# Ejercicios de aritmética

1. Algoritmo de Euclides

   - Calcula el máximo común divisor de los siguientes pares de números y exprésalo en función de los mismos
     - 38, 12
       Solución.-
       Dividimos el mayor entre el menor:
       $\underline{38} = 3 \cdot \underline{12} + 2$
       Sustituimos el menor por el resto: pasamos de $38, 12$ a $12, 2$ y volvemos a dividir el mayor por el menor:
       $\underline{12} = 6 \cdot \underline{2}$
       Como la división es exacta, hemos terminado y $mcd(38, 12) = mcd(12, 2) = 2$
       Despejamos el último resto no nulo en la igualdad en que aparezca como resto:
       $2 = \underline{38} - 3 \cdot \underline{12}$
       Ya hemos puesto $mcd(38, 12) = 2$ en función de 38 y 12
     - 53, 11
       Solución.-
       Dividimos el mayor entre el menor:
       $\underline{53} = 4 \cdot \underline{11} + 9$
       Sustituimos el menor por el resto: pasamos de $53, 11$ a $11, 9$ y volvemos a dividir el mayor por el menor:
       $\underline{11} = \underline{9} + 2$
       Sustituimos el menor por el resto: pasamos de $11, 9$ a $9, 2$ y volvemos a dividir el mayor por el menor:
       $\underline{9} = 4 \cdot \underline{2} + 1$
       Sustituimos el menor por el resto: pasamos de $9, 2$ a $2, 1$ y volvemos a dividir el mayor por el menor:
       $\underline{2} = 2 \cdot \underline{1}$
       Como la división es exacta, hemos terminado y $mcd(53, 11) = mcd(2, 1) = 1$
       Despejamos el último resto no nulo en la igualdad en que aparezca como resto:
       $1 = \underline{9} - 4 \cdot \underline{2}$
       Despejamos el menor de los dos números subrayados en la ecuación en que aparece como resto
       $\underline{2} = \underline{11} - \underline{9}$ y sustituimos:
       $1 = \underline{9} - 4 \cdot \underline{2} = \underline{9} - 4 \cdot (\underline{11} - \underline{9}) = 5 \cdot \underline{9} - 4 \cdot \underline{11}$
       Despejamos el menor de los dos números subrayados en la ecuación en que aparece como resto
       $\underline{9} = \underline{53} - 4 \cdot \underline{11}$ y sustituimos:
       $1 = 5 \cdot \underline{9} - 4 \cdot \underline{11} = 5 \cdot (\underline{53} - 4 \cdot \underline{11}) - 4 \cdot \underline{11} = 5 \cdot \underline{53} - 24 \cdot \underline{11}$
       Ya hemos puesto $mcd(53, 11) = 1$ en función de 53 y 11
     - 52, 46
       Solución.-
       Dividimos el mayor entre el menor:
       $\underline{52} = underline46 + 6$
       Sustituimos el menor por el resto: pasamos de $52, 46$ a $46, 6$ y volvemos a dividir el mayor por el menor:
       $\underline{46} = 7 \cdot \underline{6} + 4$
       Sustituimos el menor por el resto: pasamos de $46, 6$ a $6, 4$ y volvemos a dividir el mayor por el menor:
       $\underline{6} = \underline{4} + 2$

Sustituimos el menor por el resto: pasamos de $6, 4$ a $4, 2$ y volvemos a dividir el mayor por el menor:
$\underline{4} = 2 \cdot \underline{2}$
Como la división es exacta, hemos terminado y $mcd(52, 46) = mcd(4, 2) = 2$
Despejamos el último resto no nulo en la igualdad en que aparezca como resto:
$2 = \underline{6} - \underline{4}$
Despejamos el menor de los dos números subrayados en la ecuación en que aparece como resto
$\underline{4} = \underline{46} - 7 \cdot \underline{6}$ y sustituimos:
$2 = \underline{6} - \underline{4} = \underline{6} - (\underline{46} - 7 \cdot \underline{6}) = 8 \cdot \underline{6} - \underline{46}$
Despejamos el menor de los dos números subrayados en la ecuación en que aparece como resto
$\underline{6} = \underline{52} - \underline{46}$ y sustituimos:
$2 = 8 \cdot \underline{6} - \underline{46} = 8 \cdot (\underline{52} - \underline{46}) - \underline{46} = 8 \cdot \underline{52} - 9 \cdot \underline{46}$
Ya hemos puesto $mcd(52, 46) = 2$ en función de 52 y 46

  - 103, 221
  - 473, 201

- Calcula $mcd(3120, 270)$ y $x$, $y$ tales que $mcd(3120, 270) = 3120x + 270y$
- Calcula el máximo común divisor de los siguientes pares de números y exprésalo en función de los mismos
  - 402 y 31
  - 824 y 205
  - 412 y 102
  - 213 y 66

