidad

$1|n \;;\; (-1)|n$

$n|n \;;\; n|(-n)$

$$\boxed{\begin{array}{l} \text{Si } k|n \text{ y } k|m \text{, ent. } k|n \pm m \\ \text{Si } n|m \text{, ent. } n|k.m \\ \text{Si } k|n \text{ y } k|m \text{, ent. } k|s.n + t.m \end{array}}$$

3. Algoritmo de Euclides

¡OjO!

$m.c.d(70,42) = \boxed{14}$

$\begin{array}{r|l} 70 & 42 \\ \hline 28 & 1 \end{array}$ $\quad$ $\begin{array}{r|l} 42 & 28 \\ \hline 14 & 1 \end{array}$ $\quad$ $\begin{array}{r|l} 28 & 14 \\ \hline 0 & 2 \end{array}$

- Números coprimos $\Longrightarrow$ $\boxed{mcd(n,m) = 1}$
- Identidad de Bézout $\Longrightarrow$ $mcd(n,m) = n.\underline{a} + m.\underline{b}$

¡OjO!

$mcd(136, 26) = \boxed{2}$

$D = d.q + r \Longrightarrow r = D - d.q$

$\begin{array}{r|l} 136 & 26 \\ \hline 6 & 5 \end{array}$

$6 = 136 - 26.5$

$2 = 26 - 6.4$

$\begin{array}{r|l} 26 & 6 \\ \hline 2 & 4 \end{array}$

$2 = 26 - (136 - 26.5).4$

$2 = 26 - 136.4 + 26.20$

$\begin{array}{r|l} 6 & 2 \\ \hline 0 & 3 \end{array}$

$$\boxed{2 = \textcircled{136}.(-4) + \textcircled{26}.21}$$

- Forma matricial

$$\begin{pmatrix} 136 \\ 1 \\ 0 \end{pmatrix} - 5 \begin{pmatrix} 26 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \\ -5 \end{pmatrix} \;, \qquad \begin{pmatrix} 26 \\ 0 \\ 1 \end{pmatrix} - 4 \begin{pmatrix} 6 \\ 1 \\ -5 \end{pmatrix} = \begin{pmatrix} 2 \\ \boxed{-4} \\ \boxed{21} \end{pmatrix} \begin{array}{l} \\ \leftarrow \\ \leftarrow \end{array}$$

$$\boxed{2 = 136.(-4) + 26.21}$$

4. Ecuaciones diofánticas

Def. $\boxed{n \cdot x + m \cdot y = k}$ donde $n, m, k \in \mathbb{Z}$

$x, y \in \mathbb{Z}$

Tiene soluciones si $\overset{d}{\overset{\shortparallel}{\text{mcd}(n,m)}} \mid k$

$X = x_0 + \left(\frac{m}{d}\right) q$, $y = y_0 - \left(\frac{n}{d}\right) q$, $q \in \mathbb{Z}$

¡Ojo!

$14x + 21y = 70$

① $\text{mcd}(14,21) = 7$

$$\begin{array}{l|l} 21 & 14 \\ \hline \boxed{7} & 1 \end{array} \rightarrow 7 = 21 - 14 \cdot 1$$

$$\begin{array}{l|l} 14 & 7 \\ \hline \boxed{0} & 2 \end{array}$$

$7 \mid 70 \Longrightarrow$ tiene soluciones enteras

$70 = 7 \cdot \boxed{10}$

¡multiplicar!

② I. de Bezout $\Rightarrow$ $7 = 21 \cdot 1 - 14 \cdot 1$

$7 \cdot 10 = (-14 \cdot 1 + 21 \cdot 1) 10$; $70 = -14 \cdot 10 + 21 \cdot 10$;

$70 = 14 \cdot \underbrace{(-10)} + 21 \cdot \underbrace{10}$

③ Sols. particulares $\Longrightarrow$ $\boxed{x_0 = -10}$ $\boxed{y_0 = 10}$

¡restar!

