Capítulo 3

Números Enteros Módulo m

3.1. Congruencias

Definición 22 *Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}, m > 0$.*
Se dice que a es congruente a b módulo m, lo que escribiremos

$$a \equiv b(\texttt{mod}\ m) \text{ si y sólo si } m|(a-b).$$

En caso contrario, se dice incongruentes o no congruentes, lo que anotaremos

$$a \not\equiv b(\texttt{mod}\ m).$$

Ejemplo 44

1. $8 \equiv -5(\texttt{mod}\ 13)$ *ya que* $13|(8-(-5))$
2. $22 \equiv 1(\texttt{mod}\ 7)$ *ya que* $7|(22-1)$
3. $11 \equiv 1(\texttt{mod}\ 2)$ *ya que* $2|(11-1)$

Observación:

$$a \equiv b(\texttt{mod}\ m) \Leftrightarrow (\exists\, t \in \mathbb{Z})(a = b + tm).$$

Teorema 86 *Sea $m \in \mathbb{Z}, m > 0$.*

1. *Para todo $a \in \mathbb{Z}$,*
$$a \equiv a(\texttt{mod}\ m).$$
2. *Para todo $a, b \in \mathbb{Z}$,*
$$a \equiv b(\texttt{mod}\ m) \Leftrightarrow b \equiv a(\texttt{mod}\ m).$$
3. *Sean $a, b, c \in \mathbb{Z}$ cualesquiera, si $a \equiv b(\texttt{mod}\ m)$ y $b \equiv c(\texttt{mod}\ m)$, entonces*
$$a \equiv c(\texttt{mod}\ m).$$

Demostración:

1. Para todo $a \in \mathbb{Z}$, se tiene que $a \equiv a(\texttt{mod}\ m)$, pues $m|(a-a)$.

2. Sean $a, b \in \mathbb{Z}$, tales que

$$\begin{aligned} & a \equiv b(\texttt{mod}\ m) \\ \Leftrightarrow \quad & (\exists\, t \in \mathbb{Z})(a = b + mt) \\ \Leftrightarrow \quad & (\exists k \in \mathbb{Z})(b = a + mk), \quad \text{donde}\, k = -t \\ \Leftrightarrow \quad & b \equiv a(\texttt{mod}\ m). \end{aligned}$$

3. Si $a \equiv b(\texttt{mod}\ m)$ y $b \equiv c(\texttt{mod}\ m)$, entonces existen $t, k \in \mathbb{Z}$, tales que

$$a = b + mt \tag{3.1}$$
$$b = c + mk, \tag{3.2}$$

luego reemplazando (3.1) en (3.2), se tiene que

$$\begin{aligned} & a = c + mt + mk \\ \Leftrightarrow \quad & a = c + m(t+k) \\ \Leftrightarrow \quad & a \equiv c(\texttt{mod}\ m). \end{aligned}$$

□

Corolario 87 *La relación de congruencia módulo m, es una relación de equivalencia en* $\mathbb{Z}$.

Definición 23 *Sean* $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ *entonces se define la clase de equivalencia de a módulo m como el conjunto de todos los números enteros congruente a "a" módulo m, y la denotaremos por* $\overline{a}$. *El número a se llama representante de la clase a.*

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a(\texttt{mod}\ m)\}.$$

Ejemplo 45 *Sea* $m = 13$

$$\begin{aligned} \overline{1} &= \{x \in \mathbb{Z} \mid x \equiv 1(\texttt{mod}\ 13)\} \\ &= \{x \in \mathbb{Z} \mid x = 1 + 13t, \quad t \in \mathbb{Z}\} \\ &= \{\ldots, -25, -12, 1, 14, 27 \ldots\}. \end{aligned}$$

Definición 24 *El conjunto formado por todas las clases módulo m definidas sobre* $\mathbb{Z}$ *es llamado el conjunto de los números enteros módulo m y se anota*

$$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}.$$

Teorema 88 *Sea* $m \in \mathbb{Z}^+$, *la relación de equivalencia módulo m particiona a* $\mathbb{Z}$ *en m clases de equivalencia, en forma más precisa tenemos que*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}.$$

Demostración: Sea $x \in \mathbb{Z}$, luego por el algoritmo de la división tenemos que existen $q, r \in \mathbb{Z}$ tal que $0 \leq r < m$ y $x = qm + r$ que es equivalente a $x \equiv r(\texttt{mod}\ m)$, de este modo x pertenece a una de las clases anteriores.

Sean r, s enteros no negativos menores que m, tales que $r \equiv s(\texttt{mod}\ m)$, por lo tanto $r - s = mt$, de donde se obtiene que

$$0 \leq r = s + mt < m, \quad 0 \leq s < m$$

De esta manera se obtiene que $t = 0$, luego la clase es única. □

3.2. Suma en $\mathbb{Z}_m$

Teorema 89 *Sea $m \in \mathbb{Z}, m > 0$. Si $\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\}$ y $\{k_1, \ldots, k_n\}$ son conjuntos de enteros cualesquiera, tales que $a_i \equiv b_i (\mathtt{mod}\ m), 1 \leq i \leq n$, entonces*

$$\sum_{i=1}^{n} k_i a_i \equiv \sum_{i=1}^{n} k_i b_i (\mathtt{mod}\ m).$$

Demostración: Si $a_i \equiv b_i (\mathtt{mod}\ m)$, para $1 \leq i \leq n$, entonces existen enteros $d_i, 1 \leq i \leq n$, tales que

$$a_i = b_i + d_i m, \quad 1 \leq i \leq n, \tag{3.3}$$

luego multiplicando (3.3) por k_i, para $1 \leq i \leq n$ se tiene que

$$k_i a_i = k_i b_i + (k_i d_i) m, \quad 1 \leq i \leq n,$$

así

$$\begin{aligned} & \sum_{i=1}^{n} k_i a_i = \sum_{i=1}^{n} k_i b_i + m \sum_{i=1}^{n} k_i d_i \\ \Leftrightarrow \quad & \sum_{i=1}^{n} k_i a_i \equiv \sum_{i=1}^{n} k_i b_i (\mathtt{mod}\ m). \end{aligned}$$

Observación: El teorema anterior nos permite definir la suma en $\mathbb{Z}_m$ como sigue:

Definición 25 *Sean $\overline{a}$ y $\overline{b} \in \mathbb{Z}_m$, se definen la suma por:*

$$\overline{a} + \overline{b} := \overline{a + b}.$$

Teorema 90 *$(\mathbb{Z}_m, +)$ es un grupo abeliano.*

Ejemplo 46 *Construir la tabla del grupo $(\mathbb{Z}_2, +)$:*

Solución: La tabla esta dada por

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}+\overline{0}$	$\overline{0}+\overline{1}$
$\overline{1}$	$\overline{1}+\overline{0}$	$\overline{1}+\overline{1}$

al operar obtenemos

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Ejemplo 47 *Construir la tabla del grupo $(\mathbb{Z}_6, +)$:*

Solución: Al simplificar obtenemos

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Definición 26 *Sea $\overline{a} \in \mathbb{Z}_m$, y $n \in \mathbb{N}$, entonces se define por recurrencia la potencia aditiva n -esima de $\overline{a}$*

$$\begin{aligned} 0 \cdot \overline{a} &= \overline{0} \\ (n+1) \cdot \overline{a} &= n \cdot \overline{a} + \overline{a}; \\ \textit{Además} \quad (-n) \cdot \overline{a} &= n \cdot \overline{-a} \end{aligned}$$

