



irenegallegoskh

[www.wuolah.com/student/irenegallegoskh](http://www.wuolah.com/student/irenegallegoskh)

6813

## Tema-2.pdf

Tema 2



1º Álgebra Lineal y Estructuras Matemáticas



Grado en Ingeniería Informática



Escuela Técnica Superior de Ingenierías Informática y de  
Telecomunicación  
Universidad de Granada

**WUOLAH + #QuédateEnCasa**

#KeepCalm #EstudiaUnPoquito

Enhorabuena, por ponerte a estudiar te **regalamos un cartel**  
incluído entre estos apuntes para estos días.

## Tema 2: ARITMÉTICA ENTERA Y MODULAR

Sea  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ . Sobre el conjunto  $\mathbb{Z}$  hay una operación suma que verifica las siguientes propiedades:

1. Asociativa.  $a+b+c \rightarrow (a+b)+c = a+(b+c)$

2. Comutativa.  $a+b = b+a$

3. Elemento neutro.  $a+0 = a \quad \forall a \in \mathbb{Z}$

4. Elemento inverso.  $x+(-x) = 0$

5. Cancelativa. Si  $a+c=b+c \Rightarrow a=b$

En  $\mathbb{Z}$  hay también una operación producto que verifica las siguientes propiedades:

1. Asociativa.  $a(bc) = (ab)c$

2. Comutativa.  $ab = b \cdot a$

3. Elemento neutro.  $a \cdot 1 = a \quad \forall a \in \mathbb{Z}$

4. Cancelativa por elementos  $\neq 0$ : si  $ac=bc$  y  $c \neq 0 \Rightarrow a=b$

5. Distributiva.  $a(b+c) = ab+ac$

Propiedad de la división:

Si  $a, b \in \mathbb{Z}$  y  $b \neq 0 \Rightarrow \exists$  unos únicos  $g, r \in \mathbb{Z}$  tg

$a = gb+r$  y  $0 \leq r < |b|$

A los n°  $g$  y  $r$  los llamaremos el cociente y el resto de dividir  $a$  entre  $b$  y los denotaremos  $a \text{ div } b$  y  $a \text{ mod } b$  respectivamente.

Ejercicio. Calcular  $123 \text{ div } 9$  y  $123 \text{ mod } 9$ .

$$\begin{array}{r} 123 \\ \underline{\quad 9} \\ 33 \end{array}$$

$$123 \text{ div } 9 = 13$$

$$33 \quad 13$$

$$123 \text{ mod } 9 = 6$$

$$6$$

Ejercicio. Calcular  $(-123) \text{ div } 9$  y  $(-123) \text{ mod } 9$

$$123 = -13 \cdot 9 + 6$$

$$-123 \text{ div } 9 = -14$$

$$-123 = (-13) \cdot 9 - 6$$

$$-123 \text{ mod } 9 = 3$$

$$-123 = (-14) \cdot 9 + 3$$



Formación  
Manuel  
Pozo

# ACADEMIA UNIVERSITARIA MP

Academia especializada en grados universitarios.  
Cursos intensivos y clases particulares.

Profesores especializados en más de 150 asignaturas.  
Consulta todas tus asignaturas.

Matemáticas

Química

Física

Biolología

Bioquímica

Ambientales

Geología

Óptica

Estadística

Tecnología

Farmacia

Nutrición

Ingeniería

Economía

Medicina

Odontología

Psicología

Magisterio.

[www.formacionmanuelpozo.com](http://www.formacionmanuelpozo.com)

615 14 96 76

Granada

Ejercicio. Calcular:

$$(-137) \text{ div } 5 = -28$$

$$(-137) \text{ mod } 5 = 3$$

$$137 = 27 \cdot 5 + 2$$

$$\begin{array}{r} 137 \\ 37 \quad | \quad 5 \\ 27 \\ 2 \end{array} \quad \begin{array}{l} -137 = (-27)5 - 2 \\ -137 = (-27)5 - 5 + 5 - 2 \\ -137 = (-28)5 + 3 \end{array}$$

Sean  $a, b \in \mathbb{Z}$  diremos que  $a$  divide a  $b$  (que  $a$  es un divisor de  $b$ ) (que  $b$  es un múltiplo de  $a$ ) y lo denotaremos  $a|b$  si  $\exists c \in \mathbb{Z}$  tg  $b = a \cdot c$

Ejemplo.  $2|6$   $2|9$

Un número  $p \in \mathbb{Z} \setminus \{-1, -1\}$  diremos que es primo si los únicos enteros que lo dividen son  $1, -1, p, -p$ .

Ejemplos:  $2, -2, 3, -3, 5, -5, 7, -7, 11, -11, \dots$

Dos números enteros son primos relativos si los únicos divisores que tienen en común son el  $1$  y  $-1$ .

Ejemplos:  $14$  y  $25$ .

### Teorema de Bezout

Sean  $a, b \in \mathbb{Z} \Rightarrow a$  y  $b$  son primos relativos si solamente si  $\exists u, v \in \mathbb{Z}$  tg  $au + bv = 1$

Ejercicio. ¿Tiene la ecuación  $14x + 9y = 1$  solución en  $\mathbb{Z}$ ?

(La ecuación tiene solución en  $\mathbb{Z}$  si solamente si  $\exists u, v \in \mathbb{Z}$

tg  $14u + 9v = 1$ . Pero por el T<sup>a</sup> de Bezout sabemos que esto ocurre si solamente si  $14$  y  $9$  son primos relativos, como  $14$  y  $9$  son primos relativos  $\Rightarrow$  la ecuación tiene solución en  $\mathbb{Z}$ .

