

# **TEMA IV: INTRODUCCIÓN A LA TEORÍA DE NÚMEROS: ARITMETICA MODULAR.**



# OBJETIVOS GENERALES

- 1. Conocer los conjuntos de números naturales y números enteros, sus propiedades y operaciones.**
- 2. Entender ambos como ejemplos de conjuntos discretos.**
- 2. Conocer nociones básicas de aritmética modular.**



# OBJETIVOS ESPECÍFICOS

- ✓ Comprender las dos formas de definición del conjunto de los números naturales.
- ✓ Conocer las propiedades básicas de los números naturales y sus operaciones.
- ✓ Conocer las propiedades básicas de los números enteros y sus operaciones.
- ✓ Conocer la relación de divisibilidad en el conjunto de los números enteros.
- ✓ Reconocer la importancia del teorema fundamental de la aritmética.
- ✓ Saber calcular el máximo común divisor y el mínimo común múltiplo de dos enteros.
- ✓ Saber usar el algoritmo de la división entre números enteros.



# OBJETIVOS ESPECÍFICOS

- ✓ Saber obtener la identidad de Bezout de dos números enteros.
- ✓ Saber calcular el máximo común divisor de dos números enteros mediante el algoritmo de Euclides.
- ✓ Saber calcular, si existen, todas las soluciones enteras de una ecuación del tipo  $a.x + b.y = c$  donde  $a$ ,  $b$  y  $c$  son número enteros.
- ✓ Conocer el concepto de congruencia.
- ✓ Conocer los conjuntos de las clases de restos módulo  $n$ .
- ✓ Realizar con soltura operaciones de la aritmética modular (aritmética en  $\mathbb{Z}_n$ ).
- ✓ Saber cuando un elemento en  $\mathbb{Z}_n$  es una unidad y saber calcular el inverso de dicho elemento.



# OBJETIVOS ESPECÍFICOS

- ✓ Conocer el concepto de divisor de cero y saber cuando un elemento es divisor de cero en  $\mathbb{Z}_n$ .
- ✓ Resolver congruencias lineales y sistemas de congruencias.
- ✓ Conocer el concepto de sistema de numeración.
- ✓ Saber pasar un número de cualquier sistema de numeración a otro con distinta base.



# BIBLIOGRAFÍA

- **“Matemática discreta para la computación”. M.A. García-Muñoz. Servicio de Publ. Univ. Jaén. 2010.**
- **“Matemática discreta y combinatoria”. R. P. Grimaldi. Addison-Wesley Iberoamericana, 1989.**
- **“Matemática discreta”, F. García Merayo. Paraninfo, 2001.**
- **“Problemas resueltos de Matemática discreta”, F. García Merayo y otros. Paraninfo, 2003.**
- **“Álgebra abstracta aplicada”. A. Vera López y otros autores. 1992**
- **“201 problemas resueltos de Matemática Discreta”. V. Meavilla Seguí. Universidad Zaragoza, 2000.**
- **“Matemática Discreta y sus aplicaciones”. K. H. Rosen. McGraw-Hill, 2004.**



# DESARROLLO TEÓRICO

IV.1 Introducción.

IV.2 Números naturales y enteros.

IV.3 Divisibilidad en el conjunto de los números enteros

IV.4 Congruencia. Sistemas de congruencias.

IV.5 Sistemas de numeración.

# 1. INTRODUCCIÓN





Tanto el conjunto de los números naturales como el conjunto de los números enteros son conjuntos conocidos. Todos estamos familiarizados con dichos conjuntos y con sus operaciones:

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

La parte de la matemática discreta que trata de los números enteros y sus propiedades recibe el nombre de **teoría de números**. Esta teoría es parte importante de la aritmética, el álgebra y la geometría, y el primer matemático que la creó como ciencia fue Gauss (el príncipe de las matemáticas) al publicar en 1801 su obra “Disquisitiones Arithmeticae”.



Lo primero que haremos en este tema es introducir de forma rigurosa estos conjuntos. Como veremos existe varias formas de introducirlos y nosotros elegiremos la **forma axiomática** que consiste en caracterizar el conjunto de los números naturales por algunas de sus propiedades que se imponen como axiomas, de manera que cualquier otra propiedad se deduce (usando las reglas de la lógica) de estos axiomas. Esta forma de introducir los números naturales se debe a Peano. Una vez definido el conjunto de los números naturales podremos construir el conjunto de los enteros como el conjunto que, en cierto sentido, completa al conjunto de los números naturales.



En tales conjuntos tenemos definidas operaciones por todos conocidas, la suma y la multiplicación, y de las propiedades que satisfagan estas operaciones deduciremos la **estructura algebraica** de dichos conjuntos. El estudio de las estructuras algebraicas es importante y abre todo un campo de las matemáticas conocido como **Álgebra**. El Álgebra se basa en el estudio de la estructura profunda de los conjuntos dotados de operaciones y permite describir sus propiedades y estudiar características generales (podríamos decir que el Álgebra estudia las reglas del juego).