Ejemplo 48 *En $\mathbb{Z}_6$, calcular*

1. $3 \cdot \overline{1} = 2 \cdot \overline{1} + \overline{1} = \overline{1} + \overline{1} + \overline{1} = \overline{3}$
2. $3 \cdot \overline{2} = \overline{2} + \overline{2} + \overline{2} = \overline{6} = \overline{0}$
3. $5 \cdot \overline{3} = \overline{15} = \overline{3}$

Propiedad 91 *Sean $\overline{a}, \overline{b} \in \mathbb{Z}_m$, y $r, s \in \mathbb{Z}$, entonces*

1. $(r+s) \cdot \overline{a} = r \cdot \overline{a} + s \cdot \overline{a}$
2. $r \cdot \overline{a+b} = r \cdot \overline{a} + r \cdot \overline{b}$

Definición 27 *Sea $\overline{a} \in \mathbb{Z}_n$, el subgrupo cíclico, generado por $\overline{a}$ es*

$$< \overline{a} >= \{k \cdot \overline{a} \in \mathbb{Z}_m \mid k \in \mathbb{Z}\}$$

Ejemplo 49 *Determinar los subgrupos cíclicos de $(\mathbb{Z}_6, +)$*

Solución: La tabla del grupo $(\mathbb{Z}_6, +)$, esta dada en el ejemplo 47. Luego tenemos que:

$$\begin{array}{ll} < \overline{0} >= \{\overline{0}\} & < \overline{1} >= \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{0}\} \\ < \overline{2} >= \{\overline{2}, \overline{4}, \overline{0}\} & < \overline{3} >= \{\overline{3}, \overline{0}\} \\ < \overline{4} >= \{\overline{4}, \overline{2}, \overline{0}\} & < \overline{5} >= \{\overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}, \overline{0}\} \end{array}$$

De lo anterior tenemos que existen 4 subgrupos cíclicos distintos y son:

$$< \overline{0} >;\ < \overline{2} >=< \overline{4} >;\ < \overline{3} >;< \overline{1} >=< \overline{5} >= \mathbb{Z}_6$$

Teorema 92 *El grupo $\mathbb{Z}_n$ es cíclico.*

Demostración: Existe $\overline{1} \in \mathbb{Z}_n$ y dado $\overline{a} \in \mathbb{Z}_n$, se tiene que

$$\overline{a} = a \cdot \overline{1}$$

□

Definición 28 *Sea $\overline{a} \in \mathbb{Z}_n$, se dice que $k \in \mathbb{N}^*$ es el orden aditivo de $\overline{a}$ si y sólo si k es el menor entero positivo que $k \cdot \overline{a} = \overline{0}$. el número k se denota por $|\overline{a}|$*

En el ejemplo anterior $\mathbb{Z}_6$, tenemos que:

$$|\overline{0}| = 1;\ |\overline{2}| = |\overline{4}| = 3;\ |\overline{3}| = 2;\ |\overline{1}| = |\overline{5}| = 6;$$

Teorema 93 *Sea* $\overline{a} \in \mathbb{Z}_n$,
$\overline{a}$ *genera* $\mathbb{Z}_n$ *si y sólo si* $(a, n) = 1$

Demostración: Supongamos que $\overline{a}$ genera $\mathbb{Z}_n$. Luego

$$(\exists k \in \mathbb{Z})(\ k \cdot \overline{a} = \overline{1}\ )$$

es decir,

$$(\exists k \in \mathbb{Z})(\ ak - nq = 1\ )$$

por lo tanto a, n son primos relativos, $(a, n) = 1$.

En la otra dirección tenemos que $(a, n) = 1$, luego existe $x, y \in \mathbb{Z}$

$$ax + ny = 1$$

Ahora sea $\overline{b} \in \mathbb{Z}_n$, por lo tanto tenemos que

$$axb + nyb = 1b$$

es decir $(xb)a \equiv b(\mathtt{mod}, n)$, con lo cual $\overline{b} \in < \overline{a} >$. □

Teorema 94 *Sea* $\overline{a} \in \mathbb{Z}_n$, *entonces*

$$|\overline{a}| = \frac{n}{(a, n)}$$

Demostración: Sea $\overline{a} \in \mathbb{Z}_n$, luego tenemos que

$$\frac{n}{(a, n)}\overline{a} = \overline{\frac{na}{(a, n)}} = \frac{a}{(a, n)}\overline{n} = \overline{0}$$

Ahora veremos que es el menor.

$$|\overline{a}|\overline{a} = \overline{0} \ \Leftrightarrow\ |\overline{a}|a = nt,\ \exists t \in \mathbb{N}$$

luego tenemos que

$$|\overline{a}|\frac{a}{(a, n)} = \frac{n}{(a, n)}t,$$

de este modo tenemos que

$$\frac{n}{(a, n)} \mid |\overline{a}|\frac{a}{(a, n)}$$

pero $\left(\frac{n}{(a,n)}\ ,\ \frac{a}{(a,n)}\right) = 1$, de lo cual obtenemos que

$$\frac{n}{(a, n)} \mid |\overline{a}|$$

por lo tanto

$$|\overline{a}| = \frac{n}{(a, n)}q,\ \exists q \in \mathbb{Z}$$

ambos son positivos y $|\overline{a}|$ es el más pequeño con la propiedad, luego

$$|\overline{a}| = \frac{n}{(a, n)}$$

□

Ejemplo 50

a) Determinar el orden de $\overline{8} \in \mathbb{Z}_{20}$

$$|\overline{8}| = \frac{20}{(8,20)} = \frac{20}{4} = 5$$

b) Determinar el orden de $\overline{10} \in \mathbb{Z}_{15}$

$$|\overline{10}| = \frac{15}{(15,10)} = \frac{15}{5} = 3$$

Corolario 95 *Sea* $\overline{a} \in \mathbb{Z}_n$*, entonces*

$$|\overline{a}| \mid n$$

Teorema 96 *Todo los subgrupos de* $(\mathbb{Z}_n, +)$*, son cíclicos.*

Demostración: Sea H un subgrupo de $(\mathbb{Z}_n, +)$, no trivial.

Luego existe k el menor entero positivo, tal que $\overline{k} \in H$. Demostraremos que $H =< \overline{k} >$

Sea $\overline{l} \in H$, aplicando algoritmo de la división obtenemos $l = kq + r$ donde $0 \leq r < k$, despejando obtenemos

$$\overline{r} = \overline{l - kq} = \overline{l} - q\overline{k} \in H$$

pero k era el menor entero positivo, luego $r = 0$, con lo cual tenemos

$$\overline{l} = q\overline{k} \in < \overline{k} >$$

La otra contención es inmediata. □

Propiedad 97 *Si* $d|n$ *entonces existe un único subgrupos de* $(\mathbb{Z}_n, +)$*, de orden* d *y todos los elementos de orden* d *pertenece al subgrupo cíclicos.*

Demostración: Sea $d|n$, el orden de $\frac{\overline{n}}{d}$ en $\mathbb{Z}_n$ es d, ya que

$$\left|\frac{\overline{n}}{d}\right| = \frac{n}{(n, \frac{n}{d})} = \frac{n}{(d\frac{n}{d}, \frac{n}{d})} = d.$$

luego el subgrupo

$$\left\langle \frac{\overline{n}}{d} \right\rangle,$$

tiene orden d.