### Teorema fundamental de la aritmética.

Todo n° entero  $\geq 2$  se puede poner de forma única (salvo reordenaciones) como producto de n° primos positivos.

Ejercicio. Calcular la descomposición en primos de  $360$

$$\begin{array}{r} 360 \\ 180 \\ 90 \\ 45 \\ 15 \\ 5 \\ 1 \end{array} \quad \begin{array}{l} | \quad 2 \\ | \quad 2 \\ | \quad 2 \\ | \quad 3 \\ | \quad 3 \\ | \quad 5 \end{array} \quad 360 = 2^3 \cdot 3^2 \cdot 5$$

## Corolario

Si  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}$  es la descomposición en primos de un entero positivo  $n \Rightarrow (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_r+1)$  es el número de divisores positivos que tiene el número  $n$ .

Ejercicio. ¿Cuántos divisores tiene el número 360?

Sabemos que  $360 = 2^3 \cdot 3^2 \cdot 5^1$  por tanto  $(3+1)(2+1)(1+1) = 24$  es el número de divisores positivos de 360, en consecuencia, 360 tiene 48 divisores (24 positivos y 24 negativos)

Sean  $a, b \in \mathbb{Z}$  tg  $a \neq 0$  ó  $b \neq 0$  un entero d diremos que es un máximo común divisor de a y b si verifica que:

1.  $d | a$  y  $d | b$
2. si  $c | a$  y  $c | b$  entonces  $c | d$ .

Nota: si d es m.c.d. de a y b  $\Rightarrow -d$  es también un m.c.d de a y b.

Denotaremos  $m.c.d(a, b)$  al máximo común divisor de a y b que es positivo.

$$m.c.d(6, 84) = 2$$

$$m.c.d(10, 54) = 5$$

$$\cancel{m.c.d(10, 0)}$$

Sean  $a, b \in \mathbb{Z}$  un n° entero m diremos que es un mínimo común múltiplo de a y b si verifica que:

1.  $a | m$  y  $b | m$

2. Si  $a | c$  y  $b | c$  entonces  $m | c$

Nota: si m es un m.c.m de a y b  $\Rightarrow -m$  es también un m.c.m de a y b.

Denotaremos  $m.c.m(a, b)$  al mínimo común múltiplo de a y b que es  $\geq 0$ .

$$m.c.m(4, 6) = 12$$

$$m.c.m(0, 0) = 0$$

$$m.c.m(10, 5) = 0$$



Proposición: si  $a, b \in \mathbb{Z} \setminus \{0\}$  entonces:

$$1. \text{m.c.d } \{a, b\} = \text{m.c.d } \{|a|, |b|\}$$

$$2. \text{m.c.m } \{a, b\} = \text{m.c.m } \{|a|, |b|\}$$

### Teorema

Si  $P_1, P_2, \dots, P_r$  son números primos positivos y

$\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_r \in \mathbb{N}$ , entonces:

$$1. \text{m.c.d } \{P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_r^{\alpha_r}, P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_r^{\beta_r}\} = \\ = P_1^{\min\{\alpha_1, \beta_1\}} \cdot P_2^{\min\{\alpha_2, \beta_2\}} \cdot \dots \cdot P_r^{\min\{\alpha_r, \beta_r\}}$$

$$2. \text{m.c.m } \{P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_r^{\alpha_r}, P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_r^{\beta_r}\} = \\ = P_1^{\max\{\alpha_1, \beta_1\}} \cdot P_2^{\max\{\alpha_2, \beta_2\}} \cdot \dots \cdot P_r^{\max\{\alpha_r, \beta_r\}}$$

Ejercicio. Calcular el m.c.d y m.c.m de 120 y 231.

120	2
60	2
30	2
15	3
5	5
1	

231	3
77	7
11	11
1	

$$120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0$$

$$231 = 3^1 \cdot 7^1 \cdot 11^1 \cdot 2^0 \cdot 5^0$$

$$\text{m.c.d } \{120, 231\} = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3$$

$$\text{m.c.m } \{120, 231\} = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 9240$$

Proposición: si  $a$  y  $b$  son enteros positivos  $\Rightarrow \text{m.c.d } \{a, b\} \cdot \text{m.c.m } \{a, b\} = a \cdot b$

### Algoritmo de Euclides

Entrada:  $a$  y  $b$  enteros positivos

Salidas: m.c.d  $\{a, b\}$

$$(a_0, a_1) = (a, b)$$

$$\text{Mientras que } a_1 \neq 0 \rightarrow (a_0, a_1) = (a_1, a_0 \text{ mod } a_1)$$

Devuelve  $a_0$

Ejemplo. Calcular m.c.d.  $\{237, 99\}$

$$(a_0, a_1) = (237, 99) = (99, 237 \text{ mod } 99) =$$

$$= (99, 39) = (39, 21) = (21, 18) = (18, 3) =$$

$$= (3, 0)$$

$$\therefore \text{m.c.d } \{237, 99\} = 3$$

$$\begin{array}{r} 237 \\ 39 \\ \hline 2 \end{array}$$

WUOLAH

17

Ejercicio. Calcular el m.c.d. de 434 y 222 utilizando el algoritmo de Euclides.

$$\begin{aligned}(a_0, a_1) &= (434, 222) = (222, 212) = \\ &= (212, 10) = (10, 2) = (2, 0)\end{aligned}$$

$$\text{m.c.d. } \{434, 222\} = 2$$

$$\begin{array}{r} 434 \quad | 222 \\ 212 \quad | 1 \\ 222 \quad | 212 \\ 0 \quad | 0 \quad | 1 \\ 212 \quad | 10 \\ 0 \quad | 2 \quad | 2 \\ 2 \end{array}$$