La noción de divisibilidad de la que se deriva el concepto de número primo es de gran importancia en criptografía o estudio de los mensajes secretos. Aunque en el anillo de los números enteros no se puede dividir, ya que los cocientes no son enteros, si se puede hacer una división entera, obteniendo un cociente y un resto. Precisamente basada en estos restos se encuentra la **aritmética modular**, utilizada ampliamente en la ciencia de la computación y particularmente en encriptación de mensajes.



La teoría de números estudia las propiedades de la divisibilidad de los números enteros, que desde antiguo han fascinado al hombre por considerarlos mágicos. Así Fermat conjeturó, y después Lagrange demostró, que cualquier número natural puede expresarse como la suma de cuatro cuadrados. Otro ejemplo de esta magia es los números triangulares 1, 3, 6, 10, 15,..., números que representados mediante puntos forman triángulos equiláteros. En general, el  $n$ -ésimo viene dado por  $(n(n+1))/2$ .

## 2. NÚMEROS NATURALES Y ENTEROS



El conjunto de los números naturales se puede construir de dos formas:

- a) De forma **axiomática**: establecemos una serie de axiomas y a partir de ellos probamos una serie de teoremas que son sus propiedades (Peano, Hilbert).
- b) Como un conjunto de clases de equivalencia de la relación de cardinabilidad entre conjuntos (Cantor, Frege, Rusell).



Siguiendo el primer criterio, consideramos  $\mathbb{N}$  el conjunto formado por un número infinito de objetos indefinidos que llamamos **números naturales**:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

Axioma 1: El número 0 es natural ( $\mathbb{N} \neq \emptyset$ ).

Axioma 2: Para todo elemento  $n \in \mathbb{N}$ , se tiene que  $n + 1 \in \mathbb{N}$ .

Axioma 3 (Axioma de inducción): Si  $A$  es un subconjunto no vacío de  $\mathbb{N}$ , tal que:

i)  $0 \in A$ ,

ii) Si  $n \in A$ , entonces  $n + 1 \in A$ ,

entonces  $A = \mathbb{N}$ .





La **suma de números naturales** es una aplicación

$$+: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

de manera que para cada par de números naturales  $n, m$  existe un único número natural  $n + m$ . Esta operación se define por inducción mediante las reglas:

- i)  $n + 0 = n, \forall n \in \mathbb{N},$
- ii)  $n + (m + 1) = (n + m) + 1, \forall n, m \in \mathbb{N}.$

**Proposición 4.2.** La suma de números naturales satisface:

i) **Elemento neutro:**

Existe  $0 \in \mathbb{N}$  tal que  $0 + n = n = n + 0, \forall n \in \mathbb{N}.$

ii) **Conmutativa,**  $n + m = m + n, \forall n, m \in \mathbb{N}.$

iii) **Asociativa,**  $(n + m) + p = n + (m + p), \forall n, m, p \in \mathbb{N}.$

iv) **Cancelativa,**

Dados  $n, m, p \in \mathbb{N}$ , si  $n + m = n + p$ , entonces  $m = p$ .



El **producto de números naturales** es una aplicación

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

de manera que para cada par de números naturales  $n, m$  existe un único número natural  $n \cdot m$ . Esta operación de nuevo se define de forma inductiva mediante:

i)  $n \cdot 0 = 0, \forall n \in \mathbb{N},$

ii)  $n \cdot (m + 1) = (n \cdot m) + n, \forall n, m \in \mathbb{N}.$

**Proposición 4.3.** El producto de números naturales satisface:

i) **Elemento cero:**  $\exists 0 \in \mathbb{N}$  tal que  $0 \cdot n = 0 = n \cdot 0, \forall n \in \mathbb{N}.$

ii) **Elemento neutro:**  $\exists 1 \in \mathbb{N}$  tal que  $1 \cdot n = n = n \cdot 1, \forall n \in \mathbb{N}.$

iii) **Conmutativa,**  $n \cdot m = m \cdot n, \forall n, m \in \mathbb{N}.$

iv) **Asociativa,**  $(n \cdot m) \cdot p = n \cdot (m \cdot p), \forall n, m, p \in \mathbb{N}.$

v) **Cancelativa,**

Dados  $n, m, p \in \mathbb{N}$ , si  $n \cdot m = n \cdot p$  y  $n \neq 0$ , entonces  $m = p$ .

vi) **Distributivas,**  $n \cdot (m + p) = n \cdot m + n \cdot p, \forall n, m, p \in \mathbb{N}.$



### Proposición

El conjunto de los números naturales  $\mathbb{N}$  es un conjunto ordenado por la relación binaria

$$n \leq m \text{ si y solo si } \exists a \in \mathbb{N} \text{ tal que } m = n + a.$$

### Proposición

$\mathbb{N}$  respecto al orden anterior es:

- i) un conjunto totalmente ordenado.
- ii) un conjunto bien ordenado.



