Unidad N° 3: Teoría de Números

➢ El Sistema de los Números Naturales

Los números naturales con sus símbolos correspondientes existieron en todas las civilizaciones que tuvieron escritura. Si bien es un concepto formal (creado por la mente del hombre) responde a dos necesidades: **Contar** y **Ordenar.**

Filósofos y matemáticos diseñan teorías para fundamentar la existencia del número natural según los aspectos **1) Cardinal** y **2) Ordinal.**

1) Cardinal: Se conoce la teoría de clases basada en la coordinabilidad de los conjuntos finitos.
Dos conjuntos finitos son **Coordinables** si entre ellos es posible definir una función biyectiva. Esta relación es de equivalencia y en la familia de conjuntos finitos se forman clases de equivalencia. A cada clase se le da un nombre (en símbolos) y se lo llama número cardinal del conjunto

2) Ordinal: Distintas teorías matemáticas fundamentan el carácter ordinal. Veremos la teoría axiomática de PEANO porque nos interesa conocer el axioma 5 que es la base para los procesos de inducción y recurrencia. De esta teoría solamente presentaremos los axiomas.

AXIOMAS DE PEANO

- **Conceptos Primitivos:**
  - Un conjunto no vacío $\mathbb{N}$.
  - Un elemento particular llamado **uno** "$\mathbf{1}$".
  - Una relación en $\mathbb{N}$ llamada ***"siguiente"***.

- **Axioma 1:** El "$\mathbf{1}$" pertenece a $\mathbb{N}$.
- **Axioma 2:** Todo elemento de $\mathbb{N}$ tiene uno y sólo un siguiente en $\mathbb{N}$.
- **Axioma 3:** El "$\mathbf{1}$" no es siguiente de ningún elemento de $\mathbb{N}$.
- **Axioma 4:** Elementos distintos de $\mathbb{N}$ tienen siguientes distintos.
- **Axioma 5:** Inducción o Recurrencia
  Sea $\boldsymbol{P}$ un conjunto no vacío de $\mathbb{N}$
  Si: $\mathbf{1} \in \boldsymbol{P}$
  $\boldsymbol{h} \in \boldsymbol{P}$ entonces el siguiente de h pertenece a $\boldsymbol{P}$
  Luego $\boldsymbol{P} = \mathbb{N}$

Nota: La teoría de PEANO continúa definiendo, a partir de los axiomas, las operaciones SUMA y MULTIPLICACION en $\mathbb{N}$ y demostrando propiedades. No desarrollaremos dicha teoría.

Recordamos: $+$ y $\cdot$ son Leyes de Composición Interna en $\mathbb{N}$. Además $+$ y $\cdot$ son asociativas y conmutativas.
El "$\mathbf{1}$" es neutro de la multiplicación.

Ejemplos de definición por recurrencia
$a \in \mathbb{N}, n \in \mathbb{N}$
Potenciación : ¿a^n?
Definimos $\begin{cases} a^1 \overset{\text{def}}{=} a \\ a^n = a.a^{n-1} \quad si\ n > 1 \end{cases}$

Ejemplo
$a^6 = a.a^5 = a.a.a^4 = a.a.a.a^3 =$
$= a.a.a.a.a^2 = a.a.a.a.a.a^1 = a.a.a.a.a.a$

Otra forma: $n \in \mathbb{N}_0$
$\begin{cases} a^0 \overset{\text{def}}{=} 1 \\ a^n = a.a^{n-1} \quad si\ n > 0 \end{cases}$

Factorial de un número Natural: $¿n!?$

$n \in \mathbb{N}$

Definimos $\begin{cases} 1! \overset{def}{=} 1 \\ n! = n.(n-1)! \quad si\ n > 1 \end{cases}$

Ejemplo

$5! = 5.4! = 5.4.3! = 5.4.3.2! = 5.4.3.2.1! = 5.4.3.2.1$

Otra forma: $n \in \mathbb{N}_0$

$\begin{cases} 0! \overset{def}{=} 1 \\ n! = n.(n-1)! \quad si\ n > 0 \end{cases}$

Orden en $\mathbb{N}$

$a, b \in \mathbb{N}$

$$a < b \text{ si y sólo si existe } n \in \mathbb{N} \ / \ a + n = b$$

Ejemplo: $7 < 15$, $\exists\, n = 8 \ \in \mathbb{N} \ / \ 7 + 8 = 15$

Esta relación es Arreflexiva, Asimétrica y Transitiva. Por lo tanto es un **Orden Estricto Total**

A partir de la relación $<$ se definen los siguientes ordenes:

$a, b \in \mathbb{N}$

- $a \leq b \ si \ (a < b \ \vee \ a = b)$ **Orden Amplio Total**
- $a > b \ si \ b < a$ **Orden Estricto Total**
- $a \geq b \ si \ (a > b \ \vee \ a = b)$ **Orden Amplio Total**

Nota: Los naturales ordenados por la relación de $<$ verifican el **Principio de Buena Ordenación.**

Todo conjunto no vacío de números naturales tiene ***Mínimo***

A los números naturales ordenados se los llama **Sucesión** de números naturales.

Las relaciones de orden presentadas anteriormente para los números Naturales son compatibles con las operaciones SUMA y MULTIPLICACION, lo cual permite trabajar con desigualdades.

Propiedades o Leyes de Monotonía

I. **SUMA**

$i)\ a < b \ \Rightarrow a + c < b + c$

$ii)\ (a < b \wedge \ c < d) \ \Rightarrow a + c < b + c$

II. **MULTIPLICACION**

$i)\ a < b \ \Rightarrow a.c < b.c$

$ii)\ (a < b \wedge \ c < d) \ \Rightarrow a.c < b.c$

Sucesión

A partir del conjunto ordenado de los números naturales es posible ordenar cualquier conjunto de objetos no numéricos o numéricos. Este ordenamiento se hace mediante una función con dominio en los naturales y recorrido en el conjunto que queremos ordenar.

$S: \mathbb{N} \longrightarrow A$

$n \longmapsto S(n) = a_n$

Ejemplo: $1 \longrightarrow S(1) = a_1$

$2 \longrightarrow S(2) = a_2$

$\vdots$

$n \longrightarrow S(n) = a_n$ $\in A$

A la función S se la identifica con el conjunto ordenado de sus imágenes.
Esta identificación

$$S \leftrightarrow \{a_1, a_2, \dots, a_n\}$$
$$S = \{a_n\} \in \mathbb{N}$$

Ejemplo: una sucesión es numérica si el conjunto de llegada es un conjunto de números.