Una ecuación diofántica lineal es una expresión de la forma  $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$  donde  $a_1, a_2, \dots, a_n, b \in \mathbb{Z}$  y  $x_1, x_2, \dots, x_n$  son incógnitas. Una solución de dicha ecuación es n-tupla  $(c_1, c_2, \dots, c_n) \in \mathbb{Z}^n$  tg  $a_1c_1 + a_2c_2 + \dots + a_nc_n = b$

### Teorema de Bezout generalizado

Si  $a_1, a_2, \dots, a_n, b \in \mathbb{Z}$  y d es el m.c.d.  $\{a_1, a_2, \dots, a_n\}$  entonces la ecuación diofántica  $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$  tiene solución si solamente si  $d|b$

Además en dicho caso la ecuación tiene las mismas soluciones que la ecuación  $\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + \dots + \frac{a_n}{d}x_n = \frac{b}{d}$

Ejemplo. ¿Tiene solución la ecuación diofántica

$$9x - 6y + 2z - 17t = 19 ?$$

$$\text{m.c.d. } \{9, 6, 2\} = 3$$

como  $3 \nmid 19$  la ecuación diofántica no tiene solución

Ejemplo. ¿Tiene solución la ecuación diofántica

$$6x - 8y + 10z - 14t = 128 ?$$

$$\text{m.c.d. } \{6, 8, 10, 14\} = 2$$

Como  $2|128$  sabemos que la ecuación diofántica tiene solución. Además sabemos que tiene las mismas soluciones que la ecuación  $3x - 4y + 5z - 7t = 64$

→ Ecuaciones diofánticas con 2 incógnitas

Sean  $a, b, c \in \mathbb{Z}$  tg m.c.d  $\{a, b\} = 1$

Si  $(x_0, y_0)$  es una solución de la ec. diofántica  $ax+by=0 \Rightarrow$  el conjunto formado por todas las soluciones de la ecuación es

$$\{(x_0 + bk, y_0 - ak) \text{ tg } k \in \mathbb{Z}\}$$

Ejemplo. Resolver la ec. diofántica  $10x - 8y = -14$

Como m.c.d  $\{10, 8\} = 2$  y  $2 \mid 14 \Rightarrow$  sabemos que la ec. diofántica tiene solución. Además sabemos que tiene las mismas soluciones que la ecuación  $5x - 4y = 7$

Como  $(x_0 = 3, y_0 = 2)$  es una solución de la ecuación entonces el conjunto formado por todas sus soluciones es  $\{(3 - 4k, 2 - 5k) \text{ tg } k \in \mathbb{Z}\}$

### Algoritmo extendido de Euclides

Entrada:  $a$  y  $b$  enteros positivos

Salida:  $s, t, d \in \mathbb{Z}$  tg  $d = \text{m.c.d}\{a, b\}$  y  $asd + bt = d$

$$(a_0, a_1) = (a, b)$$

$$(s_0, s_1) = (1, 0)$$

$$(t_0, t_1) = (0, 1)$$

mientras  $a_1 \neq 0$

$$g = a_0 \text{ div } a_1$$

$$(a_0, a_1) = (a_1, a_0 - g \cdot a_1)$$

$$(s_0, s_1) = (s_1, s_0 - gs_1)$$

$$(t_0, t_1) = (t_1, t_0 - gt_1)$$

Devuelve  $d = a_0, s = s_0, t = t_0$

Ejercicio. Calcular todas las soluciones de la ec. diofántica

$$120x - 93y = 6.$$

- ¿Cuántas soluciones tiene la ec. anterior verificando que  $x, y \in [-200, 200]$ ?

$$\text{mcd}\{120, 93\} = 3 \quad \left\{ \begin{array}{l} \text{Como m.c.d}\{120, 93\} = 3 \\ 3 | 6 \Rightarrow \text{sabemos que la ec. diofántica} \end{array} \right. \quad \left. \begin{array}{l} \text{tiene solución. Además sabemos que tiene las} \\ \text{mismas soluciones que la ecuación } 40x - 31y = 2 \end{array} \right.$$

$$\begin{array}{r|rr} 120 & 2 & 93 & 3 \\ 60 & 2 & 31 & 31 \\ 30 & 2 & & 31 \\ 15 & 3 & & 1 \\ 5 & 5 & & \\ 1 & & & \end{array}$$

Como  $\text{m.c.d}\{40, 31\} = 1 \Rightarrow$  sabemos que si conocemos una solución de la ecuación las conocemos todas.

Para calcular una solución de la ecuación vamos a aplicar el algoritmo extendido de Euclides a los números 40 y 31

$$(a_0, a_1) = (40, 31) = (31, 9) = (9, 4) = (4, 1) = (1, 0) \quad g=1 \quad g=3 \quad g=2 \quad g=4$$

$$(s_0, s_1) = (1, 0) = (0, 1) = (-1, -3) = (-3, 7) = (7, \dots)$$

$$(t_0, t_1) = (0, 1) = (1, -1) = (-1, 4) = (4, -9) = (-9, \dots)$$

$$\text{Comprobación: } 40 \cdot 7 + 31(-9) = 1$$

$$\begin{aligned} 40 \cdot 7 - 31 \cdot 9 &= 1 && \leftarrow \text{para obtener una solución} \\ 40 \cdot 14 - 31 \cdot 18 &= 2 && \text{de la ecuación } 40x - 31y = 2 \end{aligned}$$