④ Sols. generales $\Longrightarrow$

$$\begin{array}{r} 14x + 21y = 70 \\ 14(-10) + 21 \cdot (10) = 70 \\ \hline 14(x+10) + 21(y-10) = 0 \end{array} \quad \ominus$$

Dividir pa el mcd

$2(x+10) + 3(y-10) = 0$

$2(x+10) = -3(y-10)$

$\frac{2(x+10)}{3} = -y + 10$

- Si $k = \frac{x+10}{3}$; $\boxed{x = 3k - 10}$ $k \in \mathbb{Z}$
- $2k = -y + 10$; $\boxed{y = -2k + 10}$

¡Ojo! Sólo soluciones positivos

$150x + 39y = 228$

- $x = 456 - 13k$

$456 - 13k \geq 0$

$456 \geq -13k$

$k \leq \frac{456}{13} \simeq 35'07...$

- $y = -1748 + 50k$

$-1748 + 50k \geq 0$

$50k \geq 1748$

$k \geq \frac{1748}{50} \simeq 34'96...$

$$34'96 \leq k \leq 35'07$$

$$\downarrow$$

$$\boxed{k = 35}$$

$x = 456 - 13 \cdot 35 = \boxed{1}$

$y = -1748 + 50 \cdot 35 = \boxed{2}$

5. Aritmética modular

$a, b, m \in \mathbb{Z}$, $m > 1$ **a** es congruente con **b** módulo **m** si $(a-b)$ es múltiplo de m

$$\boxed{a \equiv b \pmod m}$$

$\rightarrow$ $m \mid a-b$

$\rightarrow$ $a = mk + b$

$\rightarrow$ $[a]_m = [b]_m$

$a \equiv b \pmod m \longrightarrow \begin{array}{l|l} a & m \\ \hline r & \end{array} = \begin{array}{l|l} b & m \\ \hline r & \end{array}$ ¡mismo resto!

→ Propiedades

$$\boxed{\begin{array}{l} + \; a \equiv a \pmod m \\ + \; a \equiv b \pmod m \implies b \equiv a \pmod m \\ + \; a \equiv b \pmod m \;\; y \;\; b \equiv c \pmod m \implies a \equiv c \pmod m \end{array}}$$

→ Simplificar al resto

¡Ojo!

$2 \equiv 6 \pmod 2 \longrightarrow \begin{array}{l|l} 2 & 2 \\ \hline 0 & 1 \end{array} \implies \boxed{2 \equiv 0 \pmod 2}$

$-432 \equiv ? \pmod{200} \longrightarrow \begin{array}{l|l} -432 & 200 \\ \hline 168 & -3 \end{array} \implies \boxed{-432 \equiv 168 \pmod{200}}$

- $a, b, c, d, m \in \mathbb{Z}$ $\quad a \equiv b \pmod{m} \quad c \equiv d \pmod{m}$

  $m > 1$

$$\begin{cases} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$$

- Suma, resta, producto en $\mathbb{Z}_m$

¡Ojo!

- $[35]_{13} \cdot [35]_{13} = [35 . 35]_{13} = [22^2]_{13} = [9^2]_{13} = [81]_{13} = \boxed{[3]_{13}}$

⊛ $\begin{array}{r|l} 81 & 13 \\ \cline{2-2} 78 & 6 \\ \underline{3} & \end{array}$ $\quad \begin{array}{r|l} 35 & 13 \\ \cline{2-2} \underline{22} & 1 \end{array}$ $\quad \begin{array}{r|l} 22 & 13 \\ \cline{2-2} \underline{9} & 1 \end{array}$

- $[795^{25}]_{11} = [3^{25}]_{11} = [3 . 3^{24}]_{11} = [3 . (3^2)^{12}]_{11} = [3\ (-2)^{12}]_{11} =$

⊛ $\begin{array}{r|l} 795 & 11 \\ \cline{2-2} 25 & 72 \\ \underline{3} & \end{array}$

⊛ $3^2 = 9 \equiv -2 \pmod{11}$

⊛ $15 \equiv 4 \pmod{11}$

⊛ $2^4 = 16 \equiv 5 \pmod{11}$

⊛ $25 \equiv 3 \pmod{11}$

$= [3 . (2^4)^3]_{11} = [3 . 5^3]_{11} = [15 . 25]_{11} = [4 . 3]_{11} = [12]_{11} = \boxed{[1]_{11}}$

- Congruencias lineales (resolución de ecs.)

$a, b \in \mathbb{Z}, \quad m > 1$ $\quad \boxed{a . x \equiv b \pmod{m}}$ $\quad (a . x + m . y = b)$

Ec. diofántica ¡!

