***Módulo 3:***

## 3.1.- GRUPOS DE CLASES RESIDUALES MODULO N

Este capítulo es conveniente analizarlo con detención, porque se estudiara que bajo la relación de congruencia módulo n, el conjunto de números enteros queda particionado en n conjuntos distintos llamados clases de equivalencia; a las que llamaremos clases residuales modulo n. que servirán de ejemplos para el resto de los capítulos.

### 3.2.- Grupo aditivo de las clases residuales módulo n.

**Definición1:** Dados $a$, $b$ enteros y $n \in \mathbb{Z}^+$, diremos que:

$$a \equiv b \bmod (n) \text{ ssi } n \text{ divide } a\ (a-b)$$

$$\Leftrightarrow \exists\ k \in \mathbb{Z} \text{ tal que } a-b=kn$$

$$\Leftrightarrow \exists\ k \in \mathbb{Z} \text{ tal que } a=b+kn$$

(Notación: $a \equiv b \mod (n)$ "$a$ es congruente con $b$ módulo $n$")

**Ejemplo 1:**

$$6 \equiv 4 \mod (2) \quad \begin{cases} 4 \equiv 0 \mod (2) \\ 6 \equiv 0 \mod (2) \end{cases}$$

$$\left( 2 \mid 6-4 = 2 \mid 2 \Rightarrow \exists\ k \in \mathbb{Z} \text{ talque } 2 = 2+k, \text{donde } k=0 \right)$$



Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

La congruencia modulo $n$ es una relación de equivalencia.

Por ver que cumple ser:

✓**Refleja**

En efecto, $\forall\ a \in \mathbb{Z}, \quad a = a + 0 = a + 0\,n$

Lo que implica $a \equiv a \mod(n)$

✓**Simétrica**

En efecto, $\forall\ a,\ b \in \mathbb{Z}$ se tiene:

$$\text{Si } a \equiv b \mod(n) \Rightarrow \quad a = b + kn$$
$$-a + a = -a + b + kn$$
$$-b = -a + b + kn - b$$
$$-b = -a + b - b + kn$$
$$-b = -a + kn$$
$$b = a + (-k)n \ ; -k \in \mathbb{Z}$$
$$\therefore b \equiv a \mod(n)$$

✓**Transitiva**

En efecto, $\forall\ a,\ b,\ c \in \mathbb{Z}$ se tiene:

Si $a \equiv b \mod(n) \Rightarrow$ existe $k \in \mathbb{Z}$ tal que $a = b + kn$, y (1)

Si $b \equiv c \mod(n) \Rightarrow$ existe $k' \in \mathbb{Z}$ tal que $b = c + k'n$, (2)

Sustituyendo (2) en (1) se tiene:

$$a = c + k'n + kn = c + (k' + k)n \ , \text{con } (k' + k) \in \mathbb{Z}$$

$$\therefore\ a \equiv c \mod(n)$$

Por lo tanto, "La congruencia modulo $n$ es una relación de equivalencia".

**Observación:** Como la congruencia modulo $n$ es una relación de equivalencia, particiona al conjunto $\mathbb{Z}$ en clases de equivalencia, donde cada clase es una **clase residual** modulo $n$; esto es:

$$cl(0), cl(1), \ldots, cl(n-1).$$

**Ejemplo 2:**

$$15 \equiv x \mod (2)$$
$$\Rightarrow 15 \equiv 1 \mod (2)$$

Es decir $15 \in cl(1)$ módulo $2$.