$(x_0, y_0) = (14, -18)$  es una solución, por tanto el conjunto formado por todas sus soluciones es

$$\{(14 - 31k, -18 - 40k) \mid k \in \mathbb{Z}\}$$

$$\begin{aligned} \bullet \text{ Si } x \in [-200, 200] \Rightarrow -200 \leq 14 - 31k \leq 200 \Rightarrow -214 \leq -31k \leq 186 \Rightarrow \\ \Rightarrow -186 \leq 31k \leq 214 \Rightarrow \frac{-186}{31} \leq k \leq \frac{214}{31} \Rightarrow -6 \leq k \leq 6 \quad k \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \text{Si } y \in [-200, 200] \Rightarrow -200 \leq -18 - 40k \leq 200 \Rightarrow -218 \leq -40k \leq 182 \Rightarrow \\ \Rightarrow -182 \leq 40k \leq 218 \Rightarrow \frac{-182}{40} \leq k \leq \frac{218}{40} \Rightarrow -4.5 \leq k \leq 5.45 \Rightarrow \\ \Rightarrow -4 \leq k \leq 5 \end{aligned}$$

$$\text{Si } xy \in [-200, 200] \Rightarrow -4 \leq k \leq 5 \Rightarrow \text{Hay 10 soluciones } (5 - (-4) + 1)$$



→ Ecuaciones en congruencias de grado 1

Sea  $a, b, m \in \mathbb{Z}$  escribiremos  $a \equiv b \pmod{m}$  si  $m | a - b$  y diremos que  $a$  es congruente con  $b$  módulo  $m$

$$7 \equiv 1 \pmod{3} \rightarrow 7 - 1 = 6 \rightarrow 3 | 6 \quad \checkmark$$

$$8 \not\equiv 1 \pmod{3} \rightarrow 8 - 1 = 7 \rightarrow 3 \nmid 7$$

Una ecuación en congruencia de grado 1 es una expresión de la forma  $ax \equiv b \pmod{m}$  donde  $a, b, m \in \mathbb{Z}$  y  $x$  es una incógnita. Una solución de la ecuación es un  $n^o$  entero  $c$  verificando que  $ac \equiv b \pmod{m}$

**Ejemplo.** Resolver la ecuación  $3x \equiv 2 \pmod{5}$

$$\text{Soluciones} = \left\{ 4, 9, 14, 19, 24, \dots \right\} = \left\{ 4 + 5k \mid k \in \mathbb{Z} \right\}$$

$$\left. \begin{array}{l} \\ \\ -1, -6, -11, -16, \dots \end{array} \right\}$$

**Ejemplo.** Calcular las soluciones de la ecuación  $2x \equiv 1 \pmod{4}$

No tiene solución

Teorema:

1. La ecuación  $ax \equiv b \pmod{m}$  tiene solución si solo si  $\text{m.c.d.}\{a, m\} \mid b$

2. Si  $d = \text{m.c.d.}\{a, m\}$  y  $d \mid b \Rightarrow$  las ecuaciones  $ax \equiv b \pmod{m}$

y  $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$  tienen las mismas soluciones

3. Si el  $\text{m.c.d.}\{a, m\} = 1$  y  $u$  es una solución de  $ax \equiv b \pmod{m}$  entonces el conjunto de todas sus soluciones es  $\{u + km \mid k \in \mathbb{Z}\}$

4. La ecuación  $ax + c \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $ax \equiv b - c \pmod{m}$

5. La ecuación  $ax \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $(a \pmod{m})x \equiv b \pmod{m}$

6. Si  $u, v \in \mathbb{Z}$  y  $au + mv = 1 \Rightarrow bu \pmod{m}$  es una solución de la ecuación  $ax \equiv b \pmod{m}$

Ej. Resolver la ecuación  $237x \equiv 191 \pmod{5}$

Por el punto 5 del Tº anterior la ecuación tiene las mismas soluciones que la ecuación  $(237 \pmod{5})x \equiv 191 \pmod{5} \pmod{5}$

$$\begin{aligned} 237 \pmod{5} &= 2 \\ 191 \pmod{5} &= 1 \end{aligned} \quad \left\{ \begin{array}{l} 2x \equiv 1 \pmod{5} \end{array} \right.$$

Como  $x = 3$  es una solución de la ecuación y

m.c.d.  $\{2, 5\} = 1 \Rightarrow$  aplicando el punto 3 del Tº anterior tenemos que el conjunto de todas las soluciones es  $\{3 + 5k \mid k \in \mathbb{Z}\}$

Ej. Resolver la ecuación  $30x \equiv 20 \pmod{50}$

Como m.c.d.  $\{30, 50\} = 10$  y  $10 \mid 20$  sabemos que la ecuación tiene soluciones y además tiene las mismas soluciones que  $3x \equiv 2 \pmod{5}$

Como m.c.d.  $\{3, 5\} = 1$  y  $x = 4$  es una solución  $\Rightarrow$  el conjunto de todas sus soluciones es  $\{4 + 5k \mid k \in \mathbb{Z}\}$

Ej. Resolver la ecuación  $242x \equiv 4 \pmod{392}$

Como m.c.d.  $\{242, 392\} = 2$  y  $2 \mid 4$  sabemos que la ecuación tiene soluciones y además tiene las mismas soluciones que la ecuación  $121x \equiv 2 \pmod{196}$

Vamos a aplicar el algoritmo extendido de Euclides a  $196$  y  $121$ .

$$\begin{aligned} (a_0, a_1) &= (196, 121) = (121, 75) \stackrel{g=1}{=} (75, 46) \stackrel{g=1}{=} (46, 29) \stackrel{g=1}{=} (29, 17) \stackrel{g=1}{=} (17, 12) \stackrel{g=1}{=} (12, 5) \stackrel{g=1}{=} \\ &\quad = (5, 2) \stackrel{g=2}{=} (2, 1) \stackrel{g=2}{=} (-1, 0) \\ (s_0, s_1) &= (1, 0) = (0, -1) = (1, -1) = (-1, 2) = (2, -3) = (-3, 5) = (5, -8) = (-8, 21) = \\ &\quad = (21, -50) = (-50, \dots) \\ (t_0, t_1) &= (0, -1) = (1, -1) = (-1, 2) = (2, -3) = (-3, 5) = (5, -8) = (-8, 13) = (-13, -34) = \\ &\quad = (-34, 81) = (81, \dots) \\ 196(-50) + 121(81) &= 1 \end{aligned}$$