1) $1 \longrightarrow 1$, $2 \longrightarrow 4$, $3 \longrightarrow 3$, $4 \longrightarrow 16$, ……., $n \longrightarrow n^2$

2) $1 \longrightarrow 2$, $2 \longrightarrow 4$, $3 \longrightarrow 6$, $4 \longrightarrow 8$, ……., $n \longrightarrow 2n$

3) $1 \longrightarrow -\sqrt{5}$, $2 \longrightarrow \sqrt{5}$, $3 \longrightarrow -\sqrt{5}$, $4 \longrightarrow \sqrt{5}$, ….., $n \longrightarrow (-1)^n\sqrt{5}$

Observación:

- Si el dominio de la función es un subconjunto finito de números naturales tenemos una SUCESIÓN FINITA.

Ejemplo: $\{1,2,3,4,5\} \longrightarrow A$

$$\left.\begin{array}{l} S(1) = a_1 \\ S(2) = a_2 \\ S(3) = a_3 \\ S(4) = a_4 \\ S(5) = a_5 \end{array}\right\} \text{Sucesión Finita}$$
$$\{a_1, a_2, a_3, a_4, a_5\} = \{a_i\} \text{ con } i = 1..5$$

- Si la sucesión finita es numérica, es posible sumar los términos de dicha sucesión.

Si A es un conjunto numérico

$$a_1 + a_2 + a_3 + a_4 + a_5$$

SMATORIA en símbolos

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + a_3 + \cdots + a_n \quad Suma\ finita$$

Ejemplos:

1) $\sum_{k=1}^{6} \frac{3k}{k+1} = 3.\frac{1}{2} + 3.\frac{2}{3} + 3.\frac{3}{4} + 3.\frac{4}{5} + 3.\frac{5}{6} + 3.\frac{6}{7}$

2) $5 - 10 + 15 - 20 + 25 - 30 + 35 = \sum_{k=1}^{7} (-1)^{k+1}.5k$

Propiedades de las Sumatorias

Utilizando las propiedades asociativa, conmutativa y distributiva de la suma y multiplicación de números, se prueba que las siguientes propiedades son verdaderas.

I) $\sum_{i=1}^{n} c = n.c$ II) $\sum_{i=1}^{n} c\,a_i = c\sum_{i=1}^{n} a_i$ III) $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i)$

Ejemplo

$$\sum_{k=1}^{8} (5k+2) + \sum_{k=1}^{8} (-k+4) = \sum_{k=1}^{8} (5k+2) + (-k+4) = \sum_{k=1}^{8} (4k+6) = 2\sum_{k=1}^{8} (2k+3)$$

Recurrencia

Problema:

En un laboratorio se realiza un cultivo de bacterias. Se conoce que el número de bacterias se duplica al finalizar cada hora. Si se inicia el cultivo con 5 bacterias ¿Cuántas baterías tenemos después de 6 horas?

.

$a_0 = 5$

Al pasar

$1\ hora \longrightarrow a_1 = 2.a_0 = 2.5 = 10$
$2\ horas \longrightarrow a_2 = 2.a_1 = 2.10 = 20$
$3\ horas \longrightarrow a_3 = 2.a_2 = 2.20 = 40$
$4\ horas \longrightarrow a_4 = 2.a_3 = 2.40 = 80$
$5\ horas \longrightarrow a_5 = 2.a_4 = 2.80 = 160$
$6\ horas \longrightarrow a_6 = 2.a_5 = 2.160 = 320$

Valor inicial $\longrightarrow a_0$
Regla $\longrightarrow a_n = 2.a_{n-1}$ con $n \in \mathbb{N}$

Observamos de esta manera que una relación de Recurrencia tiene dos partes:

I. Condición o Condiciones Iniciales
Son el o los valores iniciales de la sucesión.

II. Regla de Recurrencia
Es una expresión que da el valor en cada posición de la sucesión en función de los valores anteriores.

Se dice que una sucesión es solución de una relación de recurrencia si verifica las condiciones iniciales y la regla de recurrencia.

Además:

1. **<u>El grado de la recurrencia</u>** es k si tiene k-valores iniciales y la regla hace referencia a los k-valores iniciales.
2. **<u>La recurrencia es lineal</u>** si la regla de recurrencia tiene sumas de múltiplos de valores anteriores.
3. **<u>La recurrencia es homogénea</u>** si no tiene términos independientes de los valores anteriores.

Ej. 1) En el ejemplo de las bacterias

$a_0 = 5$ ⎫ Recurrencia de Grado 1
⎬ Lineal
$a_n = 2.a_{n-1}$ ⎭ Homogénea

Ej. 2) Sucesión de Fibonacci

$a_1 = 1 \ \wedge \ a_2 = 1$ ⎫ Recurrencia de Grado 2
⎬ Lineal
$a_n = a_{n-2} + a_{n-1}$ ⎭ Homogénea

Ej. 2) Sucesión de Fibonacci

$a_1 = 2 \ \wedge \ a_2 = 1$ ⎫ Recurrencia de Grado 2
⎬ Lineal
$a_n = a_{n-1}^2 + 1 \quad \text{con} \quad n \geq 2$ ⎭ Homogénea

Método de Inducción Completa

Problema:

Se desea sumar ordenadamente los n primeros números naturales impares.

$$\begin{aligned}
n=1 &\longrightarrow 1 && \longrightarrow 1^2\\
n=2 &\longrightarrow 1+3=4 && \longrightarrow 2^2\\
n=3 &\longrightarrow 1+3+5=9 && \longrightarrow 3^2\\
n=4 &\longrightarrow 1+3+5+7=16 && \longrightarrow 4^2\\
n=5 &\longrightarrow 1+3+5+7+9=25 && \longrightarrow 5^2\\
n=6 &\longrightarrow 1+3+5+7+9+11=36 && \longrightarrow 6^2\\
n=7 &\longrightarrow 1+3+5+7+9+11+13=49 && \longrightarrow 7^2
\end{aligned}$$

Pareciera ser que la suma de los n primero números naturales impares es n^2

$$¿\sum_{k=1}^{n} 2k-1=n^2\ \ ?$$

Es imposible hacer todas las verificaciones ya que los números naturales son infinitos. Veremos el método de **Inducción Completa** fundamentado en el **Axioma 5 de Peano** que nos permitirá asegurar que la propiedad anterior es verdadera para cualquier $\boldsymbol{n}$ Natural.

