Ejercicios Hoja 1

1. Encuentra el valor reducido de cada uno de los siguientes números en el correspondiente $\mathbb{Z}_n$

- 23, 13, 55, −5, −43, −17 en $\mathbb{Z}_4$
- 21, 19, 155, −3, −23, −11 en $\mathbb{Z}_3$
- 27, 11, 58, −5, −73, −13 en $\mathbb{Z}_{11}$

Soluc.

- En $\mathbb{Z}_4$ $\quad 23 = 5\cdot4+3 \equiv 3$, $13 = 3\cdot4+1 \equiv 1$, $-5 \equiv -1 \equiv 3$

  $-43 = (-10)\cdot4 - 3 \equiv -3 \equiv 1$, $-17 = -4\cdot4 - 1 \equiv -1 \equiv 3$
- En $\mathbb{Z}_3$ $\quad 21 = 3\cdot7+0 \equiv 0$, $19 = 6\cdot3+1 \equiv 1$, $155 = 51\cdot3+2 \equiv 2$

  $-3 = (-1)\cdot3+0 \equiv 0$, $-23 = -21-2 \equiv 0-2 \equiv -2 \equiv 1$

  $-11 = -3\cdot3 - 2 \equiv -2 \equiv 1$
- En $\mathbb{Z}_{11}$ $\quad 27 \equiv 2\cdot11+5 \equiv 5$, $11 \equiv 0$, $58 = 5\cdot11+3 \equiv 3$,

$-5 \equiv -11+6 \equiv 0+6 \equiv 6$, $-73 = -11\cdot7+4 \equiv 4$, $-13 = -11-2 \equiv -2 \equiv 9$.

2. Calcula $345\cdot43 + 122\cdot5 - 225$ en $\mathbb{Z}_5$, $\mathbb{Z}_8$ y $\mathbb{Z}_{11}$.

Solución.–

En $\mathbb{Z}_5$: $\quad 345\cdot43 + 122\cdot5 - 225 \equiv 0\cdot43 + 122\cdot0 - 0 \equiv 0$.

En $\mathbb{Z}_8$: $\quad 345\cdot43 + 122\cdot5 - 225 \equiv 1\cdot3 + 2\cdot5 - 1 \equiv 12 \equiv 4$.

En $\mathbb{Z}_{11}$: $\quad 345\cdot43 + 122\cdot5 - 225 \equiv 4\cdot10 + 1\cdot5 - 5 \equiv 40 \equiv 7$.

3. Calcula el máximo común divisor de los siguientes pares de números y expresálo en función de los mismos

- 402 y 31
- 824 y 205
- 412 y 102
- 213 y 66

Solución.

- $$\left(\begin{array}{c|cc} 402 & 1 & 0 \\ 31 & 0 & 1 \end{array}\right) \underset{E_{(1)-12(2)}}{\sim} \left(\begin{array}{c|cc} 30 & 1 & -12 \\ 31 & 0 & 1 \end{array}\right) \underset{E_{(2)-(1)}}{\sim} \left(\begin{array}{c|cc} 30 & 1 & -12 \\ 1 & -1 & 13 \end{array}\right)$$

$$\underset{E_{(1)-30(2)}}{\sim} \left(\begin{array}{c|cc} 0 & 31 & -402 \\ 1 & -1 & 13 \end{array}\right) \underset{E_{(1,2)}}{\sim} \left(\begin{array}{c|cc} 1 & -1 & 13 \\ 0 & 31 & -402 \end{array}\right)$$

$\mathrm{mcd}(402, 31) = 1$ y $402(-1) + 31\cdot13 = 1$.

- $\left(\begin{array}{c|cc} 824 & 1 & 0 \\ 205 & 0 & 1 \end{array}\right) \underset{E_{(1)-4(2)}}{\sim} \left(\begin{array}{c|cc} 4 & 1 & -4 \\ 205 & 0 & 1 \end{array}\right) \underset{E_{(2)-51(1)}}{\sim} \left(\begin{array}{c|cc} 4 & 1 & -4 \\ 1 & -51 & 205 \end{array}\right)$

$\underset{E_{(1)-4(2)}}{\sim} \left(\begin{array}{c|cc} 0 & 205 & -824 \\ 1 & -51 & 205 \end{array}\right) \underset{E_{(1,2)}}{\sim} \left(\begin{array}{c|cc} 1 & -51 & 205 \\ 0 & 205 & -824 \end{array}\right)$

$\text{mcd}(824,205)=1$ y $824(-51)+205(205)=1$

- $\left(\begin{array}{c|cc} 412 & 1 & 0 \\ 102 & 0 & 1 \end{array}\right) \underset{E_{(1)-4(2)}}{\sim} \left(\begin{array}{c|cc} 4 & 1 & -4 \\ 102 & 0 & 1 \end{array}\right) \underset{E_{(2)-25(1)}}{\sim} \left(\begin{array}{c|cc} 4 & 1 & -4 \\ 2 & -25 & 101 \end{array}\right)$

$\underset{E_{(1)-2(2)}}{\sim} \left(\begin{array}{c|cc} 0 & 51 & -206 \\ 2 & -25 & 101 \end{array}\right) \underset{E_{(1,2)}}{\sim} \left(\begin{array}{c|cc} 2 & -25 & 101 \\ 0 & 51 & -206 \end{array}\right)$

$\text{mcd}(412,102)=2$ y $412(-25)+102(101)=2$.