2. Paso a $\mathbb{Z}_n$

- Representa los siguientes números en el $\mathbb{Z}_n$ correspondiente
  - 3, -6, 15, -36 en $\mathbb{Z}_7$
    Solución.-
    - 3 ya está en $\mathbb{Z}_7$
    - Como $-6$ es negativo y pequeño, le sumo 7 (porque estoy en $\mathbb{Z}_7$). En $\mathbb{Z}_7$, $-6 = -6 + 7 = 1$
    - Como $15 \geq 7$, divido entre 7. Tenemos que $15 = 2 \cdot 7 + 1$, pasando a $\mathbb{Z}_7$ obtengo $15 = 2 \cdot 0 + 1 = 1$
    - Voy a pasar primero 36 a $\mathbb{Z}_7$. Para ello, igual que antes, divido 36 entre 7, $36 = 5 \cdot 7 + 1$. Pasando a $\mathbb{Z}_7$, $36 = 5 \cdot 0 + 1 = 1$.
      Por tanto $-31 = -1$. Como $-1$ es negativo y pequeño, le sumo 7. En $\mathbb{Z}_7$ tenemos que $-1 = -1 + 7 = 6$
  - 13, -27, 145, -32 en $\mathbb{Z}_{11}$
    Solución.-
    - Como 13 es pequeño y estoy en $\mathbb{Z}_{11}$, le resto 11. En $\mathbb{Z}_{11}$, $13 = 13 - 11 = 2$
    - Primero paso 27 a $\mathbb{Z}_{11}$. Para eso, divido por 11 y tengo $27 = 2 \cdot 11 + 5$. Pasando a $\mathbb{Z}_{11}$ tengo $27 = 2 \cdot 0 + 5 = 5$.
      Luego $-27 = -5$. Como es negativo y pequeño, le sumo 11. En $\mathbb{Z}_{11}$ tendremos que $-27 = -5 = -5 + 11 = 6$.
    - Para pasar 145 a $\mathbb{Z}_{11}$, divido por 145 y tengo $145 = 13 \cdot 11 + 2$. Pasando a $\mathbb{Z}_{11}$ tengo $145 = 13 \cdot 0 + 2 = 2$.
    - Primero paso 32 a $\mathbb{Z}_{11}$. Para eso, divido por 11 y tengo $32 = 2 \cdot 11 + 10$. Pasando a $\mathbb{Z}_{11}$ tengo $32 = 2 \cdot 0 + 10 = 10$.
      Luego $-27 = -10$. Como es negativo y pequeño, le sumo 11. En $\mathbb{Z}_{11}$ tendremos que $-32 = -10 = -10 + 11 = 1$.
  - 1423, -2007, 1425, -312 en $\mathbb{Z}_5$
- Calcula $342 \cdot 453 + 123 \cdot 1987$ en $\mathbb{Z}_6$
- Encuentra el representante de cada uno de los siguientes números en el correspondiente $\mathbb{Z}_n$
  - 23, 12, 56, -3, -43, -12 en $\mathbb{Z}_4$
  - 21, 19, 156, -3, -23, -1 en $\mathbb{Z}_2$
  - 27, 11, 58, -5, -73, -11 en $\mathbb{Z}_{11}$

3. Inversos en $\mathbb{Z}_n$ con $n$ pequeño

- Indica qué némeros de $\mathbb{Z}_{12}$ tienen inverso. Para los que tengan, calcula dicho inverso
  Solución.-

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

  Como los elementos que tienen inverso son aquellos que no tienen factores comunes con 12 y $12 = 2 \cdot 2 \cdot 3$, podemos asegurar que no tienen inverso $\{0, 2, 3, 4, 6, 8, 9, 10\}$ mientras que sí lo tienen $\{1, 5, 7, 11\}$. Además, para cualquier elemento que tenga inverso, su inverso estará también en la lista de los que tienen inverso. Probando obtenemos que:

$$1^{-1} = 1$$
$$5^{-1} = 5$$
$$7^{-1} = 7$$
$$11^{-1} = 11$$

- Indica qué números de $\mathbb{Z}_{14}$. Para los que tengan, calcula dicho inversos
  Solución.-

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$$

  Como los elementos que tienen inverso son aquellos que no tienen factores comunes con 14 y $12 = 2 \cdot 7$, podemos asegurar que no tienen inverso $\{0, 2, 4, 6, 7, 8, 10, 12\}$ mientras que sí lo tienen $\{1, 3, 5, 9, 11, 13\}$. Además, para cualquier elemento que tenga inverso, su inverso estará también en la lista de los que tienen inverso. Probando obtenemos que:

$$1^{-1} = 1$$
$$3^{-1} = 5$$
$$5^{-1} = 3$$
$$9^{-1} = 11$$
$$11^{-1} = 9$$
$$13^{-1} = 13$$

- Realiza las siguientes operaciones en el correspondiente $\mathbb{Z}_n$
  - $32 \cdot 21 - 12 \cdot 24^{-1}$ en $\mathbb{Z}_5$
    Solución.-
    Pasamos primero todos los números a $\mathbb{Z}_5$

$$32 \cdot 21 - 12 \cdot 24^{-1} = 2 \cdot 1 - 2 \cdot 4^{-1}$$

    Por simple inspección $4^{-1} = 4$ luego:

$$32 \cdot 21 - 12 \cdot 24^{-1} = 2 \cdot 1 - 2 \cdot 4^{-1} = 2 \cdot 1 - 2 \cdot 4 = 2 - 8 = -6 = -1 = 4$$

- $12 \cdot 213 - 121 \cdot 3^{-1}$ en $\mathbb{Z}_7$
  Solución.-
  Pasamos primero todos los números a $\mathbb{Z}_7$
  $$12 \cdot 213 - 121 \cdot 3^{-1} = 5 \cdot 3 - 2 \cdot 3^{-1}$$
  Por simple inspección $3^{-1} = 5$ luego:
  $$12 \cdot 213 - 121 \cdot 3^{-1} = 5 \cdot 3 - 2 \cdot 15 - 10 = 5$$