El conjunto de los números enteros surge para resolver problemas que en  $\mathbb{N}$  no tienen solución. Por ejemplo, la ecuación  $x + b = a$  cuando  $a < b$  no tiene solución en  $\mathbb{N}$ , ya que  $a - b$  no tiene sentido en dicho conjunto.

La construcción del conjunto de los números enteros consiste en encontrar un conjunto dotado de una operación interna (+) inducida por la correspondiente operación interna suma en  $\mathbb{N}$ , y en el que todo elemento tenga simétrico respecto de esa operación. De esta forma la ecuación  $x + b = a$  siempre admitirá una solución en el nuevo conjunto de números. Tal simétrico lo notaremos por  $-a$  para todo  $a \in \mathbb{N}$ .



Para definir el conjunto  $\mathbb{Z}$ , partimos del conjunto dado por el producto cartesiano de  $\mathbb{N}$  consigo mismo, es decir:


$$\mathbb{N} \times \mathbb{N} = \{(n, m) / n, m \in \mathbb{N}\}$$

y sobre el definimos la relación binaria que denotaremos mediante el símbolo  $\sim$

$$(n, m) \sim (n', m') \text{ si y sólo si } n + m' = m + n.$$

**Proposición 4.11.** La relación  $\sim$  en  $\mathbb{N} \times \mathbb{N}$  es una relación de equivalencia.

Llamaremos **número entero** a cada una de las clases de equivalencia obtenidas en  $\mathbb{N} \times \mathbb{N}$  al definir la relación de equivalencia  $\sim$ . Llamaremos **conjunto de los números enteros** y lo denotaremos por  $\mathbb{Z}$  al conjunto cociente  $\mathbb{N} \times \mathbb{N} / \sim$ .




Si consideramos como representantes de cada clase los que tiene al menos una de sus componentes nula, se tiene que las distintas clases son:

(I) La clase  $[(a, 0)] = \{(a + k, k) / k \in \mathbb{N}\}$  es un número enteros que designamos por  $a$ , para cualquier  $a \in \mathbb{N}^* = \mathbb{N} - \{0\}$ . Denotamos por  $\mathbb{Z}^+$  al conjunto formado por tales enteros que llamaremos **enteros positivos**.

(II) La clase  $[(0, a)] = \{(k, a + k) / k \in \mathbb{N}\}$  es un número entero que denotaremos por  $-a$ , para todo  $a \in \mathbb{N}^*$ . Designamos con  $\mathbb{Z}^-$  al conjunto formado por dichos enteros que llamaremos **enteros negativos**.

(III) La clase  $[(0, 0)] = \{(k, k) / k \in \mathbb{N}\}$  es un número entero que denotamos por  $0$ .



Utilizando esta nueva notación para representar los números enteros, por lo que el conjunto de los números enteros vendrá dado por:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Inducida por la suma de números naturales podemos definir la **suma de números enteros** como la operación interna dada por

$$+: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

de manera que para cada par de números enteros  $a, b$  existe un único número entero  $a + b$ .

**Proposición 4.11.** La suma de números enteros satisface:

i) **Elemento neutro:**  $\exists 0 \in \mathbb{Z}$  tal que  $0 + a = a = a + 0$ ,  $\forall a \in \mathbb{Z}$ .

ii) **Conmutativa,**  $a + b = b + a$ ,  $\forall a, b \in \mathbb{Z}$ .

iii) **Asociativa,**  $(a + b) + c = a + (b + c)$ ,  $\forall a, b, c \in \mathbb{Z}$ .

iv) **Cancelativa,**

Dados  $a, b, p \in \mathbb{Z}$ , si  $a + p = b + p$ , entonces  $a = b$ .

v) **Elemento simétrico,**

$\forall a \in \mathbb{Z}$ , existe  $-a \in \mathbb{Z}$  tal que  $(-a) + a = 0 = a + (-a)$ .



La **multiplicación de números enteros** es una aplicación

$$. : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

de manera que para cada par de números enteros  $a, b$  existe un único número entero  $a . b$ .