Teorema: (Método de inducción completa)

Sea $P(n)$ una función proposicional de variable natural, es decir $n \in \mathbb{N}$

$$Si\ P(1) es\ V\ y\ [\forall\ h:\ (P(h)\ es\ V \implies P(h+1)\ es\ V)]\ entonces\ P(n)\ es\ V \quad \forall\ n \in \mathbb{N}$$

Demost:

- Sea S el conjunto de verdad de $P(n)$. $S \subset \mathbb{N}$
- Por hipótesis i) $P(1)\ es\ V$, es decir, $1 \in S$
  ii) $P(h)\ es\ V \implies P(h+1)\ es\ V$, es decir: $h \in S \implies h+1 \in S$
- Luego, por **Ax. 5** de Peano
  $S = \mathbb{N}$, es decir $P(n)\ es\ V \quad \forall\ n \in \mathbb{N}$

Nota: Para aplicar este teorema en cualquier función proposicional de variable natural se debe comprobar que la hipótesis del teorema se cumple. Si esto es cierto se concluye que P(n) es verdadera para cualquier número natural.

Ejemplo 1

La suma de los n primeros números naturales es $\frac{n(n+1)}{2}$

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\ \ "demostrar\ por\ induccion\ completa"$$

1. Probar que $P(1)\ es\ V$

$$n=1\ ;\ \left.\begin{array}{l}\sum_{k=1}^{1} k = 1\\ \frac{1(1+1)}{2} = 1\end{array}\right] = P(1)\ es\ V$$

2. Suponer la verdad de $P(h)$

$$n=h\ ;\ \sum_{k=1}^{h} k = \frac{h(h+1)}{2} \quad Hipotesis\ Inductiva$$

3. Demostrar que $P(h+1)\ es\ V$

$$n=h+1\ ;\ \sum_{k=1}^{h+1} k = \frac{(h+1)(h+2)}{2} \quad demostrar$$

$$\sum_{k=1}^{h+1} k = 1+2+3+\cdots+h+(h+1) = \sum_{k=1}^{h} k+(h+1) =$$

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

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

Luego, por Teorema de Inducción Completa $P(n) es\ V\ \ \forall\ n \in \mathbb{N}$

Ejemplo 2

La suma de los n primeros números naturales impares es n^2

$$\sum_{k=1}^{n} 2k-1 = n^2 \quad "demostrar\ por\ induccion\ completa"$$

2. Probar que $P(1)\ es\ V$

$$n=1\ ;\ \sum_{k=1}^{1} 2k-1 = 2.1-1 = 1 \\ 1^2 = 1 \Big\} = P(1)\ es\ V$$

3. Suponer la verdad de $P(h)$

$$n=h\ ;\ \sum_{k=1}^{h} 2k-1 = h^2 \quad Hipotesis\ Inductiva$$

1. Demostrar que $P(h+1)\ es\ V$

$$n=h+1\ ;\ \sum_{k=1}^{h+1} 2k-1 = (h+1)^2 \quad demostrar$$

$$\sum_{k=1}^{h+1} 2k-1 = 1+3+4+\cdots+(2h-1)+(2(h+1)-1) =$$

$$= \sum_{k=1}^{h} 2k-1+(2(h+1)-1) = h^2+2h+1 = (h+1)^2$$

Luego, por Teorema de Inducción Completa $P(n) es\ V\ \forall\ n \in \mathbb{N}$

➢ Los Números Enteros

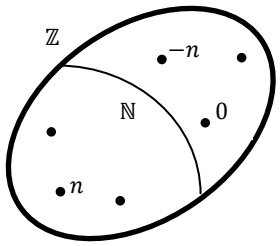
La familia de ecuaciones $a+x=b$, con a y b números naturales, son resolubles o no dependiendo de la relación que existe entre a y b de la siguiente manera:

- Si $a<b$ entonces $\exists\ n \in \mathbb{N}\ /\ \ a+n=b$. Luego $x=n$
- Si $\left.\begin{matrix} a=b \\ \vee \\ a>b \end{matrix}\right\}$ entonces $\nexists\ n \in \mathbb{N}\ /\ a+n=b$. Luego la ecuación no tiene solución en $\mathbb{N}$

Como consecuencia de esta situación, a los números Naturales se le agrega todos esos números que son soluciones de las ecuaciones no resolubles en $\mathbb{N}$. Estos números son el **cero** y los **números negativos.** De esta forma, los naturales más el cero y más los números negativos conforman un nuevo conjunto numérico llamado **Números Enteros** y se denota con $\mathbb{Z}$.

Ej:

$5+x=5 \implies x=0$
$5+x=3 \implies x=-2$ } nros negativos



Operaciones en $\mathbb{Z}$

Suma: $+ : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$
$(a,b) \mapsto a+b \in \mathbb{Z}$

Multiplicación: $\bullet : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$
$(a,b) \mapsto a \bullet b \in \mathbb{Z}$

Estructura Algebraica de los Números Enteros

Propiedad: Los números enteros con la suma y la multiplicación tienen estructura de *Anillo Conmutativo con Unidad.*

Demost: Se prueba que se verifican las siguientes propiedades

1) $+$ es **Asociativa**
2) $+$ es **Conmutativa**
Existencia de **Neutro** para $+$ puesto que
$\exists\, 0 \in \mathbb{Z} \,/\, \forall\, a \in \mathbb{Z} : a + 0 = 0 + a = a$
3) Existencia de **Opuesto** en $+$ puesto que
$\forall a \in \mathbb{Z} : \exists (-a) \in \mathbb{Z} \,/\, a + (-a) = (-a) + a = 0$

SUMA
$(\mathbb{Z}, +)$ es Grupo Conmutativo o abeliano

4) . es **Asociativa**
5) . es **Conmutativa**
6) Existencia de Neutro para . puesto que
$\exists\, 1 \in \mathbb{Z} \,/\, \forall\, a \in \mathbb{Z} : a \,.\, 1 = 1 \,.\, a = a$
7) . es Distributiva con respecto a $+$ puesto que
$\forall a, b, c \in \mathbb{Z} : a \,.\, (b + c) = a.b + a.c$