Como  $196(-50) + 121(81) = 1$  por el punto 6 del Tº anterior

sabemos que  $2^{\circ} 81 \pmod{196} = 162$  es una solución de la ecuación

$$\{162 + 196k \mid k \in \mathbb{Z}\}$$

→ Sistemas de ecuaciones en congruencias

Ej. Resolver el sistema:

$$\begin{array}{l} \left. \begin{array}{l} 4x \equiv 6 \pmod{10} \\ 3x \equiv 1 \pmod{4} \end{array} \right\} \left. \begin{array}{l} 2x \equiv 3 \pmod{5} \\ 3x \equiv 1 \pmod{4} \end{array} \right\} \left. \begin{array}{l} x = 4 + 5k = * \\ 3(4+5k) \equiv 1 \pmod{4} \Rightarrow \end{array} \right. \\ \Rightarrow 12 + 15k \equiv 1 \pmod{4} \Rightarrow \\ \Rightarrow 15k \equiv -11 \pmod{4} \Rightarrow 3k \equiv 1 \pmod{4} \\ \Rightarrow k = 3 + 4 \cdot \bar{k} \end{array}$$

$$* = 4 + 5(3 + 4\bar{k}) = 19 + 20\bar{k}$$

Ej. Resolver el sistema:

$$\begin{array}{l} \left. \begin{array}{l} 2x \equiv 2 \pmod{4} \\ 3x \equiv 6 \pmod{12} \end{array} \right\} \left. \begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{4} \end{array} \right\} \left. \begin{array}{l} x = 1 + 2k \\ 1 + 2k \equiv 2 \pmod{4} \Rightarrow 2k \equiv 1 \pmod{4} \end{array} \right. \\ \hookrightarrow \text{esta ecuación no tiene solución y por tanto el sistema no tiene solución} \end{array}$$

Ej. Resolver el sistema:

$$\begin{array}{l} \left. \begin{array}{l} 2x \equiv 2 \pmod{4} \\ 6x \equiv 3 \pmod{9} \\ 2x \equiv 3 \pmod{5} \end{array} \right\} \left. \begin{array}{l} x \equiv 1 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 2x \equiv 3 \pmod{5} \end{array} \right\} \left. \begin{array}{l} x = 1 + 2k \\ 2(1 + 2k) \equiv 1 \pmod{3} \Rightarrow k \\ 2(1 + 2k) \equiv 3 \pmod{5} \Rightarrow * \end{array} \right. \\ * 3^{\text{a}} \text{ ecuación} \\ \Rightarrow 10 + 12k \equiv 3 \pmod{5} \Rightarrow 12k \equiv -7 \pmod{5} \Rightarrow 2k \equiv 3 \pmod{5} \Rightarrow \\ \Rightarrow \bar{k} = 4 + 5\bar{k} \\ * 2^{\text{a}} \text{ ecuación} \\ \Rightarrow 2 + 4k \equiv 1 \pmod{3} \Rightarrow 4k \equiv -1 \pmod{3} \Rightarrow k \equiv 2 \pmod{3} \Rightarrow \\ \Rightarrow k = 2 + 3\bar{k} \quad \hookrightarrow \text{se puede cambiar por el resto de dividir ese n° entre m} \\ * 1^{\text{a}} \text{ ecuación} \\ \Rightarrow 5 + 6(4 + 5\bar{k}) = 29 + 30\bar{k} \end{array}$$

Ej. Cuántos números del intervalo  $[1000, 2000]$  son pares  
 ② al dividirlos entre 7 dan de resto 1 y al  
 ③ multiplicarlos por 3 y dividirlos entre 5 dan de resto 2.

$$\begin{aligned} \text{① } X &\equiv 0 \pmod{2} \rightarrow X = 0 + 2k = 2(4 + 7\bar{k}) = 8 + 14\bar{k} = 8 + 14(4 + 5\bar{k}) = 64 + 70\bar{k} \\ \text{② } X &\equiv 1 \pmod{7} \rightarrow 2k \equiv 1 \pmod{7} \Rightarrow k = 4 + 7\bar{k} \\ \text{③ } 3X &\equiv 2 \pmod{5} \rightarrow 3(8 + 14\bar{k}) \equiv 2 \pmod{5} \Rightarrow 24 + 42\bar{k} \equiv 2 \pmod{5} \Rightarrow \\ &\Rightarrow 42\bar{k} \equiv -22 \pmod{5} \Rightarrow 2\bar{k} \equiv 3 \pmod{5} \Rightarrow \bar{k} = 4 + 5\bar{k} \end{aligned}$$

$$1000 \leq 64 + 70\bar{k} \leq 2000$$

$$936 \leq 70\bar{k} \leq 1936$$

$$\frac{936}{70} \leq \bar{k} \leq \frac{1936}{70}$$

$$13'37 \leq \bar{k} \leq 27'65$$

$$14 \leq \bar{k} \leq 27 \rightarrow \text{Sol. } 14 \quad (27-14+1)$$

Ej. ¿Cuántos números naturales  $< 1000$  acaban en 7 y al dividirlos entre 55 dan de resto 12?

$$\begin{aligned} X &\equiv 7 \pmod{10} \rightarrow X = 7 + 10k = 7 + 10(6 + 11\bar{k}) = 67 + 110\bar{k} \\ X &\equiv 12 \pmod{55} \rightarrow 7 + 10k \equiv 12 \pmod{55} \Rightarrow 10k \equiv 5 \pmod{55} \Rightarrow \\ &\Rightarrow 2\bar{k} \equiv 1 \pmod{11} \Rightarrow \bar{k} = 6 + 11\bar{k} \end{aligned}$$

$$0 \leq 67 + 110\bar{k} < 1000$$

$$-67 \leq 110\bar{k} < 933$$

$$\frac{-67}{110} \leq \bar{k} < \frac{933}{110}$$

$$-0'6 \leq \bar{k} < 8'48$$

$$0 \leq \bar{k} \leq 8 \rightarrow \text{Sol. } 9$$



El anillo de los enteros módulo un entero positivo.