**Proposición 4.13.** El producto de números enteros satisface:

- i) **Elemento cero:**  $\exists 0 \in \mathbb{Z}$  tal que  $0 . a = 0 = a . 0, \forall a \in \mathbb{Z}$ .
- ii) **Elemento neutro:**  $\exists 1 \in \mathbb{Z}$  tal que  $1 . a = a = a . 1, \forall a \in \mathbb{Z}$ .
- iii) **Conmutativa,**  $a . b = b . a, \forall a, b \in \mathbb{Z}$ .
- iv) **Asociativa,**  $(a . b) . c = a . (b . c), \forall a, b, c \in \mathbb{Z}$ .

v) **Cancelativa,**

Dados  $a, b, p \in \mathbb{Z}$ , si  $a . p = b . p$  y  $p \neq 0$ , entonces  $a = b$ .

vi) **Distributivas,**  $a . (b + c) = a . b + a . c, \forall a, b, c \in \mathbb{Z}$ .

vii) **Dominio de integridad,**

Si  $a . b = 0$  entonces  $a = 0$  o  $b = 0$ .

viii) **Regla de los signos:**  $(-a) . b = -(a . b) = a . (-b);$

$-(-a) = a; \text{ y } (-a) . (-b) = a . b$





**Proposición 4.15.** Inducida por la relación de orden en el conjunto de los números naturales, podemos definir una relación de orden en  $\mathbb{Z}$  mediante

$$a \leq b \text{ si y solo si } b - a \in \mathbb{N}.$$

**Proposición 4.16.** El conjunto  $\mathbb{Z}$  respecto al orden anterior es un conjunto totalmente ordenado, pero no es un conjunto bien ordenado.

### **3. DIVISIBILIDAD EN EL CONJUNTO DE LOS NÚMEROS ENTEROS**



Dados  $a, b \in \mathbb{Z}$ . Diremos que  $a$  es **divisor** de  $b$ ,  $a$  **divide** a  $b$ ,  $a$  es **factor** de  $b$  y lo representamos mediante  $a \mid b$ , si y solo si existe un número entero  $c$  tal que  $a \cdot c = b$ , es decir,

$$a \mid b \Leftrightarrow \exists c \in \mathbb{Z} \text{ tal que } a \cdot c = b$$

En tal caso también diremos que  $b$  es **múltiplo** de  $a$ , es decir,  $b \in \langle a \rangle$ .

**Proposición 4.18.** La relación ser divisor en  $\mathbb{Z}$  es reflexiva y transitiva, es decir, es un preorden en  $\mathbb{Z}$ .

Observación: 1 es divisor y 0 es múltiplo de cualquier entero.



Un número entero  $p \in \mathbb{Z}$  se dice que es **primo** si y sólo si  $p \neq 0$ ,  $\pm 1$  y sus únicos divisores son el  $\pm 1$  y  $\pm p$ .

Diremos que un número entero es **compuesto** si no es primo, es decir, tiene divisores distintos de si mismo y de la unidad.

Observación: Si  $p$  es primo entonces  $-p$  es primo.



***Teorema 4.21. (Teorema Fundamental de la Aritmética)*** Todo número entero distinto de  $\pm 1$  y  $0$  admite una descomposición única (salvo el orden y opuestos) como producto de números primos positivos, es decir:

$$\forall a \in \mathbb{Z} - \{0, \pm 1\}, \quad a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{con } p_i < p_j \text{ si } i < j.$$

A la expresión anterior se le conoce como la **descomposición en factores primos** de  $a$ .



**Proposición 4.22.** Dado  $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \in \mathbb{Z}$  y  $a \neq 0, \pm 1$ , un elemento  $b \in \mathbb{Z}$  es un divisor de  $a$  si y sólo si todos los factores primos de  $b$  son factores primos de  $a$  con exponentes menores o iguales a los de  $b$ , es decir:

$$b = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} \quad \text{con } 0 \leq \beta_i \leq \alpha_i, \forall i = 1, \dots, r.$$

Dados  $a, b \in \mathbb{Z} - \{0, \pm 1\}$ . Llamaremos **máximo común divisor** de  $a$  y  $b$  al número entero  $d \in \mathbb{Z}$  que satisface:

- i)  $d \mid a$  y  $d \mid b$ ,
- ii) Si existe  $d' \in \mathbb{Z}$  tal que  $d' \mid a$  y  $d' \mid b$ , entonces  $d' \mid d$ .

Al máximo común divisor de  $a$  y  $b$  lo denotamos por:

$$d = (a, b) = \text{m.c.d}\{a, b\}.$$



Dados  $a, b \in \mathbb{Z} - \{0, \pm 1\}$ . Llamaremos **mínimo común múltiplo** de  $a$  y  $b$  al número entero  $M \in \mathbb{Z}$  que satisface:

- i)  $a \mid M$  y  $b \mid M$ ,
- ii) Si existe  $M' \in \mathbb{Z}$  tal que  $a \mid M'$  y  $b \mid M'$ , entonces  $M \mid M'$ .

Al mínimo común múltiplo de  $a$  y  $b$  lo denotamos por:

$$M = [a, b] = \text{m.c.m}\{a, b\}.$$

De forma análoga podemos definir el máximo común divisor y mínimo común múltiplo de  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ .



**Proposición 4.23.** Dados  $a$  y  $b \in \mathbb{Z} - \{0, \pm 1\}$  tales que:

$$a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s} \cdot p_{s+1}^{\alpha_{s+1}} \dots p_r^{\alpha_r}$$

$$b = \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_s^{\beta_s} \cdot p_{s+1}^{\beta_{s+1}} \dots p_r^{\beta_r}$$

con  $\alpha_i, \beta_j \geq 0, \forall i = 1, 2, \dots, r$ . Entonces:

$$d = (a, b) = \pm p_1^{f_1} \cdot p_2^{f_2} \dots p_s^{f_s} \cdot p_{s+1}^{f_{s+1}} \dots p_r^{f_r}$$

con  $f_i = \min\{\alpha_i, \beta_i\} \forall i = 1, 2, \dots, r$  y

$$M = [a, b] = \pm p_1^{g_1} \cdot p_2^{g_2} \dots p_s^{g_s} \cdot p_{s+1}^{g_{s+1}} \dots p_r^{g_r}$$

con  $g_i = \max\{\alpha_i, \beta_i\} \forall i = 1, 2, \dots, r$ .



**Proposición 4.24.** Sean  $a$  y  $b \in \mathbb{Z} - \{0, \pm 1\}$ , entonces  
$$[a, b] \cdot (a, b) = a \cdot b.$$

**Teorema 4.25. (Algoritmo de la división)** Sean  $a$  y  $b \in \mathbb{Z}$ , y  $b \neq 0$ . Entonces existen números enteros  $q$  y  $r$  tales que  
$$a = b \cdot q + r$$
  
con  $0 \leq r < |b|$ . Además  $q$  y  $r$  son únicos.

**Proposición 4.26. (Identidad de Bezout)** Dados  $a, b \in \mathbb{Z} - \{0, \pm 1\}$ . Si  $d = (a, b)$  entonces existen unos únicos número  $u, v \in \mathbb{Z}$  tales que  $d = a \cdot u + b \cdot v$ .





Dos número enteros  $a$  y  $b$  diremos que son **primos relativos** si y sólo si  $d = (a, b) = 1$ .

**Corolario 4.27.** Si  $a$  y  $b \in \mathbb{Z} - \{0, \pm 1\}$  son primos relativos, entonces existen unos únicos números  $u, v \in \mathbb{Z}$  tales que  $1 = a \cdot u + b \cdot v$ .

**Lema 4.28.** Dados  $a, b$  números enteros y  $b \neq 0$ , si  $a = b \cdot q + r$  con  $q, r \in \mathbb{Z}$  dados por el algoritmo de la división, entonces  $(a, b) = (b, r)$ .

Este teorema nos facilita un método para calcular el máximo común divisor de dos números y que conocemos con el nombre de **Algoritmo de Euclides**




Dados  $a, b \in \mathbb{Z} - \{0, \pm 1\}$ . Como  $(a, b) = (|a|, |b|)$  podemos suponer que  $a \geq b > 0$ . Aplicando el algoritmo de la división entre  $a$  y  $b$  obtenemos dos enteros  $q_1$  y  $r_1$  tales que

$$a = b \cdot q_1 + r_1 \text{ con } 0 \leq r_1 < b,$$

y el problema de calcular el  $\text{mcd}\{a, b\}$  se reduce a calcular el  $\text{mcd}\{b, r_1\}$  que son números más pequeños. De hecho, puede ocurrir que:

- $r_1 = 0$ , entonces  $\text{mcd}\{a, b\} = \text{mcd}\{b, 0\} = b$ .
- $r_1 \neq 0$ , en cuyo caso podemos volver a aplicar el algoritmo de la división a  $b$  y  $r_1$  y obtenemos

$$b = r_1 \cdot q_2 + r_2 \text{ con } 0 \leq r_2 < r_1,$$



y el problema de nuevo se reduce a calcular el  $\text{mcd}\{r_1, r_2\}$ , pudiendo ocurrir que:

- $r_2 = 0$ , y entonces  $\text{mcd}\{a, b\} = \text{mcd}\{b, r_1\} = \text{mcd}\{r_1, 0\} = r_1$
- $r_2 \neq 0$ , y así podríamos volver a aplicar el algoritmo de la división ahora entre  $r_1$  y  $r_2$ , obteniendo

$$r_1 = r_2 \cdot q_3 + r_3 \text{ con } 0 \leq r_3 < r_2.$$

Así sucesivamente se calcularían sucesivas divisiones con restos cada vez más pequeños. Tales números  $r_1 > r_2 > r_3 > \dots$  constituirán una sucesión de números naturales decrecientes y acotada por el 0, tras un número finito de pasos obtendremos un resto igual a  $r_s = 0$ , es decir,  $r_{s-1}$  divide a  $r_{s-2}$ :

$$\begin{aligned} & \dots\dots\dots \\ r_{s-3} &= r_{s-2} \cdot q_{s-1} + r_{s-1} \text{ con } 0 \leq r_{s-1} < r_{s-2}, \\ r_{s-2} &= r_{s-1} \cdot q_s + 0. \end{aligned}$$



y así se tiene:

$$\text{mcd}\{a, b\} = \text{mcd}\{b, r_1\} = \text{mcd}\{r_1, r_2\} = \dots = \text{mcd}\{r_{s-2}, r_{s-1}\} = \text{mcd}\{r_{s-1}, 0\} = r_{s-1},$$

es decir, el máximo común divisor de  $a$  y  $b$  vendrá dado por el último resto distinto de 0.