- $\text{mcd}(213,66)=3$ y $213(9)+66(-29)=3$

4. Para casa uno de los $\mathbb{Z}_n$ indicados estudia qué elementos son unidades y, para cada uno de ellos, calcula el inverso correspondiente.

   - 23, 13, 55, −5, −43, −17 en $\mathbb{Z}_8$
   - 21, 19, 155, −3, −23, −11 en $\mathbb{Z}_5$
   - 27, 11, 58, −5, −73, −13 en $\mathbb{Z}_{14}$

Solución:-

- En $\mathbb{Z}_8$:

  $23\equiv 7$, $\text{mcd}(7,8)=1$, existe $7^{-1}=7$

  $13\equiv 5$, $\text{mcd}(5,8)=1$, existe $5^{-1}=5$

  $55\equiv 7$, $7^{-1}=7$

  $-5\equiv 3$, $\text{mcd}(3,8)=1$, existe $3^{-1}=3$

  $-43\equiv 5$, $5^{-1}=5$

  $-17\equiv 4$, $\text{mcd}(4,8)\neq 1$, no existe 4^{-1} (en $\mathbb{Z}_8$)

- En $\mathbb{Z}_5$

$21\equiv 1$ $(1^{-1}=1)$, $19\equiv 4$ $(4^{-1}=4)$, $155\equiv 0$ (no existe 0^{-1})

$-3\equiv 2$ $(2^{-1}=2)$, $-23\equiv 3$ $(3^{-1}=3)$, $-11\equiv 4$ $(4^{-1}=4)$

- En $\mathbb{Z}_{14}$

$27\equiv 13$, $\text{mcd}(13,14)=1$, existe 13^{-1}: $13^{-1}=13$

$11\equiv 11$, $\text{mcd}(11,14)=1$, existe 11^{-1}: $11^{-1}=9$

$58 \equiv 2$, $\text{mcd}(2,14) \neq 1$, no existe 2^{-1}.

$-5 \equiv 9$, $\text{mcd}(9,14)=1$, existe 9^{-1} : $9^{-1} = 11$

$-73 \equiv -3 \equiv 11$, $11^{-1}=9$

$-13 \equiv 1$, $1^{-1}=1$

5. Para cada $\mathbb{Z}_n$ estudia qué elementos son unidades y, para los que lo sean, calcula su inverso

- $\mathbb{Z}_9$
- $\mathbb{Z}_{12}$
- $\mathbb{Z}_{18}$

Solución.-

- $\mathbb{Z}_9 = \{0,1,2,3,4,5,6,7,8\}$

números coprimos con 9 son: 1, 2, 4, 5, 7, 8

$1^{-1}=1$, $2^{-1}=5$, $4^{-1}=7$, $5^{-1}=2$, $7^{-1}=4$ y $8^{-1}=8$

- $\mathbb{Z}_{12} = \{0,1,\ldots,11\}$

Coprimos con $12 = 3\cdot 2^2$ son: 1, 5, 7, 11

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

- $\mathbb{Z}_{18} = \{0,1,2,\ldots,17\}$

Coprimos con $18 = 2\cdot 3^2$ son: 1, 5, 7, 11, 13, 17

$1^{-1}=1$, $5^{-1}=11$, $7^{-1}=13$, $11^{-1}=5$ $13^{-1}=7$, $17^{-1}=17$.

6. Calcula los siguientes inversos

- 11^{-1} en $\mathbb{Z}_{42}$
- 31^{-1} en $\mathbb{Z}_{100}$
- 13^{-1} en $\mathbb{Z}_{70}$

Solución.- • Hallamos $\text{mcd}(11,42)$.

$$\left(\begin{array}{c|cc} 42 & 1 & 0 \\ 11 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 5 & -19 \\ 0 & 11 & -42 \end{array}\right)$$

$\text{mcd}(11,42)=1$, luego existe 11^{-1} en $\mathbb{Z}_{42}$

De la relación

$$42\cdot 5 + 11\cdot(-19) = 1$$

Se tiene que $11\cdot(-19) \equiv 1 \pmod{42} \iff 11^{-1} = -19 \equiv 23$ en $\mathbb{Z}_{42}$

- Hallamamos mcd (31, 100)

$$\left(\begin{array}{c|cc} 31 & 1 & 0 \\ 100 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 71 & -22 \\ 0 & 100 & -31 \end{array}\right)$$

mcd (31,100) = 1 , luego existe 31^{-1} en $\mathbb{Z}_{100}$

De la relación $31 \cdot 71 + 100(-22) = 1$

Se tiene que $31 \cdot (71) \equiv 1 \pmod{100} \iff 31^{-1} = 71$ en $\mathbb{Z}_{100}$