Dado un entero positivo  $m$  denotaremos  $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$

Sobre dicho conjunto definimos una operación suma y una operación producto de la siguiente forma:

$$a \oplus b = (a+b) \bmod m \quad y \quad a \odot b = a \cdot b \bmod m$$

Ej. Calcular en  $\mathbb{Z}_7$   $4 \oplus 5$  y  $4 \odot 5$

$$4 \oplus 5 = 4+5 \bmod 7 = 9 \bmod 7 = 2$$

$$4 \odot 5 = 4 \cdot 5 \bmod 7 = 20 \bmod 7 = 6$$

Ej. Calcular en  $\mathbb{Z}_8$   $5 \oplus 5$  y  $5 \odot 5$

$$5 \oplus 5 = 5+5 \bmod 8 = 10 \bmod 8 = 2$$

$$5 \odot 5 = 25 \bmod 8 = 1$$

• Propiedades de  $\oplus$ :

1. Asociativa:  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
2. Comunitativa:  $a \oplus b = b \oplus a$
3. Elemento neutro:  $a \oplus 0 = a$
4. Elemento inverso:  $-a = m - a$

• Propiedades de  $\odot$ :

1. Asociativa:  $a \odot (b \odot c) = (a \odot b) \odot c$
2. Comunitativa:  $a \odot b = b \odot a$
3. Elemento neutro:  $a \odot 1 = a$
4. Distributiva:  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

En  $\mathbb{Z}_m$  hay elementos que tienen inverso para el producto y elementos que no tienen inverso para el producto.

A los elementos de  $\mathbb{Z}_m$  que tienen inverso para el producto los llamaremos unidades.

Denotaremos  $a^{-1}$  al inverso para el producto de  $a$ .

Denotaremos  $-a$  al inverso para la suma de  $a$ .

Ej. Calcular para  $\mathbb{Z}_9$   $5 \cdot 3, 6+5, -4, 5^{-1}, 3^{-1}$

$$5 \cdot 3 = 6$$

$$6+5 = 2$$

$$-4 = 5$$

$$5^{-1} = 2$$

$$3^{-1}$$

Ej. Calcular las unidades de  $\mathbb{Z}_9$

$$U(\mathbb{Z}_9) = \{1, 2, 5, 7, 8\}$$

• Teorema:

Un elemento  $a \in \mathbb{Z}_m$  tiene inverso para el producto si solamente si  $m.c.d(a, m) = 1$

Además si  $au + mv = 1$  con  $u, v \in \mathbb{Z} \Rightarrow a^{-1} = u \text{ mod } m$

Ej. Calcular las unidades de  $\mathbb{Z}_{15}$  y  $7^{-1}$

$$U(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$7^{-1} = 13$$

Ej. Calcular el inverso para el producto de 35 en  $\mathbb{Z}_{97}$

Como  $m.c.d(97, 35) = 1$  sabemos que 35 es una unidad de  $\mathbb{Z}_{97}$  y por tanto  $\exists 35^{-1}$

Vamos a aplicar el algoritmo extendido de Euclides:

$$(a_0, a_1) = (97, 35) \stackrel{g=2}{=} (35, 27) \stackrel{g=1}{=} (27, 8) \stackrel{g=3}{=} (8, 3) \stackrel{g=2}{=} (3, 2) \stackrel{g=1}{=} (2, 1) \stackrel{g=2}{=} (1, 0)$$

$$(s_0, s_1) = (1, 0) \stackrel{g=2}{=} (0, 1) = (1, -1) = (-1, 4) = (4, -9) = (-9, 13) = (13, -)$$

$$(t_0, t_1) = (0, 1) = (1, -2) = (-2, 3) = (3, -11) = (-11, 25) = (25, -36) = (-36, -)$$

$$97 \cdot 13 + 35(-36) = 1$$

$$35^{-1} = (-36) \text{ mod } 97 \Rightarrow 35^{-1} = 61$$

Ej. Resolver en  $\mathbb{Z}_9$  la ecuación  $x+7 \equiv 5x+2$

$$x+7 \equiv 5x+2 \Rightarrow 4x = 5 \Rightarrow 4^{-1} \cdot 4x = 4^{-1} \cdot 5 \Rightarrow x = 7 \cdot 5 \Rightarrow x = 8$$

Ej. Resuelve en  $\mathbb{Z}_{10}$  la ecuación  $8x+5 \equiv 2x+7$

$$8x+5 \equiv 2x+7 \Rightarrow 6x = 2 \Rightarrow 6x \equiv 2 \pmod{10} \Rightarrow 3x \equiv 1 \pmod{5} \Rightarrow$$
$$\Rightarrow x = 2+5k$$

Solución  $\{2, 7\}$

Ej. Resolver en  $\mathbb{Z}_6$  la ecuación  $2x+3 \equiv 4x+4$

$$2x+3 \equiv 4x+4 \Rightarrow 2x = -1 \Rightarrow 2x = 5 \Rightarrow 2x \equiv 5 \pmod{6}$$