MULTIPLICACION

$(\mathbb{Z}\,, +, .)$ **ANILLO CONMUTATIVO CON UNIDAD**

Orden en los Números Enteros

Sean $a, b \in \mathbb{Z}$

$$a < b \;\; si \;\; \exists\, n \in \mathbb{N} \;/\; a + n = b$$

- Se prueba que es un Orden Estricto Total
- A partir de " $<$ " se define " $\leq, >, \geq$ "

$\mathbb{Z}$ es un Anillo Conmutativo con Unidad Ordenado

- El orden en los enteros es compatible con la suma y la multiplicación.
  Leyes de Monotonía
  Sean $a, b, c, d \in \mathbb{Z}$

  1. $a < b \implies a + c < b + c$

  $(a < b \wedge\; c < d) \implies a + c < b + d$

  2. $(a < b \wedge\; c > 0) \implies a.c < b.c$

  $(a < b \wedge\; c = 0) \implies a.c = b.c$

  $(a < b \wedge\; c < 0) \implies a.c > b.c$

Resta en $\mathbb{Z}$

Sean $a, b \in \mathbb{Z}$

$$a - b \overset{\text{def}}{=} a + (-b)$$

Podemos decir entonces que

$$\text{Sean } a, b \in \mathbb{Z} : \;\; a < b \;\; si \;\; b - a \;\; \in \mathbb{N}$$

Teoría de Divisibilidad en $\mathbb{Z}$

Definición: La relación ***"divisor de"*** se define de la siguiente manera.

Sea $a \in \mathbb{Z} - \{0\}$ y $b \in \mathbb{Z}$:

$$a/b \text{ si y solo si existe } t \in \mathbb{Z} \text{ tal que } a.t = b$$

Se lee "$\boldsymbol{a}$ es divisor de $\boldsymbol{b}$"
o bien
"$\boldsymbol{b}$ es múltiplo de $\boldsymbol{a}$"

Ejemplo:
$-3/21$ pues $\exists\, t = -7$ tal que $(-3).(-7) = 21$
$5 \not| 21$ pues $\nexists\, t \in \mathbb{Z}$ tal que $5 \,.\, t = 21$
$4/0$ pues $\exists\, t = 0$ tal que $4.0 = 0$

Propiedades de la relación **" divisor de "**

1) $a \in \mathbb{Z} - \{0\}$ tiene siempre divisores: $1, -1, a, -a$

Demost:

$1/a$ pues $\exists\, t = a$ tal que $1.a = a$
$-1/a$ pues $\exists\, t = -a$ tal que $(-1).(-a) = a$
a/a pues $\exists\, t = 1$ tal que $a.1 = a$

2) La relación "divisor de" es *reflexiva* y *transitiva*

Demost:

Reflexiva: todo entero no nulo es divisor de sí mismo; a/a (por Prop.1)

Transitiva: $a, b \in \mathbb{Z} - \{0\} \wedge c \in \mathbb{Z}$: $\underbrace{(\boldsymbol{a}/\boldsymbol{b} \wedge \boldsymbol{b}/\boldsymbol{c})}_{\text{Hipótesis}} \Rightarrow \underbrace{\boldsymbol{a}/\boldsymbol{c}}_{\text{Tesis}}$ probar que $\exists\, t \in \mathbb{Z}$ tal que $a.t = c$

Partimos de las hipótesis

a/b pues $\exists\, k \in \mathbb{Z}$ tal que $a.\boldsymbol{k} = b$
b/c pues $\exists\, h \in \mathbb{Z}$ tal que $b.\boldsymbol{h} = c$

$b.h = c$
$a.\boldsymbol{k}.c = c$

$a.(k.c) = c \Rightarrow a.\boldsymbol{t} = c \Rightarrow \boldsymbol{a}/\boldsymbol{c}$ ∴ se demuestra la tesis

Ejemplo $(-3/15 \wedge 15/60) \Rightarrow (-3/60)$

$(-3).(-5) = 15 \;\wedge\; 15.4 = 60 \;\Rightarrow\; (-3).(-\mathbf{5}).\mathbf{4} = 60 \Rightarrow (-3).(-\mathbf{20}) = 60 \Rightarrow -3/60$

3) $a, b \in \mathbb{Z} - \{0\}$: $(a/b \;\wedge\; b/a) \Rightarrow (a = b \;\vee\; a = -b)$

Obs: Si la relación "divisor de" está definida en los naturales o en un subconjunto de los enteros que no tenga números opuestos se verifica la propiedad antisimétrica y la relación es un **Orden Amplio Parcial**

4) $d \in \mathbb{Z} - \{0\} \wedge a, b \in \mathbb{Z} : \underbrace{\left(d/a \wedge b/a\right)}_{\text{Hipótesis}} \Longrightarrow \underbrace{d/a+b}_{\text{Tesis}}$ ⟶ Probar que $\exists\, h \in \mathbb{Z} \,/\, d.h = a + b$

Demost.

$d/a \Longrightarrow \exists\, \boldsymbol{t} \in \mathbb{Z} \,/\, d.\boldsymbol{t} = a$

$d/b \Longrightarrow \exists\, \boldsymbol{k} \in \mathbb{Z} \,/\, d.\boldsymbol{k} = b$

$$a + b = d.\boldsymbol{t} + d.\boldsymbol{k} = d(\underbrace{\boldsymbol{t} + \boldsymbol{k}}_{h}) = d.h \Longrightarrow d/a+b$$

5) $d \in \mathbb{Z} - \{0\} \wedge t, k \in \mathbb{Z} : \underbrace{d/a}_{\text{Hipótesis}} \Longrightarrow \underbrace{d/k.a}_{\text{Tesis}}$ ⟶ Probar que $\exists\, h \in \mathbb{Z} \,/\, d.h = k.a$

Demost.

$d/a \Longrightarrow \exists\, \boldsymbol{t} \in \mathbb{Z} \,/\, \underbrace{d.\boldsymbol{t}}_{\downarrow} = a$

$$k.a = \boldsymbol{k}.d.\boldsymbol{t} = d.(\underbrace{\boldsymbol{k}.\boldsymbol{t}}_{h}) = d.h$$

<u>Nota</u>: Dados los números enteros $\boldsymbol{a}$ y $\boldsymbol{b}$, se llama **<u>Combinación Lineal Entera</u>** a toda expresión de la forma

$k.\boldsymbol{a} + t.\boldsymbol{b}$ con k y t enteros cualesquiera

Ej.