Ejemplo: Calcular el m.c.d $\{3120, 270\}$



Otro resultado interesante de este algoritmo es que nos facilita la obtención de la Identidad de Bezout, es decir, la obtención de los único número enteros  $u$  y  $v$  tales que

$$r_{s-1} = \text{mcd}\{a, b\} = a \cdot u + b \cdot v$$

De hecho, se tiene el siguiente resultado:

**Lema 4.29.** Para cada  $i \geq 1$ , existe números enteros  $u_i$  y  $v_i$  tales que

$$r_i = a \cdot u_i + b \cdot v_i$$

donde  $r_i$  son los distintos restos que se obtiene al aplicar el algoritmo de Euclides al calcular el  $\text{mcd}\{a, b\}$ .



Tales números vienen dados inductivamente por las formulas:

$$u_i = u_{i-2} - u_{i-1} \cdot q_i, \quad v_i = v_{i-2} - v_{i-1} \cdot q_i,$$

en las que  $q_i$  son los respectivos cocientes de las divisiones. En particular, los números  $u$  y  $v$  de la identidad de Bezout vendrán dados por las formulas:

$$u = u_{s-3} - u_{s-2} \cdot q_{s-1}, \quad v = v_{s-3} - v_{s-2} \cdot q_{s-1}.$$



Otra aplicación del algoritmo de Euclides es el calculo de todas las soluciones enteras de las ecuaciones lineales en dos variables

$$a.x + b.y = c, \quad a, b, c \in \mathbb{Z}.$$


***Teorema 4.30.*** La ecuación anterior tiene solución en  $\mathbb{Z}$  si y sólo si  $(a, b) \mid c$ .

***Proposición 4.31.*** Si  $(x_0, y_0)$  es una solución en  $\mathbb{Z}$  de la ecuación anterior, el resto de soluciones enteras de dicha ecuación vendrán dadas por las formulas:

$$\begin{cases} x = x_0 - k \frac{b}{d} \\ y = y_0 + k \frac{a}{d} \end{cases}$$

## 4. CONGRUENCIAS. SISTEMAS DE CONGRUENCIAS





Sea  $n \in \mathbb{N} - \{0\}$  y  $a, b \in \mathbb{Z}$ . Diremos que **a es congruente con b módulo n** y lo denotamos  $a \equiv b \pmod{n}$  si y sólo si  $a - b$  es múltiplo de  $n$ , es decir,


$$a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } a = b + k.n$$

**Proposición 4.32.** La relación de congruencia es una relación de equivalencia en  $\mathbb{Z}$ . Al conjunto cociente de la relación de congruencia lo denotamos por

$$\mathbb{Z}_n = \mathbb{Z} / \equiv \pmod{n} = \{ \bar{a} / a \in \mathbb{Z} \}$$

y lo llamamos **conjunto de las clases de restos módulo n**.

**Proposición 4.33.**  $a \equiv b \pmod{n}$  si y sólo si al dividir  $a$  y  $b$  entre  $n$  obtenemos el mismo resto. (Demostración ejercicio 4.62).



**Proposición 4.34.** Los elementos de  $\mathbb{Z}_n$  son los distintos restos que se obtienen al dividir entre  $n$ , es decir:  $\mathbb{Z}_n = \{ \overline{0}, \overline{1}, \overline{2}, \dots \}$  y así  $\text{card}(\mathbb{Z}_n) = n$  para  $n > 1$ .

**Proposición 4.35.** La relación “ser congruente módulo  $n$ ” es compatible con la suma y con el producto de números enteros. (Demostración ejercicio 4.64).

Lo anterior nos permite hablar de aritmética modular, esto es, podemos realizar sumas y productos módulo un entero  $n$  como nos enuncia el siguiente:

**Corolario 4.36.** En  $\mathbb{Z}_n$  definimos la suma y el producto de clases de la forma:

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$



**Proposición 4.37.** La suma y el producto en  $\mathbb{Z}_n$  satisface las siguientes propiedades:

i) **Asociativa para la suma,**

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}), \quad \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$$

ii) **Elemento neutro para la suma:**

$$\text{Existe } \overline{0} \in \mathbb{Z}_n \text{ tal que } \overline{0} + \overline{a} = \overline{a} = \overline{a} + \overline{0}, \quad \forall \overline{a} \in \mathbb{Z}_n.$$

iii) **Conmutativa para la suma,**

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}, \quad \forall \overline{a}, \overline{b} \in \mathbb{Z}_n.$$



iv) **Elemento simétrico respecto de la suma,**

$$\forall \bar{a} \in \mathbb{Z}_n, \text{ existe } \overline{-a} \in \mathbb{Z}_n \text{ tal que } (\overline{-a}) + \bar{a} = \bar{0} = \bar{a} + (\overline{-a}).$$

v) **Asociativa para el producto,**

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c}), \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n.$$

vi) **Elemento neutro para el producto:**

$$\text{Existe } \bar{1} \in \mathbb{Z}_n \text{ tal que } \bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}, \quad \forall \bar{a} \in \mathbb{Z}_n.$$

vii) **Conmutativa para el producto,**

$$\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}, \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_n.$$

viii) **Distributivas,**

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}, \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n.$$



Un elemento  $\overline{a} \neq \overline{0}$  en  $\mathbb{Z}_n$  se dice que es un **divisor del cero** si existe otro elemento  $\overline{b} \neq \overline{0}$  en  $\mathbb{Z}_n$  tal que  $\overline{a} \cdot \overline{b} = \overline{0}$ . Diremos que  $\mathbb{Z}_n$  es un **dominio de integridad** si no tiene divisores de cero.

**Proposición 4.38.** Un elemento  $\overline{a} \in \mathbb{Z}_n$  distinto de  $\overline{0}$  es un divisor de cero en  $\mathbb{Z}_n$  si y sólo si  $a$  y  $n$  no son primos relativos, es decir,  $(a, n) \neq 1$ . (Demostración ejercicio 4.69).

**Corolario 4.39.**  $\mathbb{Z}_n$  es un dominio de integridad si y sólo si  $n$  es un número primo. (Demostración ejercicio 4.69).



Un elemento  $\bar{a} \neq \bar{0}$  en  $\mathbb{Z}_n$  es una **unidad** en  $\mathbb{Z}_n$  si tiene inverso (elemento simétrico para el producto), es decir, si existe otro elemento  $\bar{b} \neq \bar{0}$  en  $\mathbb{Z}_n$  tal que  $\bar{a} \cdot \bar{b} = \bar{1}$ . Diremos que  $\mathbb{Z}_n$  es un **cuerpo** si todo elemento no nulo de  $\mathbb{Z}_n$  es una unidad.

**Proposición 4.40.** Un elemento  $\bar{a} \in \mathbb{Z}_n$  distinto de  $\bar{0}$  es una unidad en  $\mathbb{Z}_n$  si y sólo si  $a$  y  $n$  son primos relativos, es decir,  $(a, n) = 1$ . (Demostración ejercicio 4.71).

**Corolario 4.42.**  $\mathbb{Z}_n$  es un cuerpo si y sólo si  $n$  es un número primo. (Demostración ejercicio 4.71).



En la práctica, una forma de encontrar el inverso de  $\bar{a} \in \mathbb{Z}_n$  es ir probando realizando los distintos productos con todos los elementos de  $\mathbb{Z}_n$ , es decir, calcular  $\bar{a} \cdot \bar{1}, \bar{a} \cdot \bar{2}, \bar{a} \cdot \bar{3}, \dots$ , hasta encontrar uno que nos de igual a  $\bar{1}$ . Sin embargo si  $n$  es grande, el método anterior no es el más aconsejable. Otra aplicación de la identidad de Bezout es el cálculo de inversos en  $\mathbb{Z}_n$ :

**Corolario 4.41.** Si  $\bar{a} \in \mathbb{Z}_n$  tal que  $(a, n) = 1$ , entonces el inverso de  $\bar{a}$  en  $\mathbb{Z}_n$  es  $\bar{u}$  donde  $u \in \mathbb{Z}$  tal que  $1 = a.u + n.v$  es la identidad de Bezout.



Las operaciones aritméticas en  $\mathbb{Z}_n$  nos van a permitir plantear ecuaciones o sistemas de ecuaciones en  $\mathbb{Z}_n$ . Así podemos llamar **congruencia lineal** a una ecuación lineal de la forma:

$$a \cdot x + b \equiv c \pmod{n},$$

donde  $a$ ,  $b$ ,  $c$  y  $n$  son números enteros con  $n > 1$  y  $x$  una indeterminada.

De la misma forma que en  $\mathbb{Z}_n$  podemos plantear y resolver ecuaciones lineales, podemos también plantear y resolver **sistemas de congruencias lineales**:

$$x \equiv a_1 \pmod{p_1}$$

$$x \equiv a_2 \pmod{p_2}$$

.....

$$x \equiv a_n \pmod{p_n}$$

con  $a_i, p_i \in \mathbb{Z}$  y  $p_i > 1$ , para todo  $i = 1, 2, \dots, n$ .