- Hallamamos mcd (13, 70)

$$\left(\begin{array}{c|cc} 13 & 1 & 0 \\ 70 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 27 & -5 \\ 0 & 70 & -13 \end{array}\right)$$

mcd (13,70) = 1 , luego existe 13^{-1} en $\mathbb{Z}_{70}$

De la relación $13 \cdot 27 + 70(-5) = 1$

Se tiene que $13\,(27) \equiv 1 \pmod{70} \iff 13^{-1} = 27$ en $\mathbb{Z}_{70}$

7. Efectúa las operaciomes indicadas
   - $32 \cdot 21 - 12 \cdot 24^{-1}$ en $\mathbb{Z}_7$
   - $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4$ en $\mathbb{Z}_6$
   - $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4$ en $\mathbb{Z}_4$

Solución. En $\mathbb{Z}_7$, $32 \cdot 21 - 12 \cdot 24^{-1} \equiv 4 \cdot 0 - 5 \cdot 3^{-1} \equiv -5 \cdot 5 \equiv -25 \equiv 3.$

En $\mathbb{Z}_6$, $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4 \equiv 5 + 0 \cdot 11^{-1} + 1 \cdot 4^4 \equiv 5 + 4 \equiv 3.$

En $\mathbb{Z}_4$, $23 + 12 \cdot 11^{-1} + 43 \cdot 10^4 \equiv 3 + 0 \cdot 11^{-1} + 3 \cdot 2^4 \equiv 3 + 3 \cdot 0 \equiv 3.$

8. Calcula 6^{-1} y 11^{-1} en $\mathbb{Z}_{15}$ usando el valor de $\varphi(15)$.

Solución. $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = (3-1)(5-1) = 2 \cdot 4 = 8$

mcd(6,15) = 3 , luego no existe el inverso de 6 en $\mathbb{Z}_{15}$

mcd(11,15) = 1 , luego existe 11^{-1} en $\mathbb{Z}_{15}$ y

$$11^{-1} \equiv 11^{\varphi(15)-1} \equiv 11^7 = (11^2)^3 \cdot 11 \equiv 1^3 \cdot 11 = 11$$

$(11^2 = 121 \equiv 8 \cdot 15 + 1 \equiv 1)$

9. Calcula 5^{-1} y 13^{-1} en $\mathbb{Z}_{48}$ usando el valor de $\varphi(48)$.

Solución.- $\varphi(48) = \varphi(3 \cdot 2^4) = \varphi(3) \cdot \varphi(2^4) = (3-1)(2^4 - 2^3) = 16$

$mcd(5,48) = 1$, luego existe 5^{-1} en $\mathbb{Z}_{48}$

$$5^{-1} \equiv 5^{\varphi(48)-1} = 5^{15} = (5^3)^5 \equiv 29^5 \equiv (29^2)^2 \cdot 29 \equiv 25^2 \cdot 29$$
$$\equiv 1 \cdot 29 \equiv 29.$$

$(5^3 = 125 \equiv 29 \quad , \quad 29^2 \equiv 25 \quad , \quad 25^2 = 1)$

$mcd(13,48) = 1$, existe 13^{-1} en $\mathbb{Z}_{48}$

$$13^{-1} \equiv 13^{\varphi(48)-1} \equiv 13^{15} \equiv (13^2)^7 \cdot 13 \equiv 25^7 \cdot 13 \equiv (25^2)^3 \cdot 25 \cdot 13$$
$$\equiv 1 \cdot 25 \cdot 13 \equiv 37.$$

$(13^2 \equiv 25 \quad , \quad 25 \cdot 13 \equiv 37 \quad)$

10. Calcular las dos últimas cifras de 1237^{121} (*Indicación:* calcula esta potencia en $\mathbb{Z}_{100}$ usando $\varphi(100)$)

Solución.-

1ª forma: Las dos últimas cifras de un número es el resto de dividir dicho número entre 100.

Hallemos pues 1237^{121} en $\mathbb{Z}_{100}$.

$$1237 \equiv 37 \pmod{100} \Rightarrow 1237^{121} \equiv 37^{121} \pmod{100}$$

Tenemos $37^2 = 1369 \equiv 69 \pmod{100}$, luego

$$37^{121} = 37^{2 \cdot 60 + 1} = (37^2)^{60} \cdot 37 \equiv (69)^{60} \cdot 37 \pmod{100}$$

$69^2 = 4761 \equiv 61 \pmod{100}$, luego

$$69^{60} \cdot 37 = (69^2)^{30} \cdot 37 \equiv 61^{30} \cdot 37 \pmod{100}$$

(*) $61^2 = 3721 \equiv 21 \pmod{100}$, luego

$$61^{30} \cdot 37 = (61^2)^{15} \cdot 37 \equiv 21^{15} \cdot 37 \pmod{100}$$

$21^3 = 9261 \equiv 61 \pmod{100}$, luego

$$21^{15}\cdot 37 = (21^3)^5 \cdot 37 \equiv 61^5 \cdot 37 \pmod{100}$$

$$= 61^2\cdot 61^2 \cdot 61 \cdot 37 \pmod{100}$$

$$\underset{(*)}{\equiv} 21\cdot 21\cdot 61\cdot 37 \pmod{100}$$

$$= 995.337 \pmod{100}$$

$$\equiv 37 \pmod{100}$$

La dos últimas cifras son 37.