- Para cada $\mathbb{Z}_n$ estudia qué elementos son invertibles y, para los que lo sean, calcula su inverso
  - $\mathbb{Z}_9$
  - $\mathbb{Z}_{12}$
  - $\mathbb{Z}_{18}$
- Calcula los siguientes inversos (cuando sea posible)
  - inverso de 2 y 5 en $\mathbb{Z}_7$
  - inverso de 3, 5 y 6 en $\mathbb{Z}_8$
  - inverso de 21 y 14 en $\mathbb{Z}_{25}$
- Para cada uno de los $\mathbb{Z}_n$ indicados estudia qué elementos tienen inverso y, para cada uno de ellos, calcula el inverso correspondiente
  - $\mathbb{Z}_2$
  - $\mathbb{Z}_4$
  - $\mathbb{Z}_7$
  - $\mathbb{Z}_{10}$
- Efectúa las operaciones indicadas en el $\mathbb{Z}_n$ indicado
  - $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4$ en $\mathbb{Z}_6$
  - $21 + 10 \cdot 21^{-1} + 43 \cdot 10^4$ en $\mathbb{Z}_2$
  - $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4$ en $\mathbb{Z}_4$
- Indica qué elementos de $\mathbb{Z}_{10}$ son invertibles indicando para los que lo sean cuál es el inverso
- Indica qué elementos de $\mathbb{Z}_9$ son invertibles indicando para los que lo sean cuál es el inverso
- Calcula el inverso de 31 en $\mathbb{Z}_{100}$
- Indica qué elementos de $\mathbb{Z}_{14}$ son invertibles indicando para los que lo sean cuál es el inverso
- Indica qué elementos de $\mathbb{Z}_{12}$ son invertibles indicando para los que lo sean cuál es el inverso

4. Inversos usando la función $\phi$ de Euler

- Calcula $\phi(20)$ y úsala para ver si 3, 6 y 11 tienen inverso en $\mathbb{Z}_{20}$. Calcula $11^{-1}$ en $\mathbb{Z}_{20}$
  Solución.-
  $20 = 2^2 \cdot 5$, por lo que $\phi(20) = \phi(2^2 \cdot 5) = \phi(2^2)\phi(5) = (2^2 - 2^1) \cdot (5-1) = (4-2) \cdot 4 = 8$
  Tienen inverso aquellos números $a$ de modo que $a^{\phi(20)} = a^8$ valgan 1.
  $3^8 = 3 \cdot 3 \cdots \cdot 3 = 1$, luego 3 tiene inverso en $\mathbb{Z}_{20}$.
  $6^8 = 6 \cdot 6 \cdots \cdot 6 = 16$, por lo que 6 no tiene inverso en $\mathbb{Z}_{20}$
  $11^8 = 11 \cdot 11 \cdots \cdot 11 = 1$, luego 3 tiene inverso en $\mathbb{Z}_{20}$
  Como $11^8 = 11 \cdot 11^7 = 1$ tenemos que $11^{-1} = 11^7 = 11$
- Calcula $\phi(12)$ y úsala para ver si 3, 4 y 6 tienen inverso en $\mathbb{Z}_{12}$. Calcula $11^{-1}$ en $\mathbb{Z}_{12}$
  Solución.-
  $12 = 2^2 \cdot 3$, por lo que $\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2)\phi(3) = (2^2 - 2^1) \cdot (3-1) = (4-2) \cdot 2 = 4$
  Tienen inverso aquellos números $a$ de modo que $a^{\phi(12)} = a^4$ valgan 1.
  $3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = 81 = 9$, luego 3 no tiene inverso en $\mathbb{Z}_{12}$.
  $6^4 = 6 \cdot 6 \cdot 6 \cdot 6 = 0$, por lo que 6 no tiene inverso en $\mathbb{Z}_{20}$
  $11^4 = 11 \cdot 11 \cdot 11 \cdot 11 = 1$, luego 11 tiene inverso en $\mathbb{Z}_{20}$
  Como $11^4 = 11 \cdot 11^3 = 1$ tenemos que $11^{-1} = 11^3 = 11$
- Calcula $\phi(15)$ y úsala para ver si 3, 6 y 11 tienen inverso en $\mathbb{Z}_{15}$. Calcula $11^{-1}$ en $\mathbb{Z}_{15}$
- Calcula $\phi(16)$ y úsala para ver si 3, 6 y 11 tienen inverso en $\mathbb{Z}_{16}$. Calcula $3^{-1}$ en $\mathbb{Z}_{16}$
- Calcula $\phi(18)$ y úsala para ver si 5, 6 y 13 tienen inverso en $\mathbb{Z}_{18}$. Calcula $13^{-1}$ en $\mathbb{Z}_{18}$
- Calcula $\phi(48)$ y úsala para ver si 2, 3 y 5 tienen inverso en $\mathbb{Z}_{48}$. Calcula $5^{-1}$ en $\mathbb{Z}_{48}$
- Calcula $\phi(13)$ y úsala para ver si 3, 6 y 11 tienen inverso en $\mathbb{Z}_{13}$. Calcula $3^{-1}$ en $\mathbb{Z}_{13}$