**Teorema 4.43. (Teorema Chino del resto)** Sean  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  y  $p_1, p_2, \dots, p_n \in \mathbb{Z}$  tal que  $(p_i, p_j) = 1$  si  $i \neq j$ . Entonces:

- i) Existe  $a \in \mathbb{Z}$  tal que  $a \equiv a_i \pmod{p_i}, \forall i = 1, 2, \dots, n$ .
- ii) Si  $\exists a' \in \mathbb{Z}$  tq  $a' \equiv a_i \pmod{p_i}, \forall i = 1, 2, \dots, n, \Rightarrow a \equiv a' \pmod{p_1 \cdot p_2 \cdot \dots \cdot p_n}$ .

### Algoritmo Chino del resto

Consideremos el sistema de congruencias:

$$\begin{aligned}x &\equiv a_1 \pmod{p_1} \\x &\equiv a_2 \pmod{p_2} \\&\dots\dots\dots \\x &\equiv a_r \pmod{p_r}\end{aligned}$$

tal que  $(p_i, p_j) = 1$  si  $i \neq j$ , entonces el teorema anterior nos asegura que dicho sistema tiene solución.



Paso 1: Llamamos  $M_1 = 1$ ,  $M_2 = p_1$ ,  $M_3 = p_1 \cdot p_2, \dots$ ,  $M_r = p_1 \cdot p_2 \dots p_{r-1}$ .

Paso 2: Hallamos  $u_k \in \mathbb{Z}$  tal que  $u_k \cdot M_k \equiv 1 \pmod{p_k}$ ,  $\forall k=1,2,\dots,r$ .

Paso 3: Hallamos  $b_1 \in \mathbb{Z}$  tal que  $b_1 \equiv a_1 \pmod{p_1}$ .

Paso 4: Hallamos  $w_2 \in \mathbb{Z}$  tal que  $w_2 \equiv (a_2 - b_1) \cdot u_2 \pmod{p_2}$ .

Paso 5: Hallamos  $b_2 = b_1 + w_2 \cdot M_2$

Paso 4bis:  $\forall k \geq 3$  calculamos  $w_k \in \mathbb{Z}$  tal que  $w_k \equiv (a_k - b_{k-1}) \cdot u_k \pmod{p_k}$ .

Paso 5bis:  $\forall k \geq 3$  calculamos  $b_k = b_{k-1} + w_k \cdot M_k$ .

Paso 6: La solución del sistema es  $x = b_r$ .

# 5. SISTEMAS DE NUMERACIÓN



Teniendo en cuenta que el conjunto de números naturales es infinito, necesitamos infinitas palabras para nombrarlos e infinitos símbolos para escribirlos. De aquí la necesidad de buscar un conjunto finito de palabras, símbolos y reglas que nos permitan utilizar los números naturales con precisión y comodidad.

### Definición

Un **sistema de numeración** es un par  $\{S, R\}$  donde  $S$  es un conjunto de símbolos y  $R$  un conjunto de reglas y convenios que utilizamos para nombrar y escribir los números empleando la menor cantidad posible de palabras y símbolos. Los símbolos de  $S$  se llaman **cifras** o **dígitos** y al cardinal del conjunto  $S$  se le llama **base** del sistema de numeración.



El sistema de numeración que usamos contiene 10 dígitos

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

los 10 primeros números naturales y escribimos cada número de derecha a izquierda como una secuencia finita formada a partir de los símbolos anteriores de manera que el valor de dichos símbolos depende de la posición que ocupe:

$$17457 = 1 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0$$



Los primeros en utilizar este sistema fueron los Babilonios hace más de 3000 años, estos los pasaron a los Hindúes que a su vez lo transmitieron a los Árabes 600 años A.C. Estos lo introdujeron en Europa en el año 1200 D.C. Este sistema no fue utilizado por los Egipcios, los Chinos y los Griegos.

Se podría haber utilizado otro entero distinto de 10, de hecho, los Babilonios a veces usaban un sistema de numeración de base 60, los Mayas otro con base 20 y es bien sabido, con la aparición de las computadores ha tenido gran auge al sistema binario (base 2), el sistema octal (base 8) y al sistema hexadecimal (base 16).



Cuando la base del sistema es mayor de 10, se añaden las primeras letras del alfabeto, así para el sistema hexadecimal el conjunto  $S$  viene dado por:

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$$

de manera que  $A = 10$ ,  $B = 11$ ,  $C = 12$ , ...,  $F = 15$ .

### Teorema Fundamental de la Numeración

Sea  $b \geq 2$ , un número entero. Cualquier entero positivo  $n$  se puede escribir de forma única en base  $b$  como:

$$n = d_k b^k + \dots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

con  $d_i \in \mathbb{N}$  y  $0 \leq d_i < b$ ,  $\forall i = 0, 1, \dots, k$ . Para abreviar escribiremos

$$n = (d_k d_{k-1} \dots d_1 d_0)_b$$