<u>2ª forma</u> Si $\mathrm{mcd}(a,n)=1$, $a^{\varphi(n)} \equiv 1 \pmod n$

Como $\mathrm{mcd}(1237, 100) = 1$ (fácil de ver)

$$1237^{\varphi(100)} = 1237^{40} \equiv 1 \pmod{100}$$

Por tanto $1237^{121} = 1237^{3\cdot 40+1} = (1237^{40})^{30}\cdot 1237$

$$\equiv 1^{30}\cdot 1237 \pmod{100}$$

$$\equiv 1237 \pmod{100}$$

$$\equiv 37 \pmod{100}$$

11. Para las siguientes ecuaciones, indica si tiene solución y (caso de tener) calcula todas las posibles soluciones

- $12x + 18y = 48$
- $20x + 35y = 15$
- $16x + 28y = 22$
- $14x + 35y = 21$

<u>Solución</u>.- a) Hecho en teoría

b)

```
A=matrix(ZZ,[20,35])
AB=block_matrix([[A.T,1]])
show(AB)
```

$$\left(\begin{array}{c|cc} 20 & 1 & 0 \\ 35 & 0 & 1 \end{array}\right)$$

```
C=AB.echelon_form()
show(C)
```

$$\begin{pmatrix} 5 & 2 & -1 \\ 0 & 7 & -4 \end{pmatrix}$$

Tenemos
$$\begin{bmatrix} 2 & -1 \\ 7 & -4 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 35 \end{bmatrix} = \begin{bmatrix} 5 \\ 0 \end{bmatrix}$$

$$\begin{array}{l} 20 \cdot \overbrace{(2) \cdot 3}^{x_0} + 35 \cdot \overbrace{(-1)}^{y_0} \cdot 3 = 5 \cdot 3 = 15 \\ 20 \cdot (7) \cdot t + 35(-4) t = 0 \quad \forall t \in \mathbb{Z} \\ \hline 20(6 + 7t) + 35(-3 - 4t) = 15 \end{array}$$

La solución general sería
$$\left. \begin{array}{l} x = 6 + 7t \\ y = -3 - 4t \end{array} \right\} \quad \forall t \in \mathbb{Z}$$

12. Un coleccionista de obras de arte ha adquirido varias obras entre pinturas y dibujos. Las pinturas le han costado 210 euros cada una y los dibujos 120 euros. Cuando el coleccionista llega a casa, no sabe si se ha gastado 2700 euros o 2600 euros. ¿ Pueden haberle costado 2600 euros ?. ¿ Cuántos cuadros y dibujos ha comprado ?.

Solución: Hecho en teoría

13. 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 ?.

Solución: Si x es el número de billetes de 3 rublos e y el número de los de 5 rublos, se tiene
$$3x + 5y = 19$$

Cuya solución es:
$$\left(\begin{array}{c|cc} 5 & 1 & 0 \\ 3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} -1 & 1 & -2 \\ 3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} -1 & 1 & -2 \\ 0 & 3 & -5 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & -1 & 2 \\ 0 & 3 & -5 \end{array}\right)$$

$$\begin{pmatrix} -1 & 2 \\ 3 & -5 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \iff \begin{array}{l} 3 \cdot 2 + 5(-1) = 1 \\ 3(-5) + 5 \cdot 3 = 0 \end{array}$$

$$\begin{array}{l} 3 \cdot 2 \cdot 19 + 5(-1) 19 = 19 \\ 3(-5) t + 5 \cdot 3 \cdot t = 0 \quad \forall t \in \mathbb{Z} \\ \hline \end{array}$$

$$3(\underbrace{38-5t}_{x}) + 5(\underbrace{-19+3t}_{y}) = 19 \quad \forall t \in \mathbb{Z}$$

Solución:

$$x = 38 - 5t$$
$$y = -19 + 3t \qquad t \in \mathbb{Z}.$$

Como el valor del nº de billetes x a entregar ha ser mayor o igual que 19 (precio de la bufanda), entonces $3x \geq 19$, es decir $x \geq 7$. Así pues

$$38 - 5t \geq 7 \iff t \leq \frac{31}{5} = 6'2.$$

Tomamos $t = 6$

$x = 8$ (entregamos 8 billetes de 3)

$y = -1$ (nos devuelven 1 de 5)

14. En una bolsa hay monedas de 10 y 20 céntimos y que su valor es 2 euros. ¿Que combinaciones de monedas son posible ?.

Solución- Sea x el número de monedas de 10 céntimos e y el número de monedas de 20 céntimos.