$a = -15 \wedge b = 42$

$7.(-15) + 14.42$ donde $k = 7 \wedge t = 14$

$(-1).(-15) + 35.42$ donde $k = (-1) \wedge t = 35$

Aplicando las propiedades 4 y 5 se prueba que si un número entero es divisor de dos números enteros, entonces también es divisor de cualquier combinación lineal entera de ellos.
Esta propiedad se puede generalizar para un número **n** finito cualquiera de enteros.

6) $d \in \mathbb{Z} - \{0\}$ y $a_1, a_2, \ldots, a_n$ números enteros

$$\left(d/a_1 \wedge d/a_2 \wedge \ldots \wedge d/a_n\right) \Longrightarrow d/k_1.a_1 + k_2.a_2 + \ldots + k_n.a_n$$

Con $k_1, k_2, \ldots, k_n$ números enteros cualesquiera

➢ **Algoritmo de la División Entera** (Algoritmo de Euclides)

Teorema: Sean a y b números enteros con $b \neq 0$

Entonces existen y son únicos los enteros $\boldsymbol{c}$ y $\boldsymbol{r}$ que verifican:

$$\begin{array}{r|l} a & b \\ \hline r & = c \end{array}$$

i. $a = c.\boldsymbol{b} + \boldsymbol{r}$

ii. $0 \leq \boldsymbol{r} < |\boldsymbol{b}|$

Demost.

Euclides probó que el teorema es verdadero para todas las situaciones de a y b con respecto al signo.

Ej.

$a = 23 \ \wedge \ b = 5 \quad \Rightarrow \quad 23 = \mathbf{4}.5 + \mathbf{3}$

$a = 23 \ \wedge \ b = -5 \quad \Rightarrow \quad 23 = (-\mathbf{4}).(-5) + \mathbf{3}$

$a = -23 \ \wedge \ b = 5 \quad \Rightarrow \quad -23 = (-\mathbf{5}).5 + \mathbf{2}$

$a = -23 \ \wedge \ b = -5 \Rightarrow \quad -23 = \mathbf{5}.(-5) + \mathbf{2}$

Obs: Si b/a entonces $r = 0$

Máximo común divisor

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$.

Se dice que m es el máximo común divisor de a y b si verifica:

1) $m/a \ \wedge \ m/b$

2) $\left(d/a \ \wedge \ d/b\right) \Rightarrow d \leq m$

$\left(d/a \ \wedge \ d/b\right) \Rightarrow d/m$

Ejemplo:

-60 ⩓ 48 = 12

15 ⩓ 16 = 1

0 ⩓ (-22) = 22

0 ⩓ 0 ∄

Nota:

$$a \barwedge b = (-a) \barwedge b = a \barwedge (-b) = (-a) \barwedge (-b)$$

Teorema de la Existencia del máximo común divisor

Dados dos números enteros a y b no ambos nulos existe y es único el máximo común divisor entre ellos. Además $m = a \barwedge b$ se puede escribir como combinación lineal entera de a y b de la siguiente manera $a \barwedge b = \boldsymbol{k}.a + \boldsymbol{t}.b$ con $\boldsymbol{k}$ y $\boldsymbol{t}$ entero.

Ejemplo:

$-60 \barwedge 48 = 12 \Rightarrow 12 = (-1).(-60) + (-1).48$

$15 \barwedge 16 = 1 \Rightarrow 1 = (-1).15 + 1.16$

$-7 \barwedge 12 = 1 \Rightarrow 1 = 5.(-7) + 3.1$

Números Coprimos o Primos Relativos

Dos números enteros a y b son coprimos o primos relativos si el máximo común divisor entre ellos es 1.

Ej $21 \perp (-40) = 1$

Propiedades

1) El número 1 se puede escribir como combinación lineal entera de números enteros coprimos.
a y b coprimos $\Longrightarrow \ 1 = k.a + t.b$

Ej $21 \perp (-40) = 1 \Rightarrow 1 = (-\mathbf{19}).21 + (-\mathbf{10}).(-40)$

Si a y b no son coprimos por ej $a = 10$ y $b = 15$; $10 \quad 15 = 5 \Rightarrow {}^{5}/_{k.10 + t.15}$ múltiplo de 5, por lo tanto no puede dar 1

El teorema anterior nos asegura que el máximo común divisor, que en este caso es "1", se escribe como combinación lineal entera de los coprimos.

2) Regla de Oro de la Aritmética
Sea $d \in \mathbb{Z} - \{0\}$ y $a, b \in \mathbb{Z}$

$$\left({}^{d}/_{a.b} \ \wedge \ \boldsymbol{d}\ es\ coprimo\ con\ \boldsymbol{a}\right) \Longrightarrow {}^{d}/_{a}$$

Ej
${}^{4}/_{4.3} \ \wedge \ 4\ coprimo\ con\ 3 \ \Longrightarrow \ {}^{4}/_{4}$

Obs: Si se saca la condición "d es coprimo con a" la propiedad no se cumple.

Ej
${}^{4}/_{2.6}$ pero 4 no es coprimo con 2 ; resulta entonces ${}^{4}\!\not/_{2} \ \wedge \ {}^{4}\!\not/_{6}$
pero 4 no es coprimo con 6

Número Primo

Un número entero $p \neq 1$ es primo si sus únicos divisores son $1, -1, p, -p$.

Ej. : $5,7, -13, 2, \ldots$

Obs:

Probaremos que todo número entero se puede descomponer de manera única como producto de números primos. Para lo cuál de ahora en adelante trabajaremos solamente con los números primos $p > 1$.

Propiedades de los Números Primos

1) Sea $a \in \mathbb{Z}$ y p un número primo, entonces "p es coprimo con a" o "p es divisor de a"
Demost.

$$a \perp p = \begin{cases} 1 \Longrightarrow "a \text{ y } b \text{ son coprimos"} \\ p \Longrightarrow "p \text{ es divisor de } a" \end{cases}$$

Ej
$5 \perp 8 = 1$ son coprimos
$5 \perp (-15) = 5 \Longrightarrow {}^{5}/_{-15}$

2) Si p y q son números primos distintos entonces son coprimos.
Demost.

$$p \perp q = 1$$
$$1 \quad p \quad 1 \quad q$$

3) Regla de Oro para los números primos
Sea p un numero primo y $a, b \in \mathbb{Z}$

$$p/_{a.b} \Longrightarrow \left(p/_{a} \vee p/_{b}\right)$$

Demost.