(Notación: clase de $x$: $cl(x)$ o $\bar{x}$)

**Definición 2 :** Conjunto de clases residuales módulo $n$

$$\mathbb{Z}/_{\equiv \bmod(n)} = \{\ \bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\ \}$$

(Anotaremos $\mathbb{Z}/_{\equiv \bmod(n)}$ como $\mathbb{Z}_n$)

**Ejemplo 3:** Describir $\mathbb{Z}_2$

Se tiene $\mathbb{Z}_2 = \{\ \bar{0},\ \bar{1}\ \}$

$$\bar{0} = \{\ x \in \mathbb{Z} : x \equiv 0 \mod (2)\ \}$$
$$= \{\ x \in \mathbb{Z} : x = 0 + 2k,\ k \in \mathbb{Z}\ \}$$
$$= \{\ldots,-4,\ -2,\ 0,\ 2,\ 4,\ 6,\ldots\}$$

$$\bar{1} = \{\ x \in \mathbb{Z} : x \equiv 1 \mod (2)\ \}$$
$$= \{\ x \in \mathbb{Z} : x = 1 + 2k,\ k \in \mathbb{Z}\ \}$$
$$= \{\ldots,-3,\ -1,\ 1,\ 3,\ 5,\ 7,\ldots\}$$

**Fermat (1601-1665)**

Abogado francés, las matemáticas eran para el su hobby. Es recordado entre otras cosas por su trabajo en la Teoría de números, y por decir que había descubierto una "prueba maravillosa" pero que no había en la pagina suficiente margen para darla. Numerosos matemáticos han intentado, sin éxito probar este teorema el cual enuncia que dada la ecuación: $x^n + y^n = z^n$ no es posible satisfacerla para valores enteros de x e y, cuando n > 2.

**3.2.1.- Teorema de Fermat:** Si $a \in \mathbb{Z}$ y $p$ es un numero primo que no divide $a$, entonces $p$ divide $a^{p-1} - 1$, esto es:

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

**Corolario:** Si $a \in \mathbb{Z}$, entonces

$$a^p \equiv a \mod (p) \quad ; \forall\ b \in \mathbb{Z}$$


Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

**Teorema:** $(\mathbb{Z}_n, +)$ es un grupo abeliano.

**Demostración:**

Definamos una l.c.i. "$+$" en $\mathbb{Z}_n$ como:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

tal que

$$\forall\ x, y \in \mathbb{Z}_n \quad , \quad \bar{x} + \bar{y} := \overline{x+y}$$

i) Por ver si la operación "$+$" esta bien definida en $\mathbb{Z}_n$.

$\forall\ \bar{x},\ \bar{y},\ \bar{u},\ \bar{v} \in \mathbb{Z}_n$,

$$\begin{array}{lccc} \text{Si} & (\bar{x},\ \bar{y}) & = & (\bar{u},\ \bar{v}) \\ & \bar{x} = \bar{u} & \wedge & \bar{y} = \bar{v} \\ & \Downarrow & & \Downarrow \\ & x \equiv u \bmod n & \wedge & y \equiv v \bmod n \\ & \Downarrow & & \Downarrow \\ & \exists\ k \in \mathbb{Z} : x = u + kn & \wedge & \exists\ t \in \mathbb{Z} : y = v + tn \end{array}$$

Sumando: $x + y = u + v + n(k+t),\ \ k, t \in \mathbb{Z}$

$$\Rightarrow x + y \equiv (u+v) \bmod n$$
$$\Downarrow$$
$$\overline{x+y} = \overline{u+v}$$

$$\therefore\ (\bar{x},\ \bar{y}) = (\bar{u},\ \bar{v})$$

$\therefore$ La operación "$+$" esta bien definida.

ii) Por ver si la operación "$+$" cumple con asociatividad en $\mathbb{Z}_n$.

$\forall\ \bar{x},\ \bar{y},\ \bar{z} \in \mathbb{Z}_n$

$$\begin{aligned} \text{P.d.} \quad (\bar{x}+\bar{y})+\bar{z} &= \bar{x}+(\bar{y}+\bar{z}) \\ \text{En efecto,} \quad (\bar{x}+\bar{y})+\bar{z} &= \overline{(x+y)}+\bar{z} \\ &= \overline{(x+y)+z} \quad \text{;+ es asociativa en } \mathbb{Z} \\ &= \overline{x+(y+z)} \\ &= \bar{x}+\overline{(y+z)} \\ &= \bar{x}+(\bar{y}+\bar{z}) \end{aligned}$$

$\therefore$ La operación "$+$" cumple con asociatividad en $\mathbb{Z}_n$

iii) Existencia de elemento neutro $\mathbb{Z}_n$.