Entonces
$$10 \cdot x + 20y = 200.$$

es decir
$$x + 2y = 20$$

$$\left(\begin{array}{c|cc} 1 & 1 & 0 \\ 2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 0 & -2 & 1 \end{array}\right) \text{,} \quad \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{,} \quad \left.\begin{array}{l} 1 \cdot 1 + 2 \cdot 0 = 1 \\ 1(-2) + 2 \cdot 1 = 0 \end{array}\right\}$$

$$\begin{array}{l} 1 \cdot 1 \cdot 20 + 2 \cdot 0 \cdot 20 = 20 \\ 1 \cdot (-2)t + 2 \cdot 1 \cdot t = 0 \quad \forall t \\ \hline 1(\underbrace{20 - 2t}_{x}) + 2 \cdot \underbrace{t}_{y} = 20 \quad \forall t \end{array}$$

$$\left.\begin{array}{l} x = 20 - 2t \\ y = t \end{array}\right\} t \in \mathbb{Z}.$$

El número máximo de monedas de 20 serían 10. y mínimo 1 luego $1 \leq t < 10$ (se supone que hay monedas de ambos valores). Así para:

$$t = 1 \longrightarrow \left\{\begin{array}{l} x = 18 \\ y = 1 \end{array}\right. \qquad t = 2 \longrightarrow \left\{\begin{array}{l} x = 16 \\ y = 2 \end{array}\right.$$

$$\ldots \qquad t = 9 \longrightarrow \left\{\begin{array}{l} x = 2 \\ y = 9 \end{array}\right. .$$

15. ¿Es posible llenar exactamente un depósito de 25 litros con recipientes de 6 y 8 litros ?.

Solución.- Se trata de resolver la ecuación diofántica

$$6x+8y=25.$$

Como $mcd(6,8)=2$ y $2 \nmid 25$, el problema no tiene solución.

16. 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 ?.

Solución:- Sea x el nº de litros de leche entera e y el nº de litros de leche desnatada

Se tiene $x+y=12 \quad (*)$

Si llamamos k al valor del litro de desnatada, entonces un litro de entera valdrá $k+3$. Por tanto

$$(k+3)x+ky=120 \quad (**)$$

Despejamos y de $(*)$ y sustituimos en $(**)$

$$(k+3)x+k(12-x)=120$$

$$\Longleftrightarrow \quad 3x+12k=120$$

$$\Longleftrightarrow \quad x+4k=40.$$

Resolvemos la ec. diofántica, teniendo

$$\left(\begin{array}{c|cc} 1 & 1 & 0 \\ 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 0 \\ 0 & -4 & 1 \end{array}\right) \;\; " \;\; \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;\; " \;\; \left.\begin{array}{l} 1\cdot 1-4\cdot 0=1 \\ 1\cdot(-4)+4\cdot 1=0 \end{array}\right\}$$

$$\begin{array}{ll} 1\cdot 1\cdot 40-4\cdot 0\cdot 40=40 & \\ 1\cdot(-4)\cdot t-4\cdot 1\cdot t=0 & \forall t\in\mathbb{Z} \\ \hline 1(\underbrace{40-4t}_{x})-4\cdot \underbrace{t}_{k}=40 & \forall t\in\mathbb{Z}. \end{array}$$

Solución:

$$\left.\begin{array}{l} x=40-4t \\ k=t \end{array}\right\} \quad t\in\mathbb{Z}.$$

Como se compran ambos tipos de leche, debe suceder que $x=40-4t<12$ es decir $t>7$

Para $t=8$, $x=8$ e $y=12$ (y el litro de desnatada $=8$ euros)

LADRONES

17. 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.

Soluc Sea n uno de dichos números. Se tiene

$$n \equiv 0 \ (\text{mód } 3)$$
$$n \equiv 1 \ (\text{mód } 2)$$
$$3n \equiv 2 \ (\text{mód } 5)$$

Nos piden calcular dichos números.

Cogemos la 2ª y 3ª ecuación:

$$n = 1 + 2x \qquad x, y \in \mathbb{Z}.$$
$$3n = 2 + 5y$$

Hacemos la 1ª por 3 y restamos ambas igualdades

$$\begin{array}{rl} & 3n = 3 + 6x \\ - & 3n = 2 + 5y \\ \hline & 0 = (3+6x) - (2+5y) \end{array}$$

es decir

$$6x - 5y = -1$$

$$\left(\begin{array}{c|cc} 6 & 1 & 0 \\ -5 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 1 \\ -5 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 1 \\ 0 & 5 & 6 \end{array}\right)$$

$$\begin{pmatrix} 1 & 1 \\ 5 & 6 \end{pmatrix}\begin{pmatrix} 6 \\ -5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow 6 \cdot 1 - 5 \cdot 1 = 1$$

$$\begin{array}{l} 6 \cdot 1 \cdot (-1) - 5 \cdot 1 \cdot (-1) = 1 \cdot (-1) = -1 \\ 6 \cdot 5 \cdot t - 5 \cdot 6 \cdot t = 0 \quad \forall t \\ \hline 6(\underbrace{-1+5t}_{x}) - 5(\underbrace{-1+6t}_{y}) = -1 \end{array}$$