5. Inversos usando el algoritmo extendido de Euclides

    - Indica en $\mathbb{Z}_{80}$ dos elementos que tengan inverso y dos que no y calcula el inverso de 21 en $\mathbb{Z}_{80}$
      Solución.-
      $80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$, por tanto no serán invertibles los números pares ni los múltiplos de 5 (y los demás sí lo serán)
      Invertibles: 3, 7
      No invertibles: 2, 4
      Vamos a calcular el inverso de 21:
      $80 = 3 \cdot 21 + 17$
      $21 = 17 + 4$
      $17 = 4 \cdot 4 + 1$
      $4 = 4 \cdot 1$
      Despejando:
      $1 = 17 - 4 \cdot 4 = 17 - 4 \cdot (21 - 17) = 5 \cdot 17 - 4 \cdot 21 = 5 \cdot (80 - 3 \cdot 21) - 4 \cdot 21 = 5 \cdot 80 - 19 \cdot 21$
      Pasando a $\mathbb{Z}_{80}$
      $1 = 5 \cdot 0 - 19 \cdot 21 = -19 \cdot 21$
      por tanto $21^{-1} = -19 = 80 - 19 = 61$
    - Calcula el inverso de 13 en $\mathbb{Z}_{200}$
      $200 = 15 \cdot 13 + 5$
      $13 = 2 \cdot 5 + 3$
      $5 = 1 \cdot 3 + 2$
      $3 = 1 \cdot 2 + 1$
      $2 = 2 \cdot 1$
      Despejando (empezando por el final:
      $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5 = 2 \cdot 13 - 5 \cdot (200 - 15 \cdot 13) = 77 \cdot 13 - 5 \cdot 200$
      Pasando a $\mathbb{Z}_{200}$
      $1 = 77 \cdot 13 - 5 \cdot 0 = 77 \cdot 13$ en $\mathbb{Z}_{200}$. Luego $13^{-1} = 77$
    - Calcula el inverso de 7 en $\mathbb{Z}_{200}$
      $200 = 28 \cdot 7 + 4$
      $7 = 1 \cdot 4 + 3$
      $4 = 1 \cdot 3 + 1$
      $3 = 3 \cdot 1$
      Despejando (empezando por el final:
      $1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (200 - 28 \cdot 7) - 7 = 2 \cdot 200 - 57 \cdot 7$
      Pasando a $\mathbb{Z}_{200}$
      $1 = 2 \cdot 0 - 57 \cdot 7 = 143 \cdot 7$ en $\mathbb{Z}_{200}$. Luego $7^{-1} = 143$
    - Calcula el inverso de 21 en $\mathbb{Z}_{130}$
    - Calcula el inverso de 29 en $\mathbb{Z}_{100}$ usando el algoritmo inverso de Euclides
    - Calcula el inverso de 31 en $\mathbb{Z}_{100}$ usando el algoritmo inverso de Euclides
    - Calcula el inverso de 11 en $\mathbb{Z}_{350}$
    - Calcula los siguientes inversos en el $\mathbb{Z}_n$ indicado
        - $11^{-1}$ en $\mathbb{Z}_{42}$
        - $8^{-1}$ en $\mathbb{Z}_{35}$
        - $23^{-1}$ en $\mathbb{Z}_{100}$
        - $13^{-1}$ en $\mathbb{Z}_{70}$
    - Calcula los siguientes inversos

  - inverso de 7 en $\mathbb{Z}_{36}$
  - inverso de 11 en $\mathbb{Z}_{52}$
- Calcula el inverso de 21 en $\mathbb{Z}_{100}$
- Indica qué elementos de $\mathbb{Z}_{12}$ tienen inverso. Calcula el inverso de 17 en $\mathbb{Z}_{80}$
- Calcula el inverso de 17 en $\mathbb{Z}_{80}$
- Calcula el inverso de 7 en $\mathbb{Z}_{180}$

6. Calcular inversas de matrices en $\mathbb{Z}_n$

- Calcula la inversa de la siguiente matriz en $\mathbb{Z}_5$ usando operaciones elementales

$$\begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix}$$

Solución.-
Ampliamos con la identidad

$$\left(\begin{array}{cc|cc} 3 & 2 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 4 & 2 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 4 & 2 & 0 \\ 0 & 4 & 4 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 4 & 2 & 0 \\ 0 & 1 & 1 & 4 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 0 & 3 & 4 \\ 0 & 1 & 1 & 4 \end{array}\right)$$

Luego

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 \\ 1 & 4 \end{pmatrix}$$

- Calcula la inversa de la siguiente matriz en $\mathbb{Z}_5$ usando operaciones elementales

$$\begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}$$

Solución.-
Ampliamos con la identidad

$$\left(\begin{array}{cc|cc} 4 & 2 & 1 & 0 \\ 3 & 3 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 3 & 4 & 0 \\ 3 & 3 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 3 & 4 & 0 \\ 0 & 4 & 3 & 1 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 3 & 4 & 0 \\ 0 & 1 & 2 & 4 \end{array}\right) \simeq \left(\begin{array}{cc|cc} 1 & 0 & 3 & 3 \\ 0 & 1 & 2 & 4 \end{array}\right)$$

Luego

$$\begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 3 \\ 2 & 4 \end{pmatrix}$$

- Calcula la inversa de la siguiente matriz en $\mathbb{Z}_5$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Solución.-

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & 0 & -2 & 1 & 0 \\ 0 & -1 & -2 & -1 & 0 & 1 \end{array}\right) \simeq \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 2 & -1 & 0 \\ 0 & 1 & 2 & 1 & 0 & -1 \end{array}\right) \simeq$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & -2 & 0 \\ 0 & 1 & 2 & 1 & 0 & -1 \end{array}\right) \simeq \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 3 & 0 \\ 0 & 0 & 2 & -3 & 2 & -1 \end{array}\right) \simeq \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 3 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right) \simeq$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 3 & 4 & 0 \\ 0 & 1 & 0 & 4 & 3 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right) \simeq \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 4 & 3 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right)$$

- Reduce cada una de las siguientes matrices a forma escalonada en el $\mathbb{Z}_n$ indicado:
  - $A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 4 & 3 \\ 2 & 5 & 1 \end{pmatrix}$ en $\mathbb{Z}_2$