Debe existir $\bar{w} \in \mathbb{Z}_n$, $\forall\ \bar{x} \in \mathbb{Z}_n$ tal que $\bar{x}+\bar{w}=\bar{w}+\bar{x}=\bar{x}$

$$\begin{aligned} \text{Supongamos} \quad \bar{x}+\bar{w} &= \bar{x} \\ \text{Entonces,} \quad \overline{x+w} &= \bar{x} \\ x+w &\equiv x \mod (n) \\ w &\equiv 0 \mod (n) \\ \bar{w} &= \bar{0} \end{aligned}$$

$\therefore$ El neutro en $\mathbb{Z}_n$ es $\bar{0}$

iv) Elemento opuesto (inverso aditivo) en $\mathbb{Z}_n$

$\forall\ x \in \mathbb{Z}_n$, debe existir $\bar{u} \in \mathbb{Z}_n$ tal que $\bar{x}+\bar{u}=\bar{u}+\bar{x}=\bar{0}$

Supongamos $\quad \bar{x}+\bar{u} = \bar{0}$

Entonces, $\quad \overline{x+u} = \bar{0}$

$$x+u \equiv 0 \mod (n) \quad / \cdot (-x) \text{ izquierda}$$

$$u \equiv -x \mod (n)$$

$$\Downarrow$$

$$u \equiv (n-x) \mod (n)$$

$\therefore$ El inverso aditivo de $\bar{x}$ es $\overline{(n-x)}$ en $\mathbb{Z}_n$

Iv) Por ver si la operación "$+$" es conmutativa en $\mathbb{Z}_n$.

$\forall\ x, y \in \mathbb{Z}_n$,

p.d. $\quad \bar{x}+\bar{y} = \bar{y}+\bar{x}$

En efecto, $\quad \bar{x}+\bar{y} = \overline{x+y}$ / + es conmutativa en $\mathbb{Z}$

$$= \overline{y+x}$$

$$= \bar{y}+\bar{x}$$

$\therefore$ La operación "$+$" es conmutativa en $\mathbb{Z}_n$

$\therefore$ **$(\mathbb{Z}_n, +)$** es un grupo abeliano

**Ejemplo 4:** ¿Es $(\mathbb{Z}_2, +)$ un grupo abeliano cíclico?

Para verificar que $(\mathbb{Z}_2, +)$ es un grupo, elaboraremos la Tabla de Cayley o de doble entrada.

| $+$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

Se observa en la tabla que la operación es cerrada, la asociatividad se hereda de $\mathbb{Z}$, el elemento neutro es $\bar{0}$, y además cada elemento del grupo tiene su inverso, estos son:

- El inverso de $\bar{0}$ es $\bar{0}$.
- El inverso de $\bar{1}$ es $\bar{1}$.

Notemos además que $(\mathbb{Z}_2, +)$ es un grupo abeliano, por la simetría de la tabla

Por ver si es cíclico:

$$\bar{1}^1 = \bar{1}$$
$$\bar{1}^2 = \bar{0}$$

Claramente el grupo $(\mathbb{Z}_2, +)$ es cíclico generado por el $\bar{1}$.