Sea $\overline{y} \in \mathbb{Z}_n$, de orden d, por lo tanto

$$d\overline{y} = \overline{0},$$

de otro modo $dy = nt$, es decir, $y = t\frac{n}{d}$, note que el elemento tiene orden d si $(d, t) = 1$

$$\overline{y} \in \left\langle \frac{\overline{n}}{d} \right\rangle.$$

□

Observación: Construir un reticulado de un grupo, es hacer un diagrama donde los vértices son lo subgrupos y la flecha indica contención, recuerde que la contención es una relación de orden parcial sobre los subconjunto.

Ejemplo 51 *Construir el reticulado de los subgrupos de* $(\mathbb{Z}_{30}, +)$

Solución: Construimos los subgrupos de $\mathbb{Z}_{30}$. Pare ello tenemos los primos relativos con 30, ellos nos entregan los generadores de $\mathbb{Z}_{30}$, el orden de $|\overline{2}| = 15$, luego todos los elementos del generado por $\overline{2}$ de orden 15 generan el mismo grupo. resumiendo tenemos los siguiente

$$\begin{aligned}
\mathbb{Z}_{30} &= <\overline{1}>=<\overline{7}>=<\overline{11}>=<\overline{13}>=<\overline{17}>=<\overline{19}>=<\overline{23}>=<\overline{29}> \\
<\overline{0}> &= \{\overline{0}\} \\
<\overline{2}> &= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}\}
\end{aligned}$$

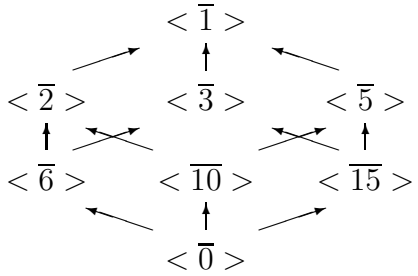
De acuerdo a la propiedad 97, el exponente aditivo t, que ser primo relativo con el orden, luego $(t, 15) = 1$ para obtener otro generador debo amplificar por $1, 2, 4, 7, 8, 11, 13, 14$.

$$\begin{aligned}
<\overline{2}> &= <\overline{4}>=<\overline{8}>=<\overline{14}>=<\overline{16}>=<\overline{22}>=<\overline{26}>=<\overline{28}> \\
<\overline{3}> &= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}
\end{aligned}$$

El elemento tiene orden 10, luego los otros generadores, se obtiene determinando los t tales que $(t, 10) = 1$, es decir, $1, 3, 7, 9$.

$$\begin{aligned}
<\overline{3}> &= <\overline{9}>=<\overline{21}>=<\overline{27}> \\
<\overline{5}> &= \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\} \\
<\overline{5}> &= <\overline{25}> \\
<\overline{6}> &= \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\} \\
<\overline{6}> &= <\overline{12}>=<\overline{18}>=<\overline{24}> \\
<\overline{10}> &= \{\overline{0}, \overline{10}, \overline{20}\} \\
<\overline{10}> &= <\overline{20}> \\
<\overline{15}> &= \{\overline{0}, \overline{15}\}
\end{aligned}$$

Ahora construimos el reticulado:



Definición 29 *Sea* $n \in \mathbb{N}^*$. *Se define la función de Euler, y esta dada por*

$$\phi(n) = \#\{a \in \mathbb{N}^* \mid a \leq n \ \wedge \ (a, n) = 1\}$$

Ejemplo 52

1. $\phi(1) = \#\{a \in \mathbb{N}^* \mid a \leq 1 \ \wedge \ (a, 1) = 1\} = \#\{1\} = 1$

2. $\phi(7) = \#\{a \in \mathbb{N}^* \mid a \leq 7 \ \wedge \ (a,7) = 1\} = \#\{1,2,3,4,5,6\} = 6$

3. $\phi(8) = \#\{a \in \mathbb{N}^* \mid a \leq 8 \ \wedge \ (a,8) = 1\} = \#\{1,3,5,7\} = 4$

4. $\phi(10) = \#\{a \in \mathbb{N}^* \mid a \leq 10 \ \wedge \ (a,10) = 1\} = \#\{1,3,7,9\} = 4$

Propiedad 98 *Sea G un grupo cíclico con n elemento entonces el número de generadores de G es $\phi(n)$.*

Propiedad 99 *Sea $p \in \mathbb{N}$ un número primo entonces $\phi(p) = p - 1$*

Demostración: Sea $a \in \mathbb{N}^*$, tal que $a < p$ y $(a,p) = d$, pero $d \neq p$, luego $d = 1$. □

Propiedad 100 *Sean $p, n \in \mathbb{N}$, tal que p un número primo entonces $\phi(p^n) = p^{n-1}(p-1)$*

Demostración: Sea $a \in \mathbb{N}$, tal que $(a, p^n) = 1$, luego a no es múltiplo de p, es decir la cantidad de primos relativos a p^n es igual a la cantidad de números menores p^n, que no son múltiplo de p, por lo tanto

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

□

Ejemplo 53
$\phi(8) = \phi^(2^3) = 2^2(2-1) = 4$
$\phi(16) = \phi^(2^4) = 2^3(2-1) = 8$

Propiedad 101 *Sean $a, b \in \mathbb{N}$, tales que $(a,b) = 1$ entonces $\phi(ab) = \phi(a)\phi(b)$*

Demostración: Consideremos

$$\begin{array}{rccc} f: & \mathbb{Z}_{ab} & \to & \mathbb{Z}_a \times \mathbb{Z}_b \\ & \overline{x} & \to & (\overline{x}, \overline{x}) \end{array}$$

Es una función ya que, dado $\overline{x} = \overline{y} \in \mathbb{Z}_{ab}$, luego $ab|(x-y)$, es decir $a|(x-y) \wedge b|(x-y)$, por lo tanto

$$(\overline{x}, \overline{x}) = (\overline{y}, \overline{y}) \in \mathbb{Z}_a \times \mathbb{Z}_b$$

Además es biyectiva, ya que, si $f(\overline{x}) = f(\overline{y})$ entonces $x \equiv y(\texttt{mod}\ a), x \equiv y(\texttt{mod}\ b)$, de lo cual

$$at = x - y = bl$$

De lo cual, $l = at'$. es decir $x - y = abt'$. Por lo tanto $x \equiv y(\texttt{mod}\ ab)$.

La epiyectiva, sean $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0 + by_0 = 1$. Sea $(\overline{u}, \overline{v}) \in \mathbb{Z}_a \times \mathbb{Z}_b$, luego definimos $x = u - ax_0(u-v) = v + by_0(u-v)$, de lo cual se obtiene que

$$x \equiv u(\texttt{mod}\ a) \wedge x \equiv v(\texttt{mod}\ b)$$

De este modo la función es biyectiva.

Además $f(\overline{x} + \overline{y}) = f(\overline{x}) + f(\overline{y})$, con lo cual envía generador en generador.