- $B = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 4 & 2 & 3 & 3 \\ 2 & 5 & 1 & 3 \end{pmatrix}$ en $\mathbb{Z}_7$
- $C = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 4 & 4 & 3 & 3 \\ 2 & 5 & 1 & 5 \\ 3 & 2 & 0 & 1 \end{pmatrix}$ en $\mathbb{Z}_5$
- $D = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 4 & 3 \\ 0 & 4 & 1 \\ 3 & 2 & 1 \end{pmatrix}$ en $\mathbb{Z}_3$

- Encuentra cuando sea posible las inversas de las siguientes matrices
  - $A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 4 & 3 \\ 2 & 5 & 1 \end{pmatrix}$ en $\mathbb{Z}_2$
  - $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ en $\mathbb{Z}_7$
  - $C = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 0 \\ 3 & 0 & 0 \end{pmatrix}$ en $\mathbb{Z}_5$
- Encuentra la inversa de la siguiente matriz en $\mathbb{Z}_7$

$$\begin{pmatrix} 2 & 1 & 3 \\ 4 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

7. Resolver sistemas de ecuaciones en $\mathbb{Z}_n$

- Resuelve el siguiente sistema en $\mathbb{Z}_7$ pasando la matriz del sistema a forma reducida

$$\begin{array}{rcl} 3x+2y+2z & = & 1 \\ 5x+y+2z & = & 2 \end{array}$$

Solución.-
Escribiendo el sistema en forma matricial tenemos

$$\left(\begin{array}{ccc|c} 3 & 2 & 2 & 1 \\ 5 & 1 & 2 & 2 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 3 & 3 & 5 \\ 5 & 1 & 2 & 2 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 3 & 3 & 5 \\ 0 & 0 & 1 & 5 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 3 & 0 & 4 \\ 0 & 0 & 1 & 5 \end{array}\right)$$

Es decir:

$$\begin{array}{rcl} x+3y & = & 4 \\ z & = & 5 \end{array}$$

Que da como soluciones $x = 4 - 3y$, $z = 5$

- Resuelve el siguiente sistema en $\mathbb{Z}_7$ pasando la matriz del sistema a forma reducida

$$\begin{array}{rcl} 2x+2y+z & = & 1 \\ 3x+3y+2z & = & 2 \end{array}$$

Solución.-
Escribiendo el sistema en forma matricial tenemos

$$\left(\begin{array}{ccc|c} 2 & 2 & 1 & 1 \\ 3 & 3 & 2 & 2 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 1 & 4 & 4 \\ 3 & 3 & 2 & 2 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 1 & 4 & 4 \\ 0 & 0 & 4 & 4 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 1 & 4 & 4 \\ 0 & 0 & 1 & 1 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

Es decir:

$$\begin{array}{rcl} x+y & = & 0 \\ z & = & 1 \end{array}$$

Que da como soluciones $x = -y$, $z = 1$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_5$

$$\begin{aligned} 3x+y+4z &= 3 \\ 2x+4y+3z &= 0 \\ 4x+3y &= 1 \\ 2x+4y+2z &= 1 \end{aligned}$$

Solución.-

$$\left(\begin{array}{ccc|c} 3 & 1 & 4 & 3 \\ 2 & 4 & 3 & 0 \\ 4 & 3 & 0 & 1 \\ 2 & 4 & 2 & 1 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 2 & 4 & 3 & 0 \\ 4 & 3 & 0 & 1 \\ 2 & 4 & 2 & 1 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 1 & 4 \end{array}\right) \simeq \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 4 \end{array}\right)$$

$$\simeq \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Hay que resolver

$$\begin{aligned} x+2y+3z &= 1 \\ z &= 4 \end{aligned}$$

Soluciones $z = 4$, $x = 1 - 2y - 3z = 4 - 2y$

- Resuelve el siguiente sistema en $\mathbb{Z}_5$
  $x + 3y + z = 0$
  $2x + 2z = 1$
  $y + 3z = 0$
- Encuentra todas las soluciones de los siguientes sistemas de ecuaciones lineales
  - En $\mathbb{Z}_7$
    $3x + 2y + 2z = 1$
    $5x + y + 2z = 2$
  - En $\mathbb{Z}_5$
    $x - y + z + t = 1$
    $2x + y - t = 2$
    $y - z + 2t = 0$
    $3x + y + z + t = 3$
  - En $\mathbb{Z}_{11}$
    $2x - y + z + t = 1$
    $2x + y - t = 2$
    $y + 2z + 3t = 0$
- Resuelve las siguientes ecuaciones
  - 2x = 3 en $\mathbb{Z}_7$
  - 3x = 2 en $\mathbb{Z}_8$
  - 5x = 4 en $\mathbb{Z}_{22}$
- Resuelve los siguientes sistemas de ecuaciones
  - En $\mathbb{Z}_7$
    $3x - 2y + z = 3$
    $x - 2y + z = 1$
    $x + y - 3z = 3$
  - En $\mathbb{Z}_5$
    $2x - 3y + z + t = 1$
    $x + y - 2z = 2$
    $2x - y + z + t = 4$
  - En $\mathbb{Z}_7$
    $2x - 3y + z = 1$
    $x + y - 2z = 2$
    $x + y + z = 0$
    $x - y - z = 2$
- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_5$

$$3x + y = 1$$
$$x + 2y + z = 1$$
$$2x + 4y = 4$$
$$3x + y + 4z = 2$$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_5$

$$3x + y + 4z = 3$$
$$2x + 3y + 4z = 0$$
$$4x + 3y = 1$$
$$2x + 4y + 2z = 1$$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_{11}$

$$\begin{aligned} 2x + y + z &= 2 \\ 3x + 4y + 2z &= 1 \\ 4x + 2y + 3z &= 0 \\ x + 3y + 4z &= 2 \end{aligned}$$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_7$

$$\begin{aligned} x + 4y + z &= 2 \\ 2x + 3y + z &= 1 \\ 3x + 2y + 3z &= 1 \end{aligned}$$