$\therefore (\mathbb{Z}_2, +)$ es un grupo abeliano cíclico

**Ejemplo 5:** Describir $\mathbb{Z}_3$, ¿Es $(\mathbb{Z}_3, +)$ un grupo abeliano cíclico?

Se tiene $\mathbb{Z}_3 = \{ \bar{0}, \bar{1}, \bar{2} \}$

$$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0 \mod(3)\}$$
$$= \{x \in \mathbb{Z} : x = 0 + 3k, \ k \in \mathbb{Z}\}$$
$$= \{..., -6, -3, 0, 3, 6, ...\}$$

$$\bar{1} = \{x \in \mathbb{Z} : x \equiv 1 \mod(3)\}$$
$$= \{x \in \mathbb{Z} : x = 1 + 3k, \ k \in \mathbb{Z}\}$$
$$= \{..., -5, -2, 1, 4, 7, ...\}$$

$$\bar{2} = \{x \in \mathbb{Z} : x \equiv 2 \mod(3)\}$$
$$= \{x \in \mathbb{Z} : x = 2 + 3k, \ k \in \mathbb{Z}\}$$
$$= \{..., -4, -1, 2, 5, 8, ...\}$$

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

Se observa en la tabla que la operación es cerrada, la asociatividad se hereda de $\mathbb{Z}$, el elemento neutro es $\bar{0}$, y además cada elemento del grupo tiene su inverso, estos son:

- El inverso de $\bar{0}$ es $\bar{0}$.
- El inverso de $\bar{1}$ es $\bar{2}$.
- El inverso de $\bar{2}$ es $\bar{1}$.

Notemos además que $(\mathbb{Z}_3, +)$ es un grupo abeliano, por la simetría de la tabla.

Por ver si es cíclico:

$$\bar{1}^1 = \bar{1} \qquad \bar{2}^1 = \bar{2} = (\bar{1}^2)^1$$
$$\bar{1}^2 = \bar{2} \qquad \bar{2}^2 = \bar{1} = (\bar{1}^2)^2$$
$$\bar{1}^3 = \bar{0} \qquad \bar{2}^3 = \bar{0} = (\bar{1}^2)^3$$

Claramente el grupo $(\mathbb{Z}_3, +)$ es cíclico generado por $\bar{1}$ y por $\bar{2}$. Lo anotaremos $\mathbb{Z}_3 = \langle\bar{1}\rangle = \langle\bar{2}\rangle$

$\therefore (\mathbb{Z}_3, +)$ es un grupo abeliano cíclico.

**Notemos que:**

- $\bar{1}^n$ es una notación multiplicativa, pero como la operación es aditiva la entenderemos como en notación aditiva, esto es $n\bar{1}$ (n veces $\bar{1}$).

- El grupo $(\mathbb{Z}_p, +)$ con $p$ primo, posee sólo subgrupos triviales, lo generan todos los elementos, salvo el $\bar{0}$

**Ejemplo 6:** Describir $\mathbb{Z}_6$

$\mathbb{Z}_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |

Notamos que:

$\bar{1}^1 = \bar{1}$ $\quad \bar{2}^1 = \bar{2}$ $\quad \bar{3}^1 = \bar{3}$ $\quad \bar{4}^1 = \bar{4}$ $\quad \bar{5}^1 = \bar{5}$

$\bar{1}^2 = \bar{2}$ $\quad \bar{2}^2 = \bar{4}$ $\quad \bar{3}^2 = \bar{0}$ $\quad \bar{4}^2 = \bar{2}$ $\quad \bar{5}^2 = \bar{4}$

$\bar{1}^3 = \bar{3}$ $\quad \bar{2}^3 = \bar{0}$ $\quad \bar{4}^3 = \bar{0}$ $\quad \bar{5}^3 = \bar{3}$

$\bar{1}^4 = \bar{4}$ $\quad \bar{5}^4 = \bar{2}$

$\bar{1}^5 = \bar{5}$ $\quad \bar{5}^5 = \bar{1}$

$\bar{1}^6 = \bar{0}$ $\quad \bar{5}^6 = \bar{0}$

Podemos decir que $\bar{1}$ y $\bar{5}$ son generadores de $\mathbb{Z}_6$, el orden de cada uno de ellos es el orden del grupo, en este caso $6$.