Si mcd (a, m) divide a b → Ecuación tiene solución

¡**Ojo**! $9x = 12 \ (\text{mod } 15)$

Ec. diofántica $\longrightarrow$ $9x + 15y = 12$

$\text{mcd}(9,15) = 3$ 3 soluciones

$\begin{array}{l|l} 15 & 9 \\ \hline \boxed{6} & 1 \end{array}$ $\begin{array}{l|l} 9 & 6 \\ \hline \boxed{3} & 1 \end{array}$ $\begin{array}{l|l} 6 & 3 \\ \hline \boxed{0} & 2 \end{array}$ $\begin{array}{l|l} 12 & 3 \\ \hline \boxed{0} & 4 \end{array}$

$3 | 12 \longrightarrow \boxed{\text{Tiene solución}}$

$3 = 9 + 6(-1)$ $\quad * \ 6 = 15 + 9(-1)$

$3 = 9 + (15 + 9(-1))(-1)$ $\quad 9 + 9(-1)(-1) = 18 \ ;$ $\begin{array}{l|l} 18 & 9 \\ \hline \boxed{0} & 2 \end{array}$

$3 = 9(2) + 15(-1)$

$\cdot 4 \Rightarrow 12 = 9(8) + 15(-4)$

Sols. particulares: $\boxed{x = 8 \ ; \ y = -4}$

Sols. generales: $x = 8 + \frac{15}{3}k = \boxed{8 + 5k}$

$y = -4 - \frac{9}{3}k = \boxed{-4 - 3k}$

- $[8]_{15} \Rightarrow k = 0$
- $[13]_{15} \Rightarrow k = 1$
- $[3]_{15} \Rightarrow k = -1$

Soluciones

- Inversos modulares

$\boxed{a \cdot x \equiv 1 \ (\text{mod } m)} \Longrightarrow$ Tiene solución si $\text{mcd}(a, m) = 1$

$[x]_m = [a]^{-1}_m$

Formas $\Longrightarrow$ Directamente, Bezout, F. Euler

¡Ojo! $6x \equiv 1 \pmod{17}$

$\text{mcd}(6, 17) = 1 \Longrightarrow$ la clase $[6]_{17}$ tiene inverso

$\begin{array}{r|l} 17 & 6 \\ \cline{2-2} \boxed{5} & 2 \end{array}$ $\begin{array}{r|l} 6 & 5 \\ \cline{2-2} \boxed{1} & 1 \end{array}$ $\begin{array}{r|l} 5 & 1 \\ \cline{2-2} \boxed{0} & 5 \end{array}$

$1 = 6 + 5(-1)$

$1 = 6 + (17 + 6(-2))(-1)$

$1 = 6(\underline{3}) + 17(-1)$

⊛ $5 = 17 + 6(-2)$

⊛ $6 + 6(-2)(-1) = 18$

$\begin{array}{r|l} 18 & 6 \\ \cline{2-2} \boxed{0} & 3 \end{array}$

- $[6]^{-1}_{17} = \boxed{[3]_{17}} \Rightarrow [6]_{17} \cdot [3]_{17} = [1]_{17}$

$\Downarrow$

¡Ojo! $6x + 14 \equiv 2 \mod (17)$

$[6x + 14]_{17} = [2]_{17}$; $[6x]_{17} = [2 - 14]_{17}$; $[6x]_{17} = [-12]_{17}$;

$[6x]_{17} = [5]_{17}$

- Multiplicamos por el inverso de $[6]_{17} \longrightarrow [3]_{17}$

$\cancelto{1}{[3]_{17} [6]_{17}} [x]_{17} = [3]_{17} [5]_{17}$

$\boxed{[x]_{17} = [15]_{17}}$

- Criterios de divisibilidad

$[12473]_3 = [1 + 2 + 4 + 7 + 3]_3 = [1 + 2 + 1 + 1 + 0]_3 = [5]_3 = \boxed{[2]_3}$

12473 no es múltiplo de 3

• Teorema de Euler

Si mcd $(a,m) = 1 \implies a^{\phi(m)} \equiv 1 \pmod{m}$

$$[a^{\phi(m)-1}]_m = [a]_m^{-1}$$

¡Ojo! $\quad 10x \equiv 14 \pmod{24}$

mcd $(10, 24) = 2 \longrightarrow$ tiene solución

$\begin{array}{l|l} 24 & 10 \\ \hline \boxed{4} & 2 \end{array} \quad \begin{array}{l|l} 10 & 4 \\ \hline \boxed{2} & 2 \end{array} \quad \begin{array}{l|l} 4 & 2 \\ \hline \boxed{0} & 2 \end{array} \quad \Bigg\| \quad 2 \mid 14 \quad \begin{array}{l|l} 14 & 2 \\ \hline \boxed{0} & 7 \end{array}$

- Simplificamos la congruencia:

$10x = 14 + 24k \;;\quad 5x = 7 + 12k \implies \boxed{5x \equiv 7 \pmod{12}}$

mcd $(5, 12) = \boxed{1} \longrightarrow$ podemos resolverla utilizando inversos

$\begin{array}{l|l} 12 & 5 \\ \hline \boxed{2} & 2 \end{array} \quad \begin{array}{l|l} 5 & 2 \\ \hline \boxed{1} & 2 \end{array} \quad \begin{array}{l|l} 2 & 1 \\ \hline \boxed{0} & 2 \end{array}$

$[5x]_{12} = [7]_{12} \;;\quad [x]_{12} = [5]_{12}^{-1} \cdot [7]_{12}$

- Euler $\implies \phi(12) = \phi(2^2 \cdot 3) = (2^2 - 2^1)(3^1 - 3^0) = 2 \cdot 2 = \boxed{4}$

$[x]_{12} = [5^{4-1}]_{12} \cdot [7]_{12} = [5^3]_{12} \cdot [7]_{12} = [1 \cdot 5]_{12} \cdot [7]_{12} =$

$= [35]_{12} = [11]_{12}$

$\rightarrow [x_1]_{24} = \boxed{[11]_{12}}$

$\rightarrow [x_2]_{24} = [11 + 12]_{24} = \boxed{[23]_{24}}$

- Sistemas de congruencias lineales

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases} \Longrightarrow \text{Tiene solución si } d \mid a-b$$

$$\text{mcd}(m_1, m_2) = d$$

<u>Solución</u> $\Longrightarrow$ $$x \equiv \frac{b \cdot s \cdot m_1 + a \cdot t \cdot m_2}{d} \mod \left(\frac{m_1 \cdot m_2}{d}\right)$$

¡ojo!

$$\begin{cases} x \equiv 0 \mod 28 \\ x \equiv 16 \mod 100 \end{cases}$$

$\begin{array}{l|l} 100 & 28 \\ \cline{2-2} \boxed{16} & 3 \end{array}$ $\begin{array}{l|l} 28 & 16 \\ \cline{2-2} \boxed{12} & 1 \end{array}$ $\begin{array}{l|l} 16 & 12 \\ \cline{2-2} \boxed{4} & 1 \end{array}$ $\begin{array}{l|l} 12 & 4 \\ \cline{2-2} \boxed{0} & 3 \end{array}$

$\text{mcd}(28, 100) = 4$; $4 \mid 0 - 16 \longrightarrow$ $\boxed{\text{Tiene solución}}$

$4 = 16 + 12(-1)$

$* \; 12 = 28 + 16(-1)$

$4 = 100 + 28(-3) + \left(28 + 16(-1)\right)(-1)$

$* \; 16 = 100 + 28(-3)$

$4 = 100 + 28(-3) + (28)(-1) + \left(100 + 28(-3)\right)(-1)(-1)$

$4 = 100(2) + 28(-7)$

$$x \equiv \frac{16 \cdot 28 \cdot (-7) + 0 \cdot 100 \cdot 2}{4} \mod \left(\frac{28 \cdot 100}{4}\right) \; ; \quad x \equiv -784 \mod 700 \; ;$$

$$\boxed{x \equiv 616 \mod 700 \longrightarrow x = 700k + 616}$$

- Método sustitución :

- $x = 100q + 16$ (ec. 2)

Ec. 1 $\Longrightarrow$ $100q + 16 \equiv 0 \mod 28$

$100q \equiv 12 \mod 28$ (x 4)

$25q \equiv 3 \mod 7$

$4q \equiv 3 \mod 7$

$\cdot \; 2 \equiv 2 \mod 7$

$q \equiv 6 \mod 7$

- $q = 7k + 6$

$\downarrow$

$x = 100(7k + 6) + 16$

$\boxed{x = 700k + 616}$

$x \equiv 616 \pmod{700}$

⊛ 3 ecuaciones

+ Comprobar que hay solución $\Longrightarrow \begin{cases} \text{mcd}(m_1, m_2) \mid a-b \\ \text{mcd}(m_1, m_3) \mid a-c \\ \text{mcd}(m_2, m_3) \mid b-c \end{cases}$

+ Resolvemos el sistema con 2 ecuaciones

+ Resultado + 3ª ecuación ⟶ $\boxed{\text{Solución}}$

⊕ Sustitución ⟶ 3 letras ¡¡

- Criterios de divisibilidad $\Longrightarrow$ $10^i \equiv z_i \ (m)$

$m \mid (a)_{10}$

¡OjO! Criterio divisibilidad del 6

$10^i \equiv z_i \ (6)$

$10^0 \equiv 1 \ (6)$
$10^1 \equiv 4 \ (6)$
$10^2 \equiv 4 \ (6)$
$10^3 \equiv 4 \ (6)$
...