Al considerar un generador de $\mathbb{Z}_a \times \mathbb{Z}_b$, sus coordenadas deben generar a cada componente. Por otro lado, dado generadores $\overline{x}, \overline{y}$ de $\mathbb{Z}_a, \mathbb{Z}_b$, se tiene,

$$k(\overline{x}, \overline{y}) = (\overline{0}, \overline{0}) \in \mathbb{Z}_a \times \mathbb{Z}_b$$

De lo cual se tiene que, $kx \equiv 0(\texttt{mod}\ a)$ y $ky \equiv 0(\texttt{mod}\ b)$ como $(x, a) = 1 = (y, b)$, luego $k = at = bl$, es decir, $ab|k$, luego $(\overline{x}, \overline{y})$ generan.

De este modo, todo generador de $\mathbb{Z}_a \times \mathbb{Z}_b$, le corresponde un generador de $\mathbb{Z}_{ab}$, y se construye con generadores de $\mathbb{Z}_a, \mathbb{Z}_b$ respectivamente. □

Ejemplo 54 *Calcular* $\phi(100)$

$$\phi(100) = \phi(2^2 5^2) = \phi(2^2)\phi(5^2) = 2 \cdot 5(5-1) = 10$$

Teorema 102 *Sea* $n \in \mathbb{N}$*, entonces*

$$\sum_{d|n \ \ d>0} \phi(d) = n$$

Demostración: En $\mathbb{Z}_n$ se define la siguiente relación

$$\overline{a} \sim \overline{b} \ \Leftrightarrow \ |\overline{a}| = |\overline{b}|$$

Es Refleja: $|\overline{a}| = |\overline{a}| \ \Leftrightarrow \ \overline{a} \sim \overline{a}$
Es Simétrica: $\overline{a} \sim \overline{b} \ \Leftrightarrow \ |\overline{a}| = |\overline{b}| \ \Leftrightarrow \ |\overline{b}| = |\overline{a}| \ \Leftrightarrow \overline{b} \sim \overline{a}$
Es Transitiva: $\overline{a} \sim \overline{b} \ \wedge \ \overline{b} \sim \overline{c}$, luego $|\overline{a}| = |\overline{b}| \ \wedge \ |\overline{b}| = |\overline{c}|$, de lo cual $|\overline{a}| = |\overline{c}|$.
Por lo tanto

$$\overline{a} \sim \overline{c}$$

De este modo $\sim$ es una relación de equivalencia, denotemos la clase de equivalencia para $d|n$

$$C_d = \{\overline{a} \in \mathbb{Z}_n \mid |\overline{a}| = d\}$$

De este modo se obtiene $\mathbb{Z}_n = \overset{\circ}{\cup}_{d|n \ \ d>0} C_d$, es decir $n = \sum_{d|n \ \ d>0} |C_d|$. Por la propiedad 97 tenemos que existe un único subgrupo de orden un divisor y todos los elementos de ese orden están en el subgrupo. Luego, debemos tener presente que el grupo cíclico $< \frac{\overline{n}}{d} >$ de orden d, tiene $\phi(d)$ generadores, luego en $\mathbb{Z}_n$ existe $\phi(d)$ elementos de orden d, así tenemos $\phi(d) = |C_d|$, reemplazando obtenemos

$$n = \sum_{d|n \ \ d>0} |C_d| = \sum_{d|n \ \ d>0} \phi(d)$$

□

3.3. Producto en $\mathbb{Z}_m$

Teorema 103 *Sean $a, b, c, d \in \mathbb{Z}, m > 0$. cualesquiera, si $a \equiv b(\mathtt{mod}\ m)$ y $c \equiv d(\mathtt{mod}\ m)$, entonces*

$$ac \equiv bd(\mathtt{mod}\ m).$$

Demostración: Si $a \equiv b(\mathtt{mod}\ m)$ y $c \equiv d(\mathtt{mod}\ m)$, entonces existen enteros r, k tales que

$$a = b + km \quad y \quad c = d + rm,$$

luego

$$ac \;=\; (b + km)(d + rm) = bd + (br + kd + kr)m.$$

Ahora bien, definiendo $t = br + kd + kr \in \mathbb{Z}$, tenemos que

$$ac = bd + tm \;\Leftrightarrow\; ac \equiv bd(\mathtt{mod}\ m).$$

□

Observación: El teorema anterior nos permite definir el producto en $\mathbb{Z}_m$ como sigue:

Definición 30 *Sean $\overline{a}$ y $\overline{b} \in \mathbb{Z}_m$, se definen producto por*

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Teorema 104 *$(\mathbb{Z}_m, +, \cdot)$ es un anillo conmutativo*

Ejemplo 55 *Construir la tabla de $(\mathbb{Z}_6, \cdot)$.*

Solución: Con las misma notación empleada en la suma, construimos la siguiente tabla:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Definición 31 *Sea $\overline{a} \in \mathbb{Z}_n$, se dice que $\overline{a}$ es invertible si y sólo si existe $\overline{b} \in \mathbb{Z}_n$, tal que $\overline{a} \cdot \overline{b} = \overline{1}$*

En el ejemplo anterior tenemos que los elemento invertible son $\overline{1}, \overline{5}$

Teorema 105 *Sea $\overline{a} \in \mathbb{Z}_n$,*

$$\overline{a} \text{ es invertible si y sólo si } (a, n) = 1$$

Corolario 106 *Si $p \in \mathbb{Z}$ es un número primo entonces todo elemento no nulo de $\mathbb{Z}_p$ es invertible. De otro modo $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.*

Corolario 107 *Si p número primo, entonces el anillo $(\mathbb{Z}_p, +, \cdot)$ no tiene divisores de cero, es decir,*

$$\overline{a}\overline{b} = \overline{0} \Rightarrow (\overline{a} = \overline{0} \vee \overline{b} = \overline{0}), \quad \textit{para todo } \overline{a}, \overline{b} \in \mathbb{Z}$$

Propiedad 108 *Si n no primo entonces $(\mathbb{Z}_n, +, \cdot)$ tiene divisores de cero*

Demostración: Si n es un número compuesto, entonces $n = ab$, con $0 < a < n,\ 0 < b < n$, luego $\overline{a} \neq 0, \overline{b} \neq 0$ en $\mathbb{Z}_n$. Y se cumple que

$$\overline{a}\overline{b} = \overline{n} = \overline{0}$$

□

Notación: El conjunto de elementos invertibles en $\mathbb{Z}_n$ se denota por

$$\mathcal{U}(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \mid \overline{a} \text{ es invertible } \}$$

El inverso multiplicativo de $\overline{a}$ se denota por $\overline{a}^{-1}$
Observación: La cantidad de elementos invertible en $\mathbb{Z}_n$ es $\phi(n) = |\mathcal{U}(\mathbb{Z}_n)|$

Teorema 109 *$(\mathcal{U}(\mathbb{Z}_n), \cdot)$ es un grupo abeliano, y es llamado el grupo de las unidades de $\mathbb{Z}_n$*

Ejemplo 56 *Construir la tabla de $(\mathcal{U}(\mathbb{Z}_7), \cdot)$ y $(\mathcal{U}(\mathbb{Z}_8), \cdot)$*

Solución:

$\mathcal{U}(\mathbb{Z}_7)$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathcal{U}(\mathbb{Z}_8)$

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

El grupo $(\mathcal{U}(\mathbb{Z}_7), \cdot)$ es cíclico
El grupo $(\mathcal{U}(\mathbb{Z}_8), \cdot)$ no es cíclico