**3.2.2.-Observaciones:**

**3.2.2.1.-** En general $(\mathbb{Z}_n, +)$ es un grupo abeliano cíclico, generado por $\bar{x}$, donde $(x, n) = 1$.

**3.2.2.2.-** El número de generadores esta dado por $\phi(n)$

Ejemplo: $\mathbb{Z}_{18} \Rightarrow n = 18$

Luego $\phi(18) = \phi\left(2 \cdot 3^2\right) = \left(2 - 2^0\right)\left(3^2 - 3\right) = 6$

$\therefore$ El número de generadores de $\mathbb{Z}_{18}$ es $6$.

**3.2.2.3.-** $H$ es un subgrupo de $\mathbb{Z}_n$ si:

$H = \langle \bar{g} \rangle$, donde $g \mid n$

Ejemplo: Hallar los subgrupos de $\mathbb{Z}_6$

Los $g$ tales que $g \mid 6$ son : $1, 2, 3$ y $6$

Pero $H_1 = \langle \bar{1} \rangle$ y $H_2 = \langle \bar{6} \rangle := \langle \bar{0} \rangle$, estos son los subgrupos

Triviales, luego los subgrupos propios de $\mathbb{Z}_6$ son $\langle \bar{2} \rangle$ y $\langle \bar{3} \rangle$.

### 3.3.- Grupo multiplicativo de las clases residuales módulo n

Se define $(\mathbb{Z}'_n, \cdot)$ un grupo multiplicativo.

Donde $\mathbb{Z}'_n = \{\bar{x} \in \mathbb{Z}_n : (x,n) = 1\}$

**Ejemplo 7:** Describir $(\mathbb{Z}'_4, \cdot)$

$$\mathbb{Z}'_4 = \{\bar{1}, \bar{3}\}$$

| · | $\bar{1}$ | $\bar{3}$ |
|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ |

Se observa en la tabla que la operación es cerrada, la asociatividad se hereda de $\mathbb{Z}$, el elemento neutro es $\bar{1}$, y además cada elemento del grupo tiene su inverso, estos son:

- El inverso de $\bar{1}$ es $\bar{1}$
- El inverso de $\bar{3}$ es $\bar{3}$

Claramente $(\mathbb{Z}'_4, \cdot)$ es un grupo abeliano cíclico generado por $\bar{3}$

$$\Rightarrow \mathbb{Z}'_4 = \langle\bar{3}\rangle$$

**Ejemplo 8:** Describir $(\mathbb{Z}'_7, \cdot)$

$$\mathbb{Z}'_7 = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \} = \mathbb{Z}_7 - \{\bar{0}\}$$

| • | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{6}$ |
|---|---|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{6}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{1}$ | $\bar{3}$ | $\bar{5}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{6}$ | $\bar{2}$ | $\bar{5}$ | $\bar{1}$ | $\bar{4}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{1}$ | $\bar{5}$ | $\bar{2}$ | $\bar{6}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{3}$ | $\bar{1}$ | $\bar{6}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{6}$ | $\bar{6}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Se observa en la tabla que la operación es cerrada, la asociatividad se hereda de $\mathbb{Z}$, el elemento neutro es $\bar{1}$, y además cada elemento del grupo tiene su inverso, estos son:

-El inverso de $\bar{1}$ es $\bar{1}$

-El inverso de $\bar{2}$ es $\bar{4}$

-El inverso de $\bar{3}$ es $\bar{5}$

-El inverso de $\bar{4}$ es $\bar{2}$

-El inverso de $\bar{5}$ es $\bar{3}$

-El inverso de $\bar{6}$ es $\bar{6}$

Claramente $(\mathbb{Z}'_7, \cdot)$ es un grupo abeliano cíclico generado por $\bar{5}$

$$\Rightarrow \mathbb{Z}'_7 = \langle \bar{5} \rangle$$

## 3.4.- Guía nº 3

1.- Escribir todas las clases de equivalencia determinadas por la relación $a \equiv b \mod(6)$ en $\mathbb{Z}_6$.Confeccionar la tabla correspondiente a $(\mathbb{Z}_6, +)$.