- Si $p\not/_{a}$ por proposición 1 "p es coprimo con a", entonces (por Regla de Oro) $p/_{b}$
- Si $p\not/_{b}$ por proposición 1 "p es coprimo con b", entonces (por Regla de Oro) $p/_{a}$

Generalización

Si un número primo es divisor de un producto de varios números enteros, entonces es divisor de alguno de esos números enteros.

4) Sea $a \in \mathbb{Z}$, p y q divisores primos de a con $p \neq q$
Entonces $p.q$ es divisor de a

$$\left(p/_{a} \wedge q/_{a}\right) \Longrightarrow p.q/_{a}$$

Obs:

Esta propiedad permitirá asegurar que los divisores de un número entero se pueden obtener como producto de divisores primos

Ej $30 \longrightarrow$ divisores primos: 2,5,3

Particularidad
$60 \longrightarrow$ divisores primos: 2,2,3,5
Otros divisores: 2.3, 2.5, 2.3.5, 2.2, 2.2.3, 2.2.5

Nota:

Euclides demostró que existen infinitos números primos. Este resultado es importante para probar que todo número entero se puede descomponer como producto de divisores primos.

Descomposición o Factorización de un número entero como producto de números primos

Proposición:

Todo número entero $a > 1$ tiene algún divisor primo $p > 1$

Demost.

Consideramos el conjunto de los divisores de número $\boldsymbol{a}$ que son mayores que $\mathbf{1}$

$$D = \left\{ d > 1 \ \ tal\ que \ \ {}^{d}/_{a} \right\}$$

Caso particular:

Si a es un número primo, su único divisor > 1 es $d = a$

Si a no es primo, el conjunto D tiene varios elementos. D es un conjunto de números naturales y tiene mínimo.

Mínimo $D = \boldsymbol{d}^*$; $1 \leq \boldsymbol{d}^* \leq a \quad \wedge \quad {}^{\boldsymbol{d}^*}/_{a}$

Probaremos que $\boldsymbol{d}^*$ es número primo

Suponemos que $\boldsymbol{d}^*$ no es número primo. Entonces existe un entero $\tilde{\boldsymbol{d}}$ que es divisor de d^* :

$$\left(1 < \tilde{\boldsymbol{d}} < d^* \ \wedge \ {}^{\tilde{\boldsymbol{d}}}/_{d^*}\right)$$

Si $\left({}^{\tilde{\boldsymbol{d}}}/_{d^*} \ \wedge \ {}^{d^*}/_{a}\right)$ entonces ${}^{\tilde{\boldsymbol{d}}}/_{a}$. Por lo tanto $\tilde{\boldsymbol{d}} \in D$

$\tilde{\boldsymbol{d}}$ es menor que el mínimo d^*
ABSURDO!!

Este absurdo provino de suponer que d^* no es número primo. Luego d^* es primo.
Ahora probaremos la descomposición de un entero como producto de primos.

Teorema:

Todo número entero $a > 1$ se descompone de manera única como producto de factores primos.

$$\boldsymbol{a} = p_1 \cdot p_2 \cdot \ldots \cdot p_n \qquad \text{con } p_1, p_2, \ldots, p_n \text{ divisores de } \boldsymbol{a}$$

Demost.

- Si $\boldsymbol{a}$ es número primo, la demostración es trivial: $a = a$
- Si $\boldsymbol{a}$ no es número primo, por proposición anterior tiene algún divisor primo p_1, entonces:

$$\boldsymbol{a} = p_1 \cdot a_1 \qquad ; \qquad 1 \leq a_1 < a$$

- Si a_1 es primo, la descomposición termina.
- Si a_1 no es primo, entonces por proposición tiene algún divisor primo p_2 y además $a_1 = p_2 \cdot a_2$, luego $\boldsymbol{a} = p_1 \cdot p_2 \cdot a_2 \quad ; \quad 1 \leq a_1 < a_1 < a$

- Si a_2 es primo, la descomposición termina.
- Si a_2 es no es primo , se reitera el razonamiento.

Como el número a es finito, el procedimiento termina luego de un número finito de pasos y se obtiene la descomposición buscada.

$$\boldsymbol{a} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$$

Ej. $a = 60$

60	3
20	2
10	2
5	5
1	

Como 5 es primo, la descomposición termina.

Probaremos que la descomposición de $\boldsymbol{a} = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ ① es única (salvo el orden de los factores)

Suponemos que $\boldsymbol{a}$ tiene otras descomposiciones como producto de primos.

$\boldsymbol{a} = q_1 \cdot q_2 \cdot \ldots \cdot q_n$ ② con $q_1, q_2, \ldots, q_n$ números primos

Veremos que las descomposiciones son iguales. Veremos que todo primo de la descomposición ① está en la descomposición ② y recíprocamente todo primo de la descomposición ② está en la descomposición ①

Sabemos que p_1 / a entonces $p_1 / q_1 \cdot q_2 \cdot \ldots \cdot q_n$. Por regla de Oro de los números primos p_1 / q_j para algún $j = 1 \ldots n$; pero q_j es primo, entonces $p_1 = q_j$.

Luego, reiterando el razonamiento, se prueba que las descomposiciones coinciden.

- **Congruencia Modular**

Estudiaremos una familia infinita de relaciones de equivalencia definidas e los enteros.

Definición

Sean $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$; diremos que $\boldsymbol{a}$ es congruente con $\boldsymbol{b}$ en módulo n si la diferencia $\boldsymbol{b} - \boldsymbol{a}$ es múltiplo de $\boldsymbol{n}$ ($\boldsymbol{n}$ es divisor de $\boldsymbol{b} - \boldsymbol{a}$).

$$\boldsymbol{a} \equiv \boldsymbol{b}\ m\acute{o}dulo\ \boldsymbol{n}\ \ si\ y\ s\acute{o}lo\ si\ \ \boldsymbol{n} / \boldsymbol{b - a}$$

Ej. $n = 5$

$8 \equiv 23 \ mod\ (5) \quad ya\ que\ 23 - 8 \equiv 15 \quad \wedge \quad 5 / 15$

$8 \not\equiv 21 \ mod\ (5) \quad ya\ que\ 21 - 8 \equiv 15 \quad \wedge \quad 5 \not| 13$

Propiedad: La congruencia módulo n es relación de equivalencia en $\mathbb{Z}$

Demost.