Sustituimos $x = -1 + 5t$ en la ecuación

$n = 1 + 2x$ y tenemos

$$n = 1 + 2x = 1 + 2(-1+5t) = -1 + 10t$$

es decir $\quad n \equiv -1 \ (\text{mod } 10) \equiv 9 \ (\text{mod } 10)$

Esta congruencia con la 1ª es

$$n \equiv 0 \ (\text{mód } 3) \iff n = 3x$$
$$n \equiv 9 \ (\text{mód } 10) \iff n = 9 + 10y \qquad x, y \in \mathbb{Z}$$

es decir

$$3x = 9 + 10y$$

$$\iff 3x - 10y = 9$$

$$\left(\begin{array}{c|cc} 3 & 1 & 0 \\ -10 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 3 & 1 & 0 \\ -1 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 0 & 10 & 3 \\ -1 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & -3 & -1 \\ 0 & 10 & 3 \end{array}\right)$$

$$\begin{pmatrix} -3 & -1 \\ 10 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ -10 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\iff \quad 3(-3) \cdot 9 - 10(-1) \cdot 9 = 1 \cdot 9 = 9$$
$$3 \cdot 10 \cdot t - 10 \cdot 3 \cdot t = 0 \quad \forall t \in \mathbb{Z}$$

$$3(\underbrace{-27 + 10t}_{x}) - 10(\underbrace{-9 + 3t}_{y}) = 9$$

Sustituimos $x = -27 + 10t$, en $n = 3x$

$$n = 3(-27 + 10t) = -81 + 30t$$

e.d. $n \equiv -81 \ (\text{mod } 30) \equiv 9 \ (\text{mód } 30)$

Los números son de la forma $9 + 30t \quad \forall t \in \mathbb{Z}$

Para $t = 0$ $n = 9$ y 9 cumple las 3 congruencias

Para $t = 1$ $n = 39$ y 39 también las cumple.

18. 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.

Soluc. Sea n el nº de soldados. Entonces

$$\left.\begin{array}{r} n \equiv 2 \ (\text{mód } 11) \\ n - 10 \equiv 3 \ (\text{mód } 9) \\ n - 6 \equiv 1 \ (\text{mód } 25) \end{array}\right\}$$

Lo que es equivalente a:

$$\left.\begin{array}{l} n \equiv 2 \pmod{11} \\ n \equiv 13 \pmod 9 \equiv 4 \pmod 9 \\ n \equiv 7 \pmod{25} \end{array}\right\}$$

Se trabaja como el ejercicio anterior

- De otra forma distinta

De $n \equiv 2 \pmod{11} \iff n = 2 + 11\cdot k \quad k \in \mathbb{Z}$. $(*)$

Sustituimos en la 2ª ec.

$$\overbrace{2+11\cdot k}^{n} \equiv 4 \pmod 9$$

$$\iff 11\cdot k \equiv 2 \pmod 9$$

$$\overset{11=2}{\iff} 2\cdot k \equiv 2 \pmod 9$$

$$\iff \underbrace{2^{-1}}_{\substack{\shortparallel \\ (5 \text{ en } \mathbb{Z}_9)}} \cdot 2\cdot k \equiv 2 \pmod 9$$

$$\iff k \equiv 2\cdot 5 \pmod 9 \equiv 1 \pmod 9$$

es decir $\quad k = 1 + 9\cdot t \quad$ para $t \in \mathbb{Z}$

Sustituimos k en $(*)$, tendremos

$$n = 2 + 11\cdot k = 2 + 11(1+9t) = 13 + 99t \qquad (**)$$

Sustituimos el valor de n en la última ecuación:

$$13 + 99t \equiv 7 \pmod{25}$$

$$\iff 99t \equiv -6 \pmod{25}$$

$$\overset{99=24}{\iff} 24t \equiv 19 \pmod{25}$$

$$\iff 24^{-1}\cdot 24t \equiv 19 \pmod{25}$$

Debemos hallar el inverso de 24 en $\mathbb{Z}_{25}$

$$\left(\begin{array}{c|cc} 25 & 1 & 0 \\ 24 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & -1 \\ 24 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & -1 \\ 0 & -24 & 25 \end{array}\right)$$

$$\begin{pmatrix} 1 & -1 \\ -24 & 25 \end{pmatrix}\begin{pmatrix} 25 \\ 24 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow 25\cdot 1 + 24\cdot(-1) = 1$$

luego en $\mathbb{Z}_{25}$ $\quad 24\cdot(-1) \equiv 1$

es decir $24^{-1} \equiv -1 \equiv 24$.