$$\mathbb{Z}_6 = \{\ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\ \}$$

$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0 \mod(6)\}$

$= \{x \in \mathbb{Z} : x = 0 + 6k,\ k \in \mathbb{Z}\}$

$= \{\ldots, -6, 0, 6, 12, 18, \ldots\}$

$\bar{1} = \{x \in \mathbb{Z} : x \equiv 1 \mod(6)\}$

$= \{x \in \mathbb{Z} : x = 1 + 6k,\ k \in \mathbb{Z}\}$

$= \{\ldots, -5, 1, 7, 13, 19 \ldots\}$

$\bar{2} = \{x \in \mathbb{Z} : x \equiv 2 \mod(6)\}$

$= \{\ldots, -4, , 2, 8, 14, 20, \ldots\}$

$\bar{3} = \{x \in \mathbb{Z} : x \equiv 3 \mod(6)\}$

$= \{\ldots, -3, , 3, 9, 15, 21, \ldots\}$

$\bar{4} = \{x \in \mathbb{Z} : x \equiv 4 \mod(6)\}$

$= \{\ldots, -2, , 4, 10, 16, 22, \ldots\}$

$\bar{5} = \{x \in \mathbb{Z} : x \equiv 5 \mod(6)\}$

$= \{\ldots, -1, , 5, 11, 17, 23, \ldots\}$

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |


Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

2.- Investigar si $\mathbb{Z}_3$ forma un grupo con la multiplicación modulo 3, ídem para $\mathbb{Z}_3 - \{\bar{0}\}$.

Se tiene $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

| $\bullet$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

$\therefore$ Evidentemente $(\mathbb{Z}_3, \cdot)$ no forma un grupo, porque carece de elemento neutro.

Luego $\mathbb{Z}_3 - \{\bar{0}\} = \{\bar{1}, \bar{2}\}$

| $\cdot$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{1}$ |

$\therefore$ $(\mathbb{Z}_3 - \{\bar{0}\}, \cdot)$ forma un grupo abeliano, es cerrada la operación, el elemento neutro es $\bar{1}$, el inverso de $\bar{1}$ es $\bar{1}$, el inverso de $\bar{2}$ es $\bar{2}$, cumple con asociatividad, y evidentemente por la simetría de la tabla es conmutativo.

3.- Resolver la ecuación $3x \equiv 6 \mod(15)$, cuando $0 < x < 15$.

Se tiene

$$\begin{aligned} 3x &\equiv 6 \mod(15) \\ 3x &= 6 + 15k \ , k \in \mathbb{Z} \\ x &= 2 + 5k \end{aligned}$$

$$\begin{aligned} 0 < \ & 2 + 5k \ < 15 \\ -2 < \ & 5k \ < 13 \\ -2/5 < \ & k \ < 13/5 \\ 0{,}4 < \ & k \ < 2{,}6 \end{aligned}$$

Pero $k \in \mathbb{Z}$

$$\Rightarrow 0 \leq \ k \ \leq 2$$

$\therefore$ SI $k = 0 \Rightarrow x = 2 \Rightarrow 6 \equiv 6 \mod(15)$

$k = 1 \Rightarrow x = 7 \Rightarrow 21 \equiv 6 \mod(15)$

$k = 2 \Rightarrow x = 12 \Rightarrow 36 \equiv 6 \mod(15)$

4.- Si $a \equiv b \bmod(n)$ demostrar que $a+c \equiv b+c \bmod(n)$

Hipótesis: $a \equiv b \bmod(n)$

Tesis : $a+c \equiv b+c \bmod(n)$

Si $a \equiv b \bmod(n)$

$\Rightarrow \quad a = b+kn \;; k \in \mathbb{Z} \quad /+c$

$\Rightarrow \quad a+c = b+kn+c$

$\Rightarrow \quad a+c = b+c+kn$

$\therefore a+c \equiv b+c \bmod(n)$

5.- Demostrar que $\forall n \in \mathbb{Z}: n^2 \equiv 0 \bmod(4)$ o bien $n^2 \equiv 1 \bmod(4)$