Definición 32 *Sea $\overline{a} \in \mathbb{Z}_n - \{\overline{0}\}$, y $m \in \mathbb{N}$, entonces se define por recurrencia la potencia multiplicativa m -esima de $\overline{a}$*

$$\begin{aligned} \overline{a}^0 &= \overline{1} \\ \overline{a}^{m+1} &= \overline{a}^m \cdot \overline{a} \end{aligned}$$

Además $\overline{a} \in \mathcal{U}(\mathbb{Z}_n)$, entonces

$$\begin{aligned} \overline{0}^m &= \overline{0}, \quad m \neq 0 \\ (\overline{a})^{-m} &= (\overline{a}^{-1})^m \end{aligned}$$

Definición 33 *Sea $\overline{a} \in \mathcal{U}(\mathbb{Z}_n)$, se dice que $k \in \mathbb{N}^*$ es el orden multiplicativo de $\overline{a}$ si y sólo si k es el menor entero positivo que $\overline{a}^k = \overline{1}$.*

Notación: $k = |\overline{a}|$, cuidado con la notación, ya que es la misma, lo que varia es el grupo, es decir, el conjunto con la operación binaria.
Observación: En el ejemplo 56, tenemos la tabla del grupo $\mathcal{U}(\mathbb{Z}_7)$ y podemos obtener los ordenes multiplicativos de cada elemento

$$|\overline{1}| = 1, \quad |\overline{2}| = 3, \quad |\overline{3}| = 6, \quad |\overline{4}| = 3, \quad |\overline{5}| = 2.$$

Teorema 110 *El grupo $\mathcal{U}(\mathbb{Z}_n)$ es cíclico si y sólo si existe p número primo impar y $m \in \mathbb{N}^*$ tal que*

$$n = p^m, \ \vee \ n = 2p^m, \ \vee \ n = 2, \ \vee \ n = 4$$

Ejemplo 57

1. *$\mathcal{U}(\mathbb{Z}_{18})$ es cíclico, ya que $18 = 2 \cdot 3^2$*
2. *$\mathcal{U}(\mathbb{Z}_{20})$ no es cíclico, ya que $20 = 2^2 \cdot 5$*
3. *$\mathcal{U}(\mathbb{Z}_{30})$ no es cíclico, ya que $30 = 2 \cdot 3 \cdot 5$*
4. *$\mathcal{U}(\mathbb{Z}_{50})$ es cíclico, ya que $50 = 2 \cdot 5^2$*

Definición 34 *Sean $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Una ecuación con congruencia de grado 1 es de la forma*

$$ax \equiv b(\texttt{mod } n)$$

donde a, b son los coeficiente y x la incognita

Ejemplo 58 *Resolver en $\mathbb{Z}$, la ecuación*

$$2x \equiv 3(\texttt{mod } 13)$$

Solución: Resolver la ecuación es equivalente a resolver

$$2x = 3 + 13t \quad \text{o bien} \quad 2x - 13t = 3$$

Como sabemos que

$$2(7) - 13(1) = 1$$

luego son primos relativos, y una solución particular es

$$x_0 = 21 \ \wedge \ t_0 = 3$$

Por lo tanto, la solución general es

$$x = 21 + 13s \ \wedge \ t = 3 + 2s, \quad s \in \mathbb{Z}$$

Con lo cual, la solución de la ecuación $2x \equiv 3(\texttt{mod } 13)$ es

$$S = \{21 + 13s \mid s \in \mathbb{Z}\}$$

Observación: La ecuación en $\mathbb{Z}_{13}$ tiene única solución y es $\overline{8}$

Teorema 111 *La congruencia* $ax \equiv b(\texttt{mod}\ n)$ *tiene solución en* $\mathbb{Z}$ *si y sólo si* $(a,n)|b$

Demostración: Supongamos que congruencia $ax \equiv b(\texttt{mod}\ n)$ tiene solución en $\mathbb{Z}$, luego existe $c \in \mathbb{Z}$ tal que

$$\begin{aligned} ac &\equiv b(\texttt{mod}\ n) \\ ac - nt &= b \end{aligned}$$

Por lo tanto la ecuación diofántica $ax + ny = b$ tiene solución, luego $(a,n)|b$.

En el otro sentido, suponemos que $(a,n)|b$, luego la ecuación diofántica $ax+ny = b$ tiene solución, sea x_0, y_0 una solución, por lo tanto

$$\begin{aligned} ax_0 + ny_0 &= b \\ ax_0 &\equiv b(\texttt{mod}\ n) \end{aligned}$$

□

Observación: recuerde que las soluciones esta dada por

$$x = x_0 + \frac{n}{(a,n)}t$$

es decir, en general la solución no es única en $\mathbb{Z}_n$

Ejemplo 59 *Resolver en* $\mathbb{Z}$*, la ecuación*

$$2x \equiv 6(\texttt{mod}\ 8)$$

Solución: Resolver la ecuación es equivalente a resolver

$$2x = 6 + 8t \quad \text{o bien} \quad x - 4t = 3$$

Como sabemos que

$$1(3) - 4(0) = 3$$

luego una solución particular es

$$x_0 = 3 \ \wedge \ t_0 = 0$$

Por lo tanto, la solución general esta dada por

$$x = 3 + 4s \ \wedge \ t = 0 + s, \quad s \in \mathbb{Z}$$

Con lo cual, la solución de la ecuación $2x \equiv 6(\texttt{mod}\ 8)$ es

$$S = \{3 + 4s \mid s \in \mathbb{Z}\}$$

Observación: La ecuación en $\mathbb{Z}_8$ tiene dos solución y son $\overline{3}, \overline{7}$

Propiedad 112 *Sean* $a_1, a_2, b_1, b_2, c_1c_2 \in \mathbb{Z}$ *y el sistema de ecuaciones lineales*

$$\boxed{\begin{array}{rcl} a_1x + b_1y & \equiv & c_1(\mathtt{mod}\ m) \\ a_2x + b_2y & \equiv & c_2(\mathtt{mod}\ m) \end{array}}$$

si $(a_1b_2 - a_2b_1, m) = 1$ *entonces tiene solución el sistema.*

Demostración: Dado el sistema

$$\boxed{\begin{array}{rcl} a_1x + b_1y & \equiv & c_1(\mathtt{mod}\ m) \\ a_2x + b_2y & \equiv & c_2(\mathtt{mod}\ m) \end{array}}$$

Amplificando las ecuaciones

$$\boxed{\begin{array}{rcll} a_1x + b_1y & \equiv & c_1(\mathtt{mod}\ m) & / \cdot a_2 \\ a_2x + b_2y & \equiv & c_2(\mathtt{mod}\ m) & / \cdot -a_1 \end{array}}$$

Sumando obtenemos

$$(a_2b_1 - a_1b_2)y = a_2c_1 - a_1c_2(\mathtt{mod}\ m)$$

Por el teorema anterior se obtiene el resto de la demostración □

Ejemplo 60 *Resolver:*

$$\boxed{\begin{array}{rcl} 2x + y & \equiv & 3(\mathtt{mod}\ 13) \\ 3x + 5y & \equiv & 1(\mathtt{mod}\ 13) \end{array}}$$

Solución:

$$\boxed{\begin{array}{rcll} 2x + y & \equiv & 3(\mathtt{mod}\ 13) & / \cdot -5 \\ 3x + 5y & \equiv & 1(\mathtt{mod}\ 13) & \end{array}}$$

$$\boxed{\begin{array}{rcl} -10x - 5y & \equiv & -15(\mathtt{mod}\ 13) \\ 3x + 5y & \equiv & 1(\mathtt{mod}\ 13) \end{array}}$$

Sumando obtenemos

$$\begin{array}{rcll} -7x & \equiv & -14(\mathtt{mod}\ 13) & / \cdot -7^{-1} \\ x & \equiv & -14(-7)^{-1}(\mathtt{mod}\ 13) & \\ x & \equiv & 2(\mathtt{mod}\ 13) & \end{array}$$

Reemplazando obtenemos

$$\begin{array}{rcll} y & \equiv & 3 - 2x(\mathtt{mod}\ 13) & \\ y & \equiv & 3 - 2 \cdot 2(\mathtt{mod}\ 13) & \\ y & \equiv & -1(\mathtt{mod}\ 13) & -1 + 13 = 12 \\ y & \equiv & 12(\mathtt{mod}\ 13) & \end{array}$$

Luego, el conjunto solución del sistema es

$$S = \{(x, y) \in \mathbb{Z}^2 \mid x \equiv 2(\mathtt{mod}\ 13) \ \wedge \ y \equiv 12(\mathtt{mod}\ 13)\}$$

Ejemplo 61 *Dada el par de congruencia*

$$x \equiv 1(\mathtt{mod}\ 4)\ \wedge\ x \equiv 2(\mathtt{mod}\ 3)$$

Construir una sola congruencia equivalente a las anteriores

Solución: La solución de las congruencia es:

$$S = \{x \in \mathbb{Z} \mid (\exists k_1 \in \mathbb{Z})(x = 4k_1 + 1)\} \cap \{x \in \mathbb{Z} \mid (\exists k_2 \in \mathbb{Z})(x = 3k_2 + 2)\}$$

Luego tenemos que dado $x \in S$ se tiene que

$$\begin{array}{rcl} x = 4k_1 + 1 & \wedge & x = 3k_2 + 2 \\ 4k_1 + 1 & = & 3k_2 + 2 \\ 4k_1 - 3k_2 & = & 1 \end{array}$$

Una solución particular de la ecuación diofántica es $k_1 = 1,\ k_2 = 1$ La solución general es

$$k_1 = 1 + 3t,\ k_2 = 1 + 4t$$

reemplazando obtenemos

$$\begin{array}{rcl} x = 4k_1 + 1 & \wedge & x = 3k_2 + 2 \\ x = 4(1 + 3t) + 1 & \wedge & x = 3(1 + 4t) + 2 \\ x = 5 + 12t & \wedge & x = 5 + 12t \end{array}$$

Por lo tanto

$$x \equiv 5(\mathtt{mod}\ 12)$$

Teorema 113 (Chino del Resto) *Si $(m_i, m_j) = 1$, para $i \neq j$, entonces el sistema de congruencias*

$$\left.\begin{array}{rcl} x & \equiv & a_1(\mathtt{mod}\ m_1) \\ x & \equiv & a_2(\mathtt{mod}\ m_2) \\ & \vdots & \\ x & \equiv & a_k(\mathtt{mod}\ m_k) \end{array}\right|$$

tiene solución. Y dos soluciones del sistema son congruentes $(\mathtt{mod}\ m_1 \cdot m_2 \cdots m_k)$.

Demostración: Sea $m = m_1 \cdot m_2 \cdot m_3 \cdots m_k$, luego tenemos que $(\frac{m}{m_j}, m_j) = 1$. Por lo tanto,

$$(\exists b_j \in \mathbb{Z})(\ \frac{m}{m_j} b_j \equiv 1(\mathtt{mod}\ m_j)\ )$$

Notemos que

$$\frac{m}{m_j} b_j a_j \equiv a_j(\mathtt{mod}\ m_j) \wedge \frac{m}{m_j} b_j a_j \equiv 0(\mathtt{mod}\ m_i) \text{ con } i \neq j$$

Definimos

$$x_0 = \sum_{i=1}^{k} \frac{m}{m_i} b_i a_i$$

Luego se tiene que x_0 es solución particular del sistema de congruencias.

Además sean x_1 y x_2 dos soluciones del sistema de congruencias, luego se tiene que

$$x_1 \equiv a_i(\mathtt{mod}\ m_i) \qquad x_2 \equiv a_i(\mathtt{mod}\ m_i)$$

es decir

$$x_1 - x_2 \equiv 0(\mathtt{mod}\ m_i))$$

Con lo cual obtenemos

$$x_1 - x_2 = m_1 t_1 = m_2 t_2 = \cdots = m_k t_k$$

Así se obtiene $m_2 | m_1 t_1$ y como $(m_1, m_2) = 1$ entonces $m_2 | t_1$,

$$x_1 - x_2 = m_1 m_2 t_1' = m_3 t_3 = \cdots = m_k t_k$$

Repitiendo el proceso tenemos que $m_3 | m_1 m_2 t_1'$ y como $(m_3, m_1) = (m_3, m_2) = 1$ entonces $m_3 | t_1'$, continuando de la misma manera se obtiene en forma recursiva que

$$x_1 - x_2 = m_1 m_2 m_3 \cdots m_k t_k' \equiv 0(\mathtt{mod}\ m_1 m_2 m_3 \cdots m_k)$$

□

Ejemplo 62 *Resolver:*

$$\begin{array}{rcl} x & \equiv & 2(\mathtt{mod}\ 3) \\ x & \equiv & 3(\mathtt{mod}\ 5) \\ x & \equiv & 2(\mathtt{mod}\ 7) \end{array}$$

Solución: Notemos que $(3,5) = 1,\ (5,7) = 1,\ (3,7) = 1$ y $m = m_1 \cdot m_2 \cdot m_3 = 105$

$$\begin{array}{rcl} \frac{m}{m_1} \cdot b_1 & \equiv & 1(\mathtt{mod}\ m_1) \\ 35 \cdot b_1 & \equiv & 1(\mathtt{mod}\ 3) \\ b_1 & \equiv & 2(\mathtt{mod}\ 3) \end{array} \qquad \begin{array}{rcl} \frac{m}{m_2} \cdot b_2 & \equiv & 1(\mathtt{mod}\ m_2) \\ 21 \cdot b_2 & \equiv & 1(\mathtt{mod}\ 5) \\ b_2 & \equiv & 1(\mathtt{mod}\ 5) \end{array} \qquad \begin{array}{rcl} \frac{m}{m_3} \cdot b_3 & \equiv & 1(\mathtt{mod}\ m_3) \\ 15 \cdot b_3 & \equiv & 1(\mathtt{mod}\ 7) \\ b_3 & \equiv & 1(\mathtt{mod}\ 7) \end{array}$$

Luego la solución particular es:

$$\begin{array}{rcl} x_0 & = & a_1 \cdot b_1 \cdot \dfrac{m}{m_1} + a_2 \cdot b_2 \cdot \dfrac{m}{m_2} + a_3 \cdot b_3 \cdot \dfrac{m}{m_3} \\ x_0 & = & 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 \\ x_0 & = & 233 \end{array}$$

La solución general esta dada por

$$\begin{array}{rcl} x & \equiv & x_0(\mathtt{mod}\ m) \\ x & \equiv & 233(\mathtt{mod}\ 105) \\ x & \equiv & 23(\mathtt{mod}\ 105) \end{array}$$

Otra forma de resolver es: En la primera obtenemos que $x = 2 + 3t$ con $t \in \mathbb{Z}$, reemplazando en la segunda se tiene que

$$\begin{aligned} x &\equiv 3(\texttt{mod } 5) \\ 2+3t &\equiv 3(\texttt{mod } 5) \\ 3t &\equiv 1(\texttt{mod } 5) \\ t &\equiv 2(\texttt{mod } 5) \end{aligned}$$

de lo cual obtenemos que $t = 2 + 5r$, reemplazando obtenemos

$$x = 2 + 3t = 2 + 3(2 + 5r) = 8 + 15r$$

Ahora reemplazamos en la tercera congruencia

$$\begin{aligned} x &\equiv 2(\texttt{mod } 7) \\ 8+15r &\equiv 2(\texttt{mod } 7) \\ r &\equiv -6(\texttt{mod } 7) \\ r &\equiv 1(\texttt{mod } 7) \end{aligned}$$

De este modo tenemos que $r = 1 + 7l$ reemplazando tenemos

$$x = 8 + 15r = 8 + 15(1 + 7l) = 23 + 105l$$

luego

$$x \equiv 23(\texttt{mod } 105)$$

De este modo se tiene que el conjunto solución es

$$S = \{23 + 105t \mid t \in \mathbb{Z}\}$$

3.4. Teorema Euler y Fermat

Definición 35 *Sean $n \in \mathbb{Z}^+$ y $S = \{r_1, r_2, \ldots r_{\phi(n)}\} \subseteq \mathbb{Z}$, se dice que S es un sistema* ***reducido*** *módulo n si y sólo si $\mathcal{U}(\mathbb{Z}_n) = \{\overline{r}_1, \overline{r}_2, \ldots \overline{r}_{\phi(n)}\}$*

Observación: Tenga presente que $(n, r_i) = 1$ para todo $i \in \{1, 2, \ldots, \phi(n)\}$.

Teorema 114 *Sean $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ tal que $(a, n) = 1$ y $\{r_1, r_2, \ldots r_{\phi(n)}\}$ un sistema reducido módulo n, entonces $\{ar_1, ar_2, \ldots ar_{\phi(n)}\}$ otro sistema reducido módulo n*

Demostración: Como $(a, n) = 1$ y $(r_i, n) = 1$, entonces para todo i se tiene que $(ar_i, n) = 1$.

Ahora veremos que las clases son distintas, para ello notemos que

$$ar_i \equiv ar_j(\texttt{mod } n) \Leftrightarrow r_i \equiv r_j(\texttt{mod } n)$$

Luego si $i \neq j \Rightarrow r_i \not\equiv r_j(\texttt{mod } n)$ □

Teorema 115 *Sean $p \in \mathbb{Z}^+$, primo y $\{r_1, r_2, \ldots r_{\phi(p)}\}$ un sistema reducido módulo p, entonces*

$$r_1 r_2, \cdots r_{\phi(p)} \equiv -1(\mathtt{mod}\ p)$$

Demostración: Supongamos que $p \neq 2$, luego $1 \not\equiv -1(\mathtt{mod}\ p)$, ahora reordenemos el producto

$$r_1 r_2 \cdots r_{\phi(p)} \equiv (1)(-1) r_1'(r_1')^{-1} \cdots r_l'(r_l')^{-1} \equiv -1(\mathtt{mod}\ p)$$

□

Observación: La demostración anterior se puede extender para el caso que $\mathcal{U}(\mathbb{Z}_n)$ es cíclico.

Corolario 116 (Teorema de Wilson) *Sean $p \in \mathbb{Z}^+$, primo*

$$(p-1)! \equiv -1(\mathtt{mod}\ p)$$

Teorema 117 (Euler) *Sean $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ tal que $(a, n) = 1$ entonces*

$$a^{\phi(n)} \equiv 1(\mathtt{mod}\ n)$$

Demostración: Sea $\{r_1, r_2, \ldots r_{\phi(n)}\}$ un sistema reducido módulo n, como $(a, n) = 1$ entonces $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ un sistema reducido módulo n. luego tenemos

$$\begin{aligned} r_1 r_2, \cdots r_{\phi(n)} &\equiv (ar_1)(ar_2)\cdots(ar_{\phi(n)})(\mathtt{mod}\ n) \\ r_1 r_2, \cdots r_{\phi(n)} &\equiv (a)^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)}(\mathtt{mod}\ n) \\ 1 &\equiv (a)^{\phi(n)}(\mathtt{mod}\ n) \end{aligned}$$

□

Ejemplo 63 *Determinar el resto al dividir 7^{1000} por 48*

Solución: Como $(7, 48) = 1 \Rightarrow 7^{\phi(48)} \equiv 1(\mathtt{mod}\ 48)$

$$\phi(48) = \phi(2^4 3) = \phi(2^4)\phi(3) = (2^4 - 2^3)\cdot(3-1) = 2^3\,(2-1)\,2 = 2^4 = 16.$$

Luego tenemos que $7^{16} \equiv 1(\mathtt{mod}\ 48)$.

Aplicamos el algoritmo de la división, obtenemos que $1000 = 16 \cdot 62 + 8$

$$\begin{aligned} 7^{1000} &\equiv 7^{16\cdot 62+8}(\mathtt{mod}\ 48) \\ 7^{1000} &\equiv (7^{16})^{62} \cdot 7^8(\mathtt{mod}\ 48) \\ 7^{1000} &\equiv 1^{62}(7^2)^4(\mathtt{mod}\ 48) \\ 7^{1000} &\equiv 1 \cdot (49)^4(\mathtt{mod}\ 48),\ \text{ya que } 49 \equiv 1(\mathtt{mod}\ 48) \\ 7^{1000} &\equiv 1^4(\mathtt{mod}\ 48) \\ 7^{1000} &\equiv 1(\mathtt{mod}\ 48) \end{aligned}$$

Por lo tanto el resto al dividir 7^{1000} por 48 es 1

Teorema 118 (Fermat) *Sean $p \in \mathbb{Z}^+$ un número primo, $a \in \mathbb{Z}$ tal que $(a, n) = 1$ entonces*

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

Ejemplo 64 *Resolver la ecuación*

$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0(\mathtt{mod}\ 5)$$

Solución: Al factorizar la expresión, tenemos

$$x(3x^{13} + 4x^{12} + 3x^{11} + 2x^{10} + x^8 + 2x^7 + 4x^6 + x^5 + 3x^3 + x^2 + 4x + 2) \equiv 0(\mathtt{mod}\ 5)$$

note que 5 es un número primo, luego no tiene divisores de cero, de esta manera se tiene

$$x \equiv 0 \quad \vee \quad 3x^{13} + 4x^{12} + 3x^{11} + 2x^{10} + x^8 + 2x^7 + 4x^6 + x^5 + 3x^3 + x^2 + 4x + 2 \equiv 0(\mathtt{mod}\ 5)$$

Para las raíces no nulas, aplicamos el teorema Fermat, es decir $x^4 \equiv 1(\mathtt{mod}\ 5)$, con $x \not\equiv 0(\mathtt{mod}\ 5)$, luego tenemos $x^{4q+r} \equiv x^r(\mathtt{mod}\ 5)$

$$13 \equiv 1;\ 12 \equiv 0;\ 11 \equiv 3;\ 10 \equiv 2;\ 8 \equiv 0;\ 7 \equiv 3;\ 6 \equiv 2;\ 5 \equiv 1;\ 8 \equiv 0;\ (\mathtt{mod}\ 4)$$

$$\begin{aligned}
3x^{13} + 4x^{12} + 3x^{11} + 2x^{10} + x^8 + 2x^7 + 4x^6 + x^5 + 3x^3 + x^2 + 4x + 2 &\equiv 0(\mathtt{mod}\ 5)\\
3x^1 + 4x^0 + 3x^3 + 2x^2 + x^0 + 2x^3 + 4x^2 + x^1 + 3x^3 + x^2 + 4x^1 + 2 &\equiv (0\mathtt{mod}\ 5)\\
(3+2+3)x^3 + (2+4+1)x^2 + (3+1+4)x + (4+1+2) &\equiv 0(\mathtt{mod}\ 5)\\
3x^3 + 2x^2 + 3x + 2 &\equiv 0(\mathtt{mod}\ 5)\\
3x(x^2+1) + 2(x^2+1) &\equiv 0(\mathtt{mod}\ 5)\\
(3x+2)(x^2+1) &\equiv 0(\mathtt{mod}\ 5)
\end{aligned}$$

Luego tenemos que

$$3x + 2 \equiv 0(\mathtt{mod}\ 5)\ \vee\ (x^2 + 1) \equiv 0(\mathtt{mod}\ 5)$$

La primera ecuación obtenemos que

$$(3x + 2) \equiv 0(\mathtt{mod}\ 5) \Leftrightarrow 3x \equiv -2(\mathtt{mod}\ 5) \Leftrightarrow x \equiv -4 \equiv 1(\mathtt{mod}\ 5)$$

La segunda ecuación

$$x^2 + 1 \equiv 0(\mathtt{mod}\ 5) \Leftrightarrow x^2 - 4 \equiv 0(\mathtt{mod}\ 5) \Leftrightarrow (x-2)(x+2) \equiv 0(\mathtt{mod}\ 5)$$

de lo cual obtenemos

$$x \equiv 2(\mathtt{mod}\ 5)\ \vee\ x \equiv -2 \equiv 3(\mathtt{mod}\ 5)$$

Por lo tanto el conjunto solución es

$$S = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

3.5. Congruencia de grado 2

Solamente resolveremos ecuaciones de segundo grado en $\mathbb{Z}_p$, con p primo impar, ya que en este caso $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Sean $a, b, c \in \mathbb{Z}^*$, tal que $(a, p) = 1$, entonces debemos estudiar el conjunto solución de la ecuación

$$ax^2 + bx + c \equiv 0(\texttt{mod } p)$$

La solución en general podemos obtenerla de

$$\begin{aligned} ax^2 + bx + c &\equiv 0(\texttt{mod } p) \ /4a \\ 4a^2x^2 + 4abx + 4ac &\equiv 0(\texttt{mod } p) \\ (2ax)^2 + 2(2ax)b + 4ac &\equiv 0(\texttt{mod } p)/ + b^2 \\ (2ax)^2 + 2(2ax)b + +b^2 + 4ac &\equiv b^2(\texttt{mod } p) \ / - 4ac \\ (2ax + b)^2 &\equiv b^2 - 4ac(\texttt{mod } p) \end{aligned}$$

Definición 36 *Sea $\Delta = b^2 - 4ac$, se llama el discriminate de la ecuación*

$$ax^2 + bx + c \equiv 0(\texttt{mod } p)$$

Observación: Realizando un cambio de variable $z = 2ax + b$ la ecuación cuadrática se traduce en

$$z^2 \equiv \Delta(\texttt{mod } p)$$

Definición 37 *Sea $a \in \mathbb{Z}^*$ tal que $(a, p) = 1$.*

*Se dice que a es un **residuo** cuadrático o un cuadrado módulo p si y sólo si $x^2 \equiv a(\texttt{mod } p)$ tiene solución, de otro modo si existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a(\texttt{mod } p)$.*

En caso contrario, se dice que a no es un residuo cuadrático o que no es un cuadrado módulo p.

Notación: Se denota el conjunto de los cuadrado módulo p

$$\square_p = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_p)\}.$$

Ejemplo 65 *Determinar el conjunto $\square_5 = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_5)\}$ y $\not\square_5 = \mathcal{U}(\mathbb{Z}_5) - \square_5$*

Solución: Calculemos el cuadrado de cada elemento

$$\overline{1}^2 = 1 \ (\texttt{mod } 5) \quad \overline{2}^2 = 4 \ (\texttt{mod } 5) \quad \overline{3}^2 = 4 \ (\texttt{mod } 5) \quad \overline{4}^2 = 1 \ (\texttt{mod } 5)$$

Luego tenemos

$$\square_5 = \{\overline{1}, \overline{4}\} \qquad \not\square_5 = \{\overline{2}, \overline{3}\}$$

Ejemplo 66 *Resolver las ecuaciones*

$$x^2 \equiv 2(\texttt{mod } 7) \qquad x^2 \equiv 3(\texttt{mod } 7)$$

Solución: Al calcular el cuadrado de cada elemento obtenemos que

$$\begin{aligned}\square_7 &= \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_7)\} \\ &= \{\overline{1}^2,\ \overline{2}^2,\ \overline{3}^2,\ \overline{4}^2,\ \overline{5}^2,\ \overline{6}^2\} \\ &= \{\overline{1},\ \overline{4},\ \overline{2},\ \overline{2},\ \overline{4},\ \overline{1}\} \\ &= \{\overline{1},\ \overline{4},\ \overline{2}\}.\end{aligned}$$

Luego la ecuación $x^2 \equiv 2(\texttt{mod } 7)$, tiene dos soluciones en $\mathbb{Z}_7$ y son $\overline{3},\ \overline{4}$. El conjunto solución de la otra ecuación $x^2 \equiv 3(\texttt{mod } 7)$, es vacío.

Teorema 119 *La congruencia* $ax^2 + bx + c \equiv 0(\texttt{mod } p)$ *tiene solución no vacía si y sólo si* $\overline{\Delta} \in \square_p \cup \{\overline{0}\}$

Teorema 120 *El conjunto* $\square_p$ *es un subgrupo de* $\mathcal{U}(\mathbb{Z}_p)$.

Demostración: i) *Clausura*: Sean $\overline{x}^2,\ \overline{y}^2 \in \square_p$, entonces tenemos

$$\overline{x}^2 \cdot \overline{y}^2 = (\overline{x} \cdot \overline{y})^2 \in \square_p$$

ii) *Neutro*:

$$\overline{1} = \overline{1}^2 \in \square_p$$

iii) *Inverso*:

$$(\overline{x}^2)^{-1} = (\overline{x}^{-1})^2 \in \square_p$$

Por lo tanto se tiene que $\square_p$ es un subgrupo de $\mathcal{U}(\mathbb{Z}_p)$. □

Teorema 121 *Sea* $p \in \mathbb{Z}$*, un número primo impar entonces*

$$|\square_p| = \frac{p-1}{2}$$

Demostración: Sean $\overline{a}, \overline{b}, \overline{c} \in \mathcal{U}(\mathbb{Z}_p)$ se define la siguiente relación

$$\overline{a} \sim \overline{b} \ \Leftrightarrow\ \overline