Volviendo a nuestra ecuación

$$24^{-1}\cdot 24t \equiv 19 \pmod{25}$$
$$\Rightarrow \quad t \equiv 24\cdot 19 \pmod{25}$$
$$\equiv 6 \pmod{25}$$

e.d $\quad t = 6 + 25\cdot s \quad$ para $s \in \mathbb{Z}$.

Sustituyendo este valor de t en $(**)$ tendremos

$$n = 13 + 99t = 13 + 99(6 + 25s)$$
$$= 607 + (\underbrace{11\cdot 9\cdot 25}_{2475})s$$

Comprobación: Solo compruebo que 607 es solución particular del sistema de congruencias:

$$607 = 11\cdot 55 + 2 \quad \Rightarrow \quad 607 \equiv 2 \pmod{11}$$
$$607 = 9\cdot 67 + 4 \quad \Rightarrow \quad 607 \equiv 4 \pmod{9}$$
$$607 = 25\cdot 24 + 7 \quad \Rightarrow \quad 607 \equiv 7 \pmod{25}$$

19. De un cierto número se sabe que al dividirlo por 7 el resto es 3. El resto al dividir el doble de ese número por 11 es 5 y el número es múltiplo de 4. ¿Cuánto puede valer ese número ?.

Solución.- Sea n dicho número. Entonces

$$\left.\begin{array}{r} n \equiv 3 \pmod{7} \\ 2n \equiv 5 \pmod{11} \\ n \equiv 0 \pmod{4} \end{array}\right\}$$

o equivalentemente

$$\left.\begin{array}{r} n \equiv 3 \pmod{7} \\ n \equiv 8 \pmod{11} \\ n \equiv 0 \pmod{4} \end{array}\right\}$$

donde en la segunda congruencia se ha multiplicado por el inverso del 2 en $\mathbb{Z}_{11}$ que es: 6

$$(6\cdot 2n \equiv 6\cdot 5 \pmod{11} \Leftrightarrow n \equiv 30 \pmod{11} \Leftrightarrow n \equiv 8 \pmod{11})$$

Tomamos la 2ª y 3ª congruencia, entonces

$$\left.\begin{array}{l} n = 3 + 7x \\ n = 8 + 11y \end{array}\right\} \quad x, y \in \mathbb{Z}$$

De donde se obtiene la ec. diofántica

$$7x - 11y = 5 \qquad x,y \in \mathbb{Z}.$$

$$\left(\begin{array}{c|cc} 7 & 1 & 0 \\ -11 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 7 & 1 & 0 \\ 3 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & -3 & -2 \\ 3 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & -3 & -2 \\ 0 & 11 & 7 \end{array}\right)$$

$$\begin{pmatrix} -3 & -2 \\ 11 & 7 \end{pmatrix}\begin{pmatrix} 7 \\ -11 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \Longleftrightarrow \quad \left.\begin{array}{l} 7(-3) - 11(-2) = 1 \\ 7(11) - 11(7) = 0 \end{array}\right\}$$

$$\begin{array}{l} 7\cdot(-3)\cdot 5 - 11\cdot(-2)\cdot 5 = 5 \\ 7\,(11)\cdot t - 11\cdot(7)\cdot t = 0 \qquad \forall t \in \mathbb{Z} \\ \hline 7\,(\underbrace{-15+11t}_{x}) - 11\,(\underbrace{-10+7t}_{y}) = 5 \end{array}$$

Sustituimos $x = -15 + 11t$ en la ecuación $n = 3 + 7x$ teniendo

$$n = 3 + 7x = 3 + 7(-15 + 11t) = -102 + 77t.$$

es decir $\quad n \equiv -102 \pmod{77} \equiv 52 \pmod{77}$

Esta congruencia con la tercera, sería

$$\begin{array}{l} n \equiv 52 \pmod{77} \\ n \equiv 0 \pmod{4} \end{array} \quad \Longleftrightarrow \quad \left\{\begin{array}{l} n = 52 + 77x \\ n = 4y \end{array}\right. \quad x,y \in \mathbb{Z}$$

es decir $\quad 77x - 4y = -52 \qquad x,y \in \mathbb{Z}.$

$$\left(\begin{array}{c|cc} 77 & 1 & 0 \\ -4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 5 & 1 & 18 \\ -4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 19 \\ -4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{c|cc} 1 & 1 & 19 \\ 0 & 4 & 77 \end{array}\right)$$

$$\begin{pmatrix} 1 & 19 \\ 4 & 77 \end{pmatrix}\begin{pmatrix} 77 \\ -4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Longleftrightarrow \left.\begin{array}{l} 77\cdot 1 - 4\cdot 19 = 1 \\ 77\cdot 4 - 4\cdot 77 = 0 \end{array}\right\}$$

$$\begin{array}{l} 77\cdot 1\cdot(-52) - 4\cdot 19(-52) = -52 \\ 77\cdot 4\cdot t - 4\cdot 77\cdot t = 0 \qquad \forall t \in \mathbb{Z} \\ \hline 77\,(\underbrace{-52+4t}_{x}) - 4\cdot(\underbrace{-988+77t}_{y}) = -52 \qquad \forall t \in \mathbb{Z} \end{array}$$