Si $n$ es par $\Rightarrow \exists\, p \in \mathbb{Z}$ tal que $n = 2p$

$\Rightarrow \quad n^2 = (2p)^2$

$\Rightarrow \quad n^2 = 4p^2$

$\therefore \; n^2 \equiv 0 \bmod(4)$

Si $n$ es impar $\Rightarrow \exists\, p \in \mathbb{Z}$ tal que $n = 2p+1$

$\Rightarrow n^2 = 4p^2 + 4p + 1$

$\therefore n^2 \equiv 1 \bmod(4)$

6.- Determinar el número de generadores de $\mathbb{Z}_{90}$, hallar sus subgrupos y hacer la red de estos.

El número de generadores esta dado por $\phi(90) = (2 \cdot 3^2 \cdot 5) = (2-2^0)(3^2-3)(5-5^0) = (1)(6)(4) = 24$

$\therefore$ $\mathbb{Z}_{90}$ tiene 24 generadores

$\mathbb{Z}_{90} = \langle \bar{x} \rangle$ tal que $(x, 90) = 1$

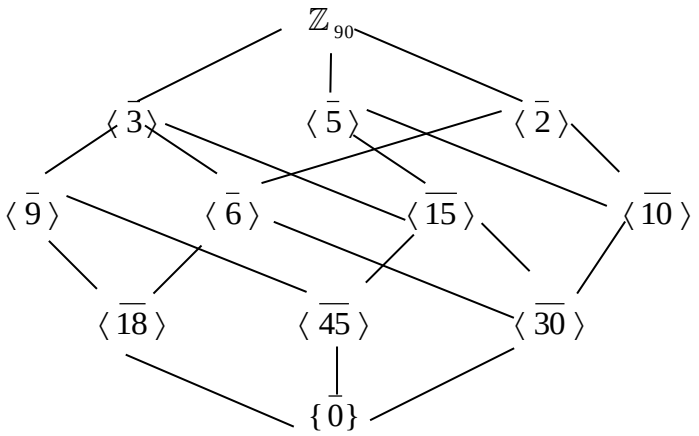
Determinemos los subgrupos de $\mathbb{Z}_{90}$

$H$ es un subgrupo de $\mathbb{Z}_n$, si $H = \langle \bar{g} \rangle$, donde $g \mid n$

Sea $H \leq \mathbb{Z}_{90} \Rightarrow H = \langle \bar{u} \rangle$, donde $u \mid 90$

$\therefore$ $u \in \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$

Red de Subgrupos de $\mathbb{Z}_{90}$:



## 3.5.- Autoevaluación 3

1.- Escribir todas las clases de equivalencia determinadas por la relación $a \equiv b \mod(8)$ definidas en $\mathbb{Z}$. Confeccionar la tabla correspondiente al grupo $\mathbb{Z}_8$.

2.- Resolver las siguientes ecuaciones:

a) $x + 22 \equiv 8 \mod(5)$

b) $5x - 3 \equiv -7 \mod(11)$

c) $-2x + 1 \equiv 4x - 7 \mod(27)$

3.- Si $a \equiv b \mod n$ demostrar que $a\ c \equiv bc \mod(n)$

4.- Determinar el número de generadores de $\mathbb{Z}_{72}$, hallar sus subgrupos, sus órdenes y hacer la red de subgrupos.

5.- Cuales de los siguientes grupos son cíclicos: $(\mathbb{Z}'_5, \cdot)$; $(\mathbb{Z}'_8, \cdot)$; $(\mathbb{Z}'_9, \cdot)$.

6.- Determinar los distintos subgrupos de $\mathbb{Z}'_8$, $\mathbb{Z}_8$, generados por un solo elemento.

7.- Demuestre o refute si $\mathbb{Z}_3 \times \mathbb{Z}_2$ es cíclico.