↑  
No tiene solución

Ej. Calcular en  $\mathbb{Z}_{10}$   $3^{127}$

$$3^1 = 3 \quad 127 \not\equiv 1 \pmod{4}$$

$$3^2 = 9 \quad 0 \not\equiv 3 \pmod{4}$$

$$127 = 4 \cdot 31 + 3$$

$$3^3 = 7 \quad 3^{127} = 3^{4 \cdot 31 + 3}$$

$$3^4 = 1$$

$$= 3^{4 \cdot 31} \cdot 3^3 = (3^4)^{31} \cdot 3^3 = 1^{31} \cdot 7 = 7$$

Ej. Calcular en  $\mathbb{Z}_{15}$   $3^{127}$

$$\begin{array}{|l} \hline 3^1 = 3 \\ 3^2 = 9 \\ 3^3 = 12 \\ 3^4 = 6 \\ \hline 3^5 = 3 \end{array}$$

$$127 \not\equiv 1 \pmod{4}$$

$$3^{4 \cdot 31} = 6$$

$$3^{4 \cdot 31 + 1} = 3$$

$$3^{4 \cdot 31 + 2} = 9$$

$$3^6 = 9$$

$$3^{127} = 3^{4 \cdot 31 + 3} = 12$$

$$3^7 = 12$$

$$3^8 = 6$$

$$3^9 = 3$$

.

:

## • Proposición.

Si  $a_1, a_2, \dots, a_k, m \in \mathbb{Z}$  entonces:

$$1. (a_1 + a_2 + \dots + a_k) \bmod m = (a_1 \bmod m + a_2 \bmod m + \dots + a_k \bmod m) \bmod m$$

$$2. (a_1 \cdot a_2 \cdot \dots \cdot a_k) \bmod m = (a_1 \bmod m \cdot a_2 \bmod m \cdot \dots \cdot a_k \bmod m) \bmod m$$

Ej. Calcular el resto de dividir  $4225^{1001}$  entre 7

$$\begin{aligned} 4225^{1001} \bmod 7 &= (4225 \cdot \underbrace{\dots \cdot 4225}_{1001}) \bmod 7 = \\ &= (4225 \bmod 7 \cdot \dots \cdot 4225 \bmod 7) \bmod 7 = \\ &= (4 \cdot \underbrace{\dots \cdot 4}_{1001}) \bmod 7 = 4^{1001} \bmod 7 \end{aligned}$$

Esta cantidad coincide con el valor de  $4^{1001}$  en  $\mathbb{Z}_7$

$$\begin{array}{lll} 4^1 = 4 & 1001 & \begin{array}{r} 13 \\ 10 \quad | \\ 11 \\ \quad 1 \end{array} \\ 4^2 = 2 & & 333 \\ 4^3 = 1 & & 2 \end{array} \quad \begin{array}{l} 1001 = 3 \cdot 333 + 2 \\ 4^{1001} = 4^{3 \cdot 333 + 2} = (4^3)^{333} \cdot 4^2 = 2 \end{array}$$

## → Sistemas de numeración

Sea  $B$  un número entero  $\geq 2 \Rightarrow$  todo número natural  $n \neq 0$  se puede poner de forma única como

$$n = a_k B^k + a_{k-1} B^{k-1} + \dots + a_1 B + a_0$$

donde  $\{a_0, a_1, \dots, a_k\} \subseteq \{0, 1, \dots, B-1\}$  y  $a_k \neq 0$

A la  $(k+1)$ -tuple  $(a_k, a_{k-1}, \dots, a_1, a_0)$  la llamaremos expresión en base  $B$  del nº natural  $n$ .

Por definición (0) es la expresión en base  $B$  del número natural 0.

Ej. Calcular la expresión en base 3 del nº 25.

$$25 = 2 \cdot 3^2 + 2 \cdot 3 + 1$$

(2, 2, 1) es la expresión en base 3 del nº 25



Ej. ¿Qué número tiene la expresión  $(-10, -10, 10)$  en base 2?

$$1 \cdot 2^5 + 0 \cdot 2^4 + -1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 42$$

Ej. Calcular la expresión en base 7 del nº 1538

$$\begin{array}{r} 1538 \\ 13 \quad \overline{)219} \\ 68 \quad \overline{)09} \\ \textcircled{5} \quad \textcircled{3} \quad \textcircled{3} \quad \textcircled{4} \\ \end{array}$$

$(4, 3, 2, 5)$  es la expresión en base 7 de 1538.

Ej. Calcular la expresión en base 9 del nº 2531

$$\begin{array}{r} 2531 \\ 73 \quad \overline{)2819} \\ 11 \quad \overline{)11} \quad \overline{)319} \\ \textcircled{2} \quad \textcircled{2} \quad \textcircled{4} \quad \textcircled{3} \\ \end{array}$$

$(3, 4, 2, 2)$

Ej. Si la expresión de un nº en base 3 es  $(1, 2, -1, 0, -1)$  calcular la expresión de dicho nº en base 5

$$1 \cdot 3^4 + 2 \cdot 3^3 + -1 \cdot 3^2 + 0 \cdot 3 + -1 = 81 + 54 + 9 + 1 = 145 \rightarrow \text{en base } 10$$

$$\begin{array}{r} 145 \\ 45 \quad \overline{)2915} \\ \textcircled{0} \quad \textcircled{4} \quad \textcircled{0} \quad \textcircled{1} \\ \end{array}$$

$(1, 0, 4, 0)$  en base 5

→ Método para pasar de base  $B$  a base  $B^r$

Ej. Si la expresión de un nº en base 2 es  $(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, -1, 0, 1, 1, 1, 0, -1, 0, -1)$  calcular la expresión de dicho nº en base 8.