Para $n \in \mathbb{N}$

- Reflexiva: $\forall\, a \in \mathbb{Z} : a \equiv a \; mod\,(n)$

  ${}^{n}/_{a-a}$ (Todo entero no nulo es divisor de 0)

- Simétrica: $\forall\, a, b \in \mathbb{Z} : a \equiv b \;\; mod\,(n) \Longrightarrow \; b \equiv a \;\; mod(n)$

$$a \equiv b \;\; mod\,(n) \Longrightarrow {}^{n}/_{b-a} \Longrightarrow {}^{n}/_{(-1).(b-a)} \Longrightarrow {}^{n}/_{a-b}$$

- Transitiva: $\forall\, a, b, c \in \mathbb{Z} : \left(a \equiv b \;\; mod\,(n) \;\wedge\; b \equiv c \; mod\,(n)\right) \Longrightarrow \; a \equiv c \;\; mod(n)$

$$\left(a \equiv b \;\; mod\,(n) \;\wedge\; b \equiv c \; mod\,(n)\right) \Longrightarrow \left({}^{n}/_{b-a} \;\wedge\; {}^{n}/_{c-b}\right) \Longrightarrow {}^{n}/_{(b-a)+(c-b)} \Longrightarrow$$
$${}^{n}/_{\cancel{b}-a+c-\cancel{b}} \Longrightarrow {}^{n}/_{-a+c} \Longrightarrow {}^{n}/_{c-a} \Longrightarrow a \equiv c \;\; mod(n)$$

Nota:

Sabemos que toda relación de equivalencia particiona al conjunto en clase de equivalencia. Al conjunto de clases de congruencia modulo n lo llamaremos $\mathbb{Z}_n$.
Ahora bien. ¿Cómo podemos identificar las clases?

Teorema:

Sea $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$; $\;a \equiv b \;\; módulo \;\; n\;$ si y solo si $\;a \div n\;$ y $\;b \div n\;$ tienen el mismo RESTO.

Demost.

$$a \equiv b \;\; mod\,(n) \Leftrightarrow {}^{n}/_{b-a} \Leftrightarrow \begin{array}{l} b-a \;\big\lfloor\; n \\ r=0 \;\; = c \end{array} \Leftrightarrow b-a = c.n+0$$

$$\begin{array}{l} a \;\big\lfloor\; n \\ r_1 \;\; = c_1 \end{array} \quad ; \; a = c_1.n + r_1 \;\; \wedge \;\; 0 \le r_1 < n$$

$$\begin{array}{l} b \;\big\lfloor\; n \\ r_2 \;\; = c_2 \end{array} \quad ; \; b = c_2.n + r_2 \;\; \wedge \;\; 0 \le r_2 < n$$

$$b - a = (c_2.n + r_2) - (c_1.n + r_1) =$$
$$= \underbrace{(c_2 - c_1)}_{c}.n + \underbrace{(r_2 - r_1)}_{r} = c.n + r \Leftrightarrow$$
$$\Leftrightarrow r = r_2 - r_1 = 0 \Leftrightarrow r_2 = r_1$$

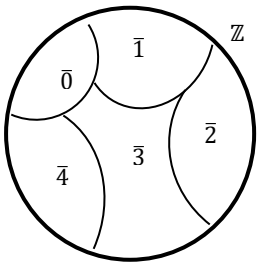
Consecuencia

Dos enteros están en la misma clase de congruencia si tienen el mismo resto en la división entre n. Por lo tanto las clases se identifican con los restos posibles $n \in \mathbb{N}$.

Restos posibles: $0, 1, 2, \dots, n-1$; $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

Ejemplo: $n = 5$

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$



$\bar{0} = \{5.k \ con \ k \in \mathbb{Z}\} = \{\dots, -15, -10, -5, 0, 5, 10, 15 \dots\}$
$\bar{1} = \{5.k + 1 \ con \ k \in \mathbb{Z}\} = \{\dots, -14, -9, -4, 1, 6, 11, 16 \dots\}$
$\bar{2} = \{5.k + 2 \ con \ k \in \mathbb{Z}\} = \{\dots, -13, -8, -3, 2, 7, 12, 17 \dots\}$
$\bar{3} = \{5.k + 3 \ con \ k \in \mathbb{Z}\} = \{\dots, -12, -7, -2, 3, 8, 13, 18 \dots\}$
$\bar{4} = \{5.k + 4 \ con \ k \in \mathbb{Z}\} = \{\dots, -11, -6, -1, 4, 9, 14, 19 \dots\}$

Observación: Todas las clases tienen infinitos número enteros

Propiedades

❖ **Teorema 1:** sea $n \in \mathbb{N}$ y $a, b, c \in \mathbb{Z}$

i) $a \equiv b \ mod \ (n) \implies a + c \equiv b + c \ mod \ (n)$
ii) $a \equiv b \ mod \ (n) \implies a \,.\, c \equiv b.c \ mod \ (n)$

Observación: si $a.c \equiv b.c \ mod\,(n) \ \wedge \ c$ es coprimo con n, entonces $a \equiv b \ mod\,(n)$

❖ **Teorema 2:** sea $n \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$

i) $\big(a \equiv b \ mod \ (n) \wedge \ c \equiv d \ mod\,(n)\big) \implies a + c \equiv b + d \ mod \ (n)$
ii) $\big(a \equiv b \ mod \ (n) \wedge \ c \equiv d \ mod\,(n)\big) \implies a \,.\, c \equiv b \,.\, d \ mod \ (n)$

➢ **Aritmética Modular**

Sean $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y $a \equiv b \ mod\,(n)$

Las propiedades anteriores vinculadas a la suma y la multiplicación de los enteros permiten definir la suma y la multiplicación entre las clases de la Congruencia Modular.