- Resuelve el siguiente sistema de ecuaciones en $\mathbb{Z}_7$

$$2x + 2y + 4z + 4t = 2 \tag{1}$$
$$3x + 3y + 2z + 6t = 2 \tag{2}$$
$$x + y + 2z + 3t = 4 \tag{3}$$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_{11}$

$$\begin{aligned} 3x + 2y + z &= 1 \\ 6x + 4y + 4z &= 4 \\ 9x + 6y + 7z &= 7 \end{aligned}$$

- Encuentra todas las soluciones del siguiente sistema en $\mathbb{Z}_7$

$$\begin{aligned} 3x + 6y + 3z &= 2 \\ 2x + 4y + 3z &= 1 \\ 5x + 3y + 4z &= 6 \end{aligned}$$

8. Problemas del teorema Chino de los Restos

- Encuentra todas las soluciones del siguiente sistema de ecuaciones

$$\begin{aligned} 2x &= 5 \text{ en } \mathbb{Z}_9 \\ 3x &= 2 \text{ en } \mathbb{Z}_7 \\ 5x &= 1 \text{ en } \mathbb{Z}_4 \end{aligned}$$

  De la primera ecuación $2x = 5$ en $\mathbb{Z}_9$. Multiplicando por $5$ que es el inverso de $2$ en $\mathbb{Z}_9$ obtengo $x = 25 = 7$ en $\mathbb{Z}_9$, luego $x = 7 + 9 \cdot y$
  De la segunda ecuación $3x = 3 \cdot (7 + 9y) = 21 + 27y = 2$ en $\mathbb{Z}_7$. Luego $27y = 6y = 2 - 21 = 2$ en $\mathbb{Z}_7$. Multiplicando por $6$ que es el inverso de $6$ en $\mathbb{Z}_7$, tengo $y = 12 = 5$ en $\mathbb{Z}_7$. Por tanto $y = 5 + 7z$ y $x = 7 + 9y = 7 + 9 \cdot (5 + 7z) = 52 + 63z$
  De la tercera ecuación $x = 52 + 63z = 3z = 1$. Multiplicando por $3$ (el inverso de $3$ en $\mathbb{Z}_4$, tengo $z = 3$ en $\mathbb{Z}_4$, luego $z = 3 + 4k$ y $x = 52 + 63 \cdot (3 + 4k) = 241 + 252k$

- Encuentra todas las soluciones del siguiente sistema de ecuaciones

$$\begin{aligned} 2x &= 3 \text{ en } \mathbb{Z}_5 \\ 3x &= 2 \text{ en } \mathbb{Z}_7 \\ x &= 3 \text{ en } \mathbb{Z}_6 \end{aligned}$$

  De la primera ecuación $2x = 3$ en $\mathbb{Z}_5$. Multiplicando por $3$ que es el inverso de $2$ en $\mathbb{Z}_5$ obtengo $x = 9 = 4$ en $\mathbb{Z}_9$, luego $x = 4 + 5 \cdot y$
  De la segunda ecuación $3x = 3 \cdot (4+5y) = 12+15y = 2$ en $\mathbb{Z}_7$. Luego $15y = y = 2-12 = -10 = 4$ en $\mathbb{Z}_7$.Por tanto $y = 4 + 7z$ y $x = 4 + 5 \cdot (4 + 7z) = 24 + 35z$
  De la tercera ecuación $x = 24 + 35z = 5z = 3$. Multiplicando por $5$ (el inverso de $5$ en $\mathbb{Z}_6$, tengo $z = 15 = 3$ en $\mathbb{Z}_6$, luego $z = 3 + 6k$ y $x = 24 + 35 \cdot (3 + 6k) = 129 + 210k$

- Un programa produce números que se sabe que son siempre múltiplos de 3, que son impares y que el triple de esos números siempre dan resto 2 al dividirlos por 5 ¿qué forma tienen esos números? Calcula dos de ellos y comprueba que cumplen las condiciones
  Solución.-
  Llamando $x$ a uno de los números que produce el programa, tendremos que debe cumplir:

$$\begin{aligned} x &\equiv 0 \text{ (en } \mathbb{Z}_3) \\ x &\equiv 1 \text{ (en } \mathbb{Z}_2) \\ 3x &\equiv 2 \text{ (en } \mathbb{Z}_5) \end{aligned}$$

  De la primera ecuación $x = 0 + 3 \cdot a = 3 \cdot a$
  Sustituyo en la segunda ecuación:
  $x = 3 \cdot a = a = 1$ en $\mathbb{Z}_2$, luego $a = 1 + 2 \cdot b$ y $x = 3 \cdot a = 3 + 6 \cdot b$
  Sustituyo en la tercera ecuación:
  $3 \cdot (3 + 6 \cdot b) = 9 + 18 \cdot b = 2$ en $\mathbb{Z}_5$, es decir $18b = 3 \cdot b = -7 = 3$, con lo que $b = 1$ en $\mathbb{Z}_5$ y $b = 1 + 5 \cdot c$.
  Sustituyendo, obtengo que:

$$x = 3 + 6 \cdot b = 9 + 30 \cdot c$$

  Dando a $c$ valores $0$ y $1$ obtengo los dos valores de $x$ que son $x = 9$ y $x = 39$ que cumplen las condiciones pedidas