$$8 = 2^3$$

$(1, 3, 0, 6, 5, 6, 5)$  en base 8

Ej. Si la expresión de un nº en base 3 es

$(1, 0, 2, 1, 0, \textcircled{1}, 1, 1, 2, 1, 0, 0, 1, 2)$  calcular la expresión de

$$27 = 3^3$$

dicho nº en base 27

$(1, 7, 4, 21, 5)$

Ej. Si la expresión de un nº en base 9 es

(6, 7, 3, 8, 1) calcular la expresión de dicho nº en base 3  
 $\begin{array}{r} 6 \\ 7 \\ 3 \\ 8 \\ 1 \end{array}$     $\begin{array}{r} 20 \\ 21 \\ 10 \\ 22 \\ 01 \end{array}$

Ej. Si la expresión de un nº en base 8 es (16324513)

calcular la expresión de dicho nº en base 2.

(~~1~~1 110 011 010 100 101 001 011)

• Suma y producto en base B

Ej. Calcular  $(4, 3, 2, 4, 3)_5 + (3, 4, 1, 3)_5 = (1, 0, 2, 2, 1, 1)_5$

$$\begin{array}{r} 4 & 3 & 2 & 4 & 3 \\ + & 3 & 4 & 1 & 3 \\ \hline 10 & 2 & 2 & 1 & 1 \end{array}$$

$6 = 1 \cdot 5 + 1$

Ej. Calcular  $(2, 3, 4, 1)_5 \times (3, 4)_5 = (2, 0, 2, 2, 4, 4)_5$

$$\begin{array}{r} 2 & 3 & 4 & 1 \\ \times & 3 & 4 \\ \hline 6 & 1 & 0 & 1 & 4 \\ + & 2 & 1 & 0 & 1 & 4 \\ \hline 1 & 3 & 1 & 2 & 3 \\ \hline 2 & 0 & 2 & 2 & 4 & 4 \end{array}$$

Ej. Encontrar la base B que existe en que  $(3, 4, 3, 2)_B \times (3, 4)_B = (1, 5, 6, 6, 5, 1)_5$

$$(3B^3 + 4B^2 + 3B + 2) \cdot (3B + 4) = (B^5 + 5B^4 + 6B^3 + 6B^2 + 5B + 1)$$

$$9B^4 + 12B^3 + 12B^2 + 16B^2 + 9B^2 + 12B + 6B + 8 = B^5 + 5B^4 + 6B^3 + 6B^2 + 5B + 1$$

$$B^5 - 4B^4 - 18B^3 - 19B^2 - 13B - 7 = 0$$

$$\begin{array}{r|cccccc} 1 & -4 & -18 & -19 & -13 & -7 \\ \hline 1 & 7 & 21 & 21 & 14 & 7 \\ \hline 1 & 3 & 3 & 2 & 1 & 0 \end{array}$$

$$B = 7$$

Ej: Calcular todos los nº naturales que al expresarlos en base 8 terminan en -12 y al expresarlos en base 9 terminan en -15

$$x = a_n \cdot 8^n + a_{n-1} \cdot 8^{n-1} + \dots + a_2 \cdot 8^2 + 1 \cdot 8 + 2 =$$

$$= 8^2(a_n \cdot 8^{n-2} + a_{n-1} \cdot 8^{n-3} + \dots + a_2) + 10$$

$$\begin{aligned} x &\equiv -10 \pmod{64} \\ x &\equiv 14 \pmod{81} \end{aligned}$$

Ej: ¿Qué significa en congruencias que un nº en base 3 termine en 1012? Es un base 3 y son 4 cifras:  $3^4 = 81$

$$x \equiv 32 \pmod{81}$$

$$1 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^1 + 2 = 32$$

Ej: ¿Qué significa en congruencias que un nº en base 5 termine en 104? Como es en base 5 y son 3 cifras:  $5^3 = 125$

$$x \equiv 29 \pmod{125}$$

$$1 \cdot 5^2 + 0 \cdot 5 + 4 = 29$$

Ej: Demostrar que un nº escrito en base 10 es múltiplo de 3 si solamente si la suma de sus cifras es múltiplo de 3

$$(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0) \text{ es múltiplo de } 3 \iff$$

$$\iff (a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0) \pmod{3} = 0 \iff *$$

$$\iff (a_n \cdot 10^n \pmod{3} + a_{n-1} \cdot 10^{n-1} \pmod{3} + \dots + a_1 \cdot 10 \pmod{3} + a_0 \pmod{3}) \pmod{3} = 0$$

$$\begin{aligned} a_k \cdot 10^k \pmod{3} &= (a_k \cdot 10 \cdot \dots \cdot 10) \pmod{3} \iff (a_k \pmod{3} \cdot 10 \pmod{3} \cdot \dots \cdot 10 \pmod{3}) \pmod{3} = \\ &= (a_k \pmod{3}) \pmod{3} = a_k \pmod{3} \end{aligned}$$

$$*\iff (a_n \pmod{3} + a_{n-1} \pmod{3} + \dots + a_1 \pmod{3} + a_0 \pmod{3}) \pmod{3} = 0 \iff$$

$$\iff (a_n + a_{n-1} + \dots + a_1 + a_0) \pmod{3} = 0 \iff a_n + a_{n-1} + \dots + a_1 + a_0 \text{ es múltiplo de } 3$$

31

- Si donde pone 3 colocamos un 9 hemos demostrado la regla del 9.
- Para demostrar la regla del 11:  $10 \bmod 11 = (-1) \bmod 11$
- Un nº en base 9 es múltiplo de 3 si termina en 0, 3, 6.