$\mathbb{Z}_n \longrightarrow$ Clases de Congruencia Módulo n

Sean $\bar{a}, \bar{b} \in \mathbb{Z}_n$; definimos :

i) $\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a + b}$
ii) $\bar{a} \,.\, \bar{b} \stackrel{\text{def}}{=} \overline{a \,.\, b}$

Ejemplo: $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Suma: Sea $n \in \mathbb{N}$ y $\mathbb{Z}_n$

- **Asociativa** $\forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$: $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$
  Demost.
  $$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{b+c} = \bar{a} + (\bar{b} + \bar{c})$$

- **Conmutativa** $\forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$
  Demost.
  $$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

- **Neutro** $\boldsymbol{e} = \bar{0}$

- **Opuestos** en $\mathbb{Z}_n$ Opuesto de $\bar{0}$ es $\bar{0}$
  Opuesto de $\bar{1}$ es $\bar{4}$ y viceversa
  Opuesto de $\bar{2}$ es 3 y viceversa
  En general, si $\bar{k} \in \mathbb{Z}_n$ su opuesta es $\overline{n-k} \in \mathbb{Z}_n$

$(\mathbb{Z}_5, +)$ es Grupo Conmutativo y en general $(\mathbb{Z}_n, +)$ es **Grupo Conmutativo**

Multiplicación Sea $n \in \mathbb{N}$ y $\mathbb{Z}_n$

- **Asociativa** $\forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$: $(\bar{a}.\bar{b}).\bar{c} = \bar{a}.(\bar{b}.\bar{c})$
  Demost.
  $$(\bar{a}.\bar{b}).\bar{c} = \overline{a.b}.\bar{c} = \overline{(a.b).c} = \overline{a.(b.c)} = \bar{a}.\overline{b.c} = \bar{a}.(\bar{b}.\bar{c})$$

- **Conmutativa** $\forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$: $\bar{a}.\bar{b} = \bar{b}.\bar{a}$
  Demost.
  $$\bar{a}.\bar{b} = \overline{a.b} = \overline{b.a} = \bar{b}.\bar{a}$$

- **Neutro** $\boldsymbol{e} = \bar{1}$

$(\mathbb{Z}_5, +)$ es Semigrupo conmutativo con unidad (neutro)

Propiedad Distributiva del producto respecto de la suma. $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$

Luego, $(\mathbb{Z}_5, +, .)$ es un **Anillo Conmutativo con Unidad**

Situaciones particulares que dependen del módulo

Siendo $n = 6$; $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$
Ocurre, por ejemplo que $\bar{2}.\bar{3} = \bar{6} = \bar{0} \;\wedge\; \bar{3}.\bar{4} = \overline{12} = \bar{0}$

Tenemos entonces que el producto de clases no nulas da como resultado la clase nula o clase del 0

Obs.

Si el módulo n es un número primo, estas situaciones particulares no se dan. Pero si el módulo es primo y se saca el 0 , el producto de clases tiene estructura de **Grupo Conmutativo**, por lo tanto $(\mathbb{Z}_n, +), (\mathbb{Z}_n - \{0\}, .)$ tiene estructura de **Cuerpo**.

- **Ecuación Lineal de Congruencia**

La forma general, con $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ es:

$$a \,.\, x \equiv b \mod (n)$$

Resolverla es hallar todas las clases de congruencia que al reemplazarlos en la incógnita $\boldsymbol{x}$, verifican la congruencia.

Nota: Una ecuación de congruencia no siempre tiene solución.

Ej

$4x \equiv 7 \, mod(2)$; $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$.

No hay que olvidar que tenemos que aplicar aritmética de clases, entonces en la presente ecuación debemos encontrar un valor para $\boldsymbol{x}$ **(una de las clases de** $\mathbb{Z}_2$**)** que haga que el producto $4.x$ dé como resultado un elemento de la misma clase de **7** ($7 \in \bar{1}$).

Ahora bien, como $4.x$ siempre es par $\forall\, x \in \mathbb{Z}$ nunca pertenecerá a la clase de **7**

Luego, $\boldsymbol{4x \not\equiv 7 \; mod\,(2)}$**, es decir** $\nexists$ **solución.**

- **Teorema 1**

Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

Si en la ecuación $ax \equiv b \, mod\,(n)$ se verifica que $\boldsymbol{a}$ y $\boldsymbol{n}$ son coprimos, entonces la ecuación tiene una **única** solución (una sola clase).

Ejemplo

$4x \equiv 7 \, mod(5)$; $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$4 \perp 5 = 1$ entonces son coprimos.

La solución se obtiene reemplazando las clases en el lugar de $\boldsymbol{x}$

Luego, $\boldsymbol{x = \bar{3}}$ **puesto que** $\boldsymbol{4.3 = 12 \;\wedge\; 12 \in \bar{2}}$

- **Teorema 2**

Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

La ecuación $ax \equiv b \, mod\,(n)$ tiene solución si y solo sí, el máximo común divisor entre $\boldsymbol{a}$ y $\boldsymbol{n}$ es divisor de $\boldsymbol{b}$.

En símbolos $a \perp n / b$

Ejemplo

$6x \equiv 14\ mod(10)$; $\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$

$6 \perp 10 = 2$ $\wedge$ ${}^{2}/_{14}$ $\Longrightarrow$ la ecuación tiene más de una solución.

Las soluciones se pueden obtener de dos maneras:

1. Probando todas las clases
2. Método más rápido :
   a) Se dividen todos los datos entre $a \perp n$
   b) Se resuelve la nueva ecuación.

$3x \equiv 7\ mod\ (5) \Longrightarrow x = \overline{4}$ puesto que $3.4 = 12 \wedge 12 \in \overline{2}$

   c) Las otras soluciones se obtienen sumando la primera solución al nuevo módulo tantas veces como entre en el módulo original.
   $x_1 = \overline{4}$, $x_2 = \overline{4} + \overline{5} = \overline{9}$

Luego, las soluciones de $6x \equiv 14\ mod(10)$ son $x_1 = \overline{4} \wedge x_2 = \overline{9}$

Teorema de Fermat

Sean $a \in \mathbb{Z}$ y p un número primo perteneciente a $\mathbb{N}$, se verifica que

$$a^p \equiv a\ mod(p)$$

Consecuencia

Si a es coprimo con p se tiene que

$$a^{p-1} \equiv 1\ mod(p)$$

Ej . $8^{11} \equiv 8\ mod\ (11) \wedge 8 \perp 11 = 1 \Longrightarrow 8^{10} \equiv 1\ mod\ (11)$