$\Longrightarrow$ $10^0 \equiv 1 \ (6)$; $10^i \equiv 4 \ (6) \quad \forall i \geq 1$

$6 \mid (a)_{10} \Longrightarrow 6 \mid (a_0 + 4(a_1 + a_2 \ldots))$

"Un nº es divisible por 6 si la suma de su último dígito más 4 veces la de los siguientes es divisible por 6"

Importante:

$\boxed{7^{242} \equiv x \pmod{20}}$ ⟶ ¡Euler!

$\boxed{\begin{cases} 4x \equiv 3 \pmod{15} \\ x - 2 \equiv 0 \pmod{35} \end{cases}}$ ⟶ ¡Simplificar joder!

$\boxed{3x82 \equiv 1 \pmod{9}}$ ⟶ ¡Forma decimal + $0.\ 10^0 \equiv 1.\ \_$ mod!

6 Principio de Inducción

• Operador sumatorio

$$\sum_{i=m}^{n} i = m + (m+1) + \dots + n$$

¡Ojo!

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \dots + n$$

$$\sum_{i=1}^{n} (2i-1) = 1 + 3 + 5 + \dots + n$$

$$\sum_{i=1}^{10} i = 1 + 2 + 3 + \dots + 10.$$

$$\sum_{i=1}^{10} 2 = 2 \cdot 10$$

• Factoriales y números combinatorios

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{0} = \binom{n}{n} = 1$$

¡Ojo!

$$\binom{10}{7} = \frac{10!}{7!\,3!} = \frac{10 \cdot 9 \cdot 8 \cdot \cancel{7!}}{\cancel{7!}\,3!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2} = \boxed{120}$$

$$\binom{-1/2}{5} = \frac{-\frac{1}{2}\left(-\frac{1}{2}-1\right)\left(-\frac{1}{2}-2\right)\left(-\frac{1}{2}-3\right)\left(-\frac{1}{2}-4\right)}{5!} = \frac{-\frac{1}{2}\left(-\frac{\cancel{3}}{2}\right)\left(-\frac{\cancel{5}}{2}\right)\left(-\frac{7}{2}\right)\left(-\frac{9}{2}\right)}{\cancel{5} \cdot 4 \cdot \cancel{3} \cdot 2 \cdot 1} =$$

$$= \boxed{\frac{-63}{2^8}}$$

• Binomio de Newton

¡Triángulo de Tartaglia!

1

1 1

1 2 1

1 3 3 1

$$(x+y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3 = \boxed{x^3 + 3x^2y + 3xy^2 + y^3}$$

- Principio de inducción   caso base + hipótesis de inducción
  paso inductivo

¡Ej! $1+2+3+\dots+n = \frac{n(n+1)}{2}$

1) Caso base

$\boxed{n=1} \Longrightarrow 1 = \frac{1(1+1)}{2}$; $1 = 1$

2) Paso inductivo

Suponemos que es cierto para $\boxed{n=k} \Longrightarrow 1+2+\dots+k = \frac{k(k+1)}{2}$

Demostramos que es cierta para $\boxed{n=k+1} \Longrightarrow 1+2+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1)$

$$= \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

Por lo tanto, la igualdad $P(n)$ es válida para todo $n \geq 1$

¡Ojo! $n \geq 5$; $2^n > n^2+n$

1) Caso base

$\boxed{n=5} \Longrightarrow 2^5 > 5^2+5$; $32 > 30$

2) Paso inductivo

Suponemos q es cierto para $\boxed{n=k} \Longrightarrow 2^k > k^2+k$

Demostramos que es cierta para $\boxed{n=k+1} \Longrightarrow 2^{k+1} > (k+1)^2+(k+1)$ ←

¡Objetivo! ⊛

$$2^{k+1} = 2^k \cdot 2 > (k^2+k)\cdot 2 = 2k^2+2k =$$

$$= \underline{k^2} + k^2 + \underline{2k}$$

- Ya que $k \geq 2 \Longrightarrow k^2 \geq 2k = k+k \geq k+2$

Por lo tanto, $2^n > n^2+n$ para todo $n \geq 5$

⊛ $(k+1)^2+(k+1) = k^2+1+2k+k+1 = \underline{k^2} + \underline{2k} + k+2$