- Un general quiere distribuir a sus soldados en grupos. Primero dispone a sus soldados en grupos de 11 y le sobran 2. Decide quitar 10 soldados y agruparlos en grupos de 9 y ahora le sobran 3. Finalmente añade de nuevo 4 de los 10 soldados que quitó y, al agruparlos en grupos de 25 le sobra 1. Calcula dos posibles soluciones del número de soldados y comprueba que

la primera de ellas cumple las condiciones
Solución.-
Sea $x$ el número de soldados. Las tres condiciones que nos dan son:

$$\begin{array}{c} x = 2 \text{ en } \mathbb{Z}_{11} \\ x - 10 = 3 \text{ en } \mathbb{Z}_9 \\ x - 6 = 1 \text{ en } \mathbb{Z}_{25} \end{array}$$

De la primera ecuación obtenemos $x = 2 + 11 \cdot a$
Sustituyo en la segunda:
$2 + 11 \cdot a - 10 = 3$, luego $11 \cdot a = 11$ por lo que $a = 1$ en $\mathbb{Z}_9$ o, lo que es lo mismo, $a = 1 + 9 \cdot b$. Sustituyendo obtengo $x = 13 + 99 \cdot b$
Yendo a la tercera ecuación:
$x - 6 = 13 + 99 \cdot b - 6 = 1$, de donde $99b = -6$ con lo que $b = 6$ en $\mathbb{Z}_{25}$ o, $b = 6 + 25 \cdot c$.
Sustituyendo:

$$x = 13 + 99 \cdot 6 + 99 \cdot 25c$$

Para $c = 1$ obtengo $x = 607$ para el que es fácil comprobar que se cumplen las condiciones.

- En una Facultad hay tres grupos, todos ellos con el mismo número de alumnos. El primer examen lo hacen todos juntos en grupos de 5 y sobra un alumno. Otro día hacen un examen solamente los dos primeros grupos, se ponen en aulas de 9 y sobran 2. Finalmente se sabe que el número de alumnos en cada grupo es múltiplo de 7 ¿cuántos alumnos puede haber en cada grupo?
  Solución.-
  Ecuaciones:

  $$\begin{array}{c} 3x = 1 \text{ en } \mathbb{Z}_5 \\ 2x = 2 \text{ en } \mathbb{Z}_9 \\ x = 0 \text{ en } \mathbb{Z}_7 \end{array}$$

  Multiplico por 2 la primera ecuación y obtengo $x = 2$ en $\mathbb{Z}_5$, por lo que $x = 2 + 5 \cdot k$
  La segunda ecuación queda $2 \cdot (2 + 5 \cdot k) = 2$ en $\mathbb{Z}_9$. Operando obtenemos $k = -2 = 7$ en $\mathbb{Z}_9$, es decir, $k = 7 + 9 \cdot a$ por lo que $x = 2 + 5 \cdot (7 + 9 \cdot a) = 37 + 45 \cdot a$.
  Sustituyendo en la tercera ecuación, $2 + 3 \cdot a = 0$ en $\mathbb{Z}_7$, por lo que $3 \cdot a = 5$ y $a = 4$ en $\mathbb{Z}_7$, es decir $a = 4 + 7 \cdot b$. Sustituyendo obtenemos:

  $$x = 37 + 45 \cdot (4 + 7 \cdot b) = 217 + 315 \cdot b$$

- Unas determinadas piezas se distribuyen en cajas. Se sabe que en cada caja hay $x$ piezas y queremos saber el valor de $x$. Sabemos que si cogemos 2 cajas y las piezas las repartimos en 5 montones sobran 3 piezas. Si cogemos 3 cajas y las piezas las repartimos entre 8 montones sobran 2 y que el número de piezas por caja es múltiplo de 3. ¿Cuánto puede valer $x$?
  Solución.-
  Tenemos las condiciones:

  $$\begin{array}{c} 2x = 3 \text{ en } \mathbb{Z}_5 \\ 3x = 2 \text{ en } \mathbb{Z}_8 \\ x = 0 \text{ en } \mathbb{Z}_3 \end{array}$$

  En $\mathbb{Z}_5$: $2x = 3$, multiplicando por $2^{-1} = 3$ tenemos $x = 4$ en $\mathbb{Z}_5$, por lo que $x = 4 + 5k$
  En $\mathbb{Z}_8$: $3x = 3(4 + 5k) = 12 + 15k = 4 + 7k = 2$, luego $7k = -2 = 6$. Multiplicando por

$7^{-1} = 7$ obtengo $k = 42 = 2$ en $\mathbb{Z}_8$, con lo que $k = 2 + 8a$ y $x = 4 + 5(2 + 8a) = 14 + 40a$ En $\mathbb{Z}_3$: $x = 14 + 40a = 2 + a = 0$, luego $a = -2 = 1$ en $\mathbb{Z}_3$, es decir, $a = 1 + 3b$ y, por tanto, $x = 14 + 40(1 + 3b) = 54 + 120b$

- resuelve los siguientes sistemas
  - $x \equiv 3 \pmod 6$
    $x \equiv 4 \pmod{31}$
    $x \equiv 1 \pmod 7$
  - $x \equiv 1 \pmod 8$
    $x \equiv 4 \pmod 9$
    $x \equiv -1 \pmod 5$
- De un cierto número se sabe que al dividirlo por siete el resto es 3. El resto al dividir el doble de ese número por 11 es 5 y el úmero es múltiplo de 4. ¿Cuánto puede valer ese número?

9. Ecuaciones diofánticas

- Encuentra todas las soluciones de la ecuación $21x + 35y = 14$
  Solución.-
  Simplificamos por 7 para obtener $3x + 5y = 2$
  Pasamos a $\mathbb{Z}_5$, $3x = 2$, luego $x = 4$. Por tanto $x = 4 + 5r$
  Pasamos a $\mathbb{Z}_3$, $2y = 2$, luego $y = 1$. Por tanto $y = 1 + 3s$
  Sustituimos $3 \cdot (4 + 5r) + 5 \cdot (1 + 3s) = 2$. Simplificando $r + s = -1$, luego $s = -1 - r$.
  Soluciones $x = 4 + 5r$, $y = -2 - 3r$
- Encuentra todas las soluciones de la ecuación $30x + 42y = 66$
  Solución.-
  Simplifico la ecuación por 6
  $$5x + 7y = 11$$
  Paso a $\mathbb{Z}_7$:
  $$5x = 4$$
  Multiplico por $5^{-1} = 3$ y obtengo $x = 5$ en $\mathbb{Z}_7$. Por lo que $x = 5 + 7 \cdot r$
  Paso a $\mathbb{Z}_5$:
  $$2y = 1$$
  Multiplico por $2^{-1} = 3$ y obtengo $y = 3$ en $\mathbb{Z}_5$. Por lo que $y = 3 + 5 \cdot s$
  Volviendo a la ecuación y sustituyendo:
  $$5 \cdot (5 + 7r) + 7 \cdot (3 + 5s) = 11$$
  $$25 + 35r + 21 + 35s = 11$$
  $$35 \cdot (r + s) = 11 - 21 - 25 = -35$$
  $$r + s = -1$$
  $$s = 1 - -r$$
  Soluciones:
  $$x = 5 + 7r$$
  $$y = 3 + 5 \cdot (-1 - r) = -2 - 5r$$
  para cualquier valor entero de $r$
- En una fiesta hay 32 personas. Para entrar o salir de la fiesta tenemos dos autobuses con capacidad para 12 y 8 personas. Sabiendo que esos autobuses solamente hacen viajes completas ¿cómo podemos conseguir que al final queden exactamente 4 personas en la fiesta?
  Solución.-
  Sean $x$ e $y$ el número de viajes que hacen los autobuses con capacidad para 12 y 8 personas (respectivamente). Como hay 32 personas y al final queremos que queden 4, se habrán llevado a $32 - 4 = 28$ personas. Por tanto la ecuación a resolver es:
  $$12x + 8y = 28$$
  Simplificando: $3x + 2y = 7$
  Paso a $\mathbb{Z}_2$: $x = 1$ en $\mathbb{Z}_2$, por lo que $x = 1 + 2k$
  Paso a $\mathbb{Z}_3$: $2y = 1$, por lo que $y = 2$ en $\mathbb{Z}_3$, en general $y = 2 + 3a$
  Sustituyendo en la ecuación original:
  $$3 \cdot (1 + 2k) + 2 \cdot (2 + 3a) = 7$$

$$3+6k+4+6a=7$$
$$6k+6a=0$$
$$k+a=0$$
$$a=-k$$

Luego las soluciones son:

$$x=1+2k$$
$$y=2+3a=2-3k$$

- Tenemos dos recipientes de agua con capacidad de 33 y 24 litros y con ellos queremos conseguir una cantidad de exactamente 75 litros. Calcula todas las formas de hacerlo
  Solución.-
  Sean $x$ e $y$ el número de veces que usamos cada cubo. La ecuación a resolver será:

  $$33x+24y=75$$

  Simplificando por 3 tendremos $11x+8y=25$
  Paso a $\mathbb{Z}_8$: $3x=1$. Multiplicando por $3^{-1}=3$ obtengo $x=3$ en $\mathbb{Z}_8$, por lo que $x=3+8k$
  Paso a $\mathbb{Z}_{11}$: $8y=3$. Multiplicando por $8^{-1}=7$ obtengo $y=21=10$ en $\mathbb{Z}_{11}$, por lo que $y=10+11a$
  Sustituimos en nuestra ecuación:

  $$11x+8y=11(3+8k)+8(10+11a)=25$$

  Simplificando: $88(k+a)=-88$, por lo que $k+a=-1$ y tendré $a=-1-k$.
  Soluciones:

  $$x=3+8k$$
  $$y=10+11(-1-k)=-1-11k$$

- Encuentra todas las soluciones de la ecuación $24x+33y=15$
- Para las siguientes ecuaciones, indica si tiene solución y (caso de tener) calcula todas las posibles soluciones
  - 12x + 18y = 48
  - 20x + 35y = 15
  - 16x + 28y = 22
  - 14x + 35 y = 21
- Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos; y la cajera, sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?
- ¿Es posible llenar exactamente un depósito de 25 litros con recipientes de 6 y 8 litros?
- Una persona va a un supermercado y compra 12 litros de leche, unos de leche entera y otros de desnatada, por 120 euros. Si la leche entera vale 3 euros más por litro que la desnatada, y ha comprado el mínimo posible de leche desnatada, ¿Cuántos litros habrá comprado de cada una?
- En una bolsa hay monedas de 10 y 20 céntimos y que su valor es 2 euros. ¿Qué combinaciones de monedas son posibles?

- Tenemos dos recipientes de agua con capacidad de 15 y 50 litros y con ellos queremos conseguir una cantidad de exactamente 85 litros. Calcula todas las formas de hacerlo
- En una fábrica se puede trabajar con bloques de 12 o 21 componentes (poniéndolos o quitándolos). Se quiere conseguir tener exactamente 27 componentes. Indica todas las posibles formas de hacerlo