Sustituyendo $x = -52 + 4t$ en la ecuación $n = 52 + 77x$ tenemos

$$n = 52 + 77(-52 + 4t) = -3952 + 308t \equiv 52 + 308t.$$

20. Encuentra todas las soluciones de los siguientes sistemas de ecuaciones lineales pasando la matriz del sistema a forma reducida

- $\left.\begin{array}{rcl} 3x+2y+z &=& 1 \\ 5x+y+2z &=& 2 \end{array}\right\}$ en $\mathbb{Z}_7$, $\left.\begin{array}{rcl} x-y+z+t &=& 1 \\ 2x+y-t &=& 2 \\ y-z+2t &=& 0 \\ 3x+y+z+t &=& 3 \end{array}\right\}$ en $\mathbb{Z}_5$
- $\left.\begin{array}{rcl} 2x-y+z+t &=& 1 \\ 2x+y-t &=& 2 \\ y+2z+3t &=& 0 \end{array}\right\}$ en $\mathbb{Z}_{11}$, $\left.\begin{array}{rcl} 2x+4z &=& 0 \\ -x-z &=& 3 \\ 2x+y+5z &=& -4 \end{array}\right\}$ en $\mathbb{Z}_5$
- $\left.\begin{array}{rcl} x+2z+5t &=& 2 \\ y-3z &=& 1 \end{array}\right\}$ en $\mathbb{R}$, $\left.\begin{array}{rcl} 2x+y+z+t &=& 4 \\ z+4t &=& 2 \end{array}\right\}$ en $\mathbb{Z}_{11}$
- $\left.\begin{array}{rcl} 3x+2z+5t &=& 2 \\ y-3z &=& 1 \\ 4z &=& 12 \end{array}\right\}$ en $\mathbb{R}$, $\left.\begin{array}{rcl} 3x+y+3z+5t+2u &=& 3 \\ 3z+3t+u &=& 1 \\ 4u &=& 12 \end{array}\right\}$ en $\mathbb{Z}_7$
- $\left.\begin{array}{rcl} x+y+z+t &=& 1 \\ x+y+3z+4t &=& 2 \\ x+y+5z+7t &=& 3 \end{array}\right\}$ en $\mathbb{Z}_7$, $\left.\begin{array}{rcl} 2x+y &=& 4 \\ 3x+z &=& 2 \end{array}\right\}$ en $\mathbb{Z}_5$
- $\left.\begin{array}{rcl} x-y+z+t &=& 1 \\ 2x+y-t &=& 2 \\ y-2z+t &=& 0 \\ 3x+y+z+t &=& 3 \end{array}\right\}$ en $\mathbb{R}$, $\left.\begin{array}{rcl} 2x-y+z+t &=& 1 \\ 2x+y-t &=& 2 \\ y+2z+3t &=& 0 \end{array}\right\}$ en $\mathbb{Z}_5$
- $\left.\begin{array}{rcl} -x-5z+v &=& -1 \\ 3x+y+z+u &=& 0 \\ -2x+t &=& 3 \end{array}\right\}$ en $\mathbb{R}$, $\left.\begin{array}{l} 3x+y-z \;=\; 2 \\ 2x+z+u \;=\; 1 \\ x+t=7 \end{array}\right\}$ en $\mathbb{Z}_7$

Solución.-

$$\left.\begin{array}{rcl} -x-5z+v &=& -1 \\ 3x+y+z+u &=& 0 \\ -2x+t &=& 3 \end{array}\right\} \text{ en } \mathbb{R}.$$

Matriz ampliada

$$\left(\begin{array}{cccccc|c} -1 & 0 & -5 & 0 & 1 & 0 & -1 \\ 3 & 1 & 1 & 1 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 & 3 \end{array}\right)$$

El nº máximo de pivotes será 3: coinciden con las columnas 2ª (o 4ª), la 5ª y 6ª. Correspondientes a las variables: y, u y v

Solución:

$$\left.\begin{array}{l} x = a \\ y = -3a-b-c \\ z = b \\ t = c \\ u = -1+a+5b \\ v = 3+2a \end{array}\right\} \quad a,b,c\in\mathbb{R}$$

21. Encuentra la forma reducida de cada una de las siguientes matrices:

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

22. Encuentra cuando sea posible las inversas de las siguientes matrices

- $\begin{pmatrix} 2 & 3 & 1 \\ 1 & 4 & 3 \\ 2 & 5 & 1 \end{pmatrix}$ en $\mathbb{Z}_2$
- $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ en $\mathbb{Z}_7$
- $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 0 \\ 3 & 0 & 0 \end{pmatrix}$ en $\mathbb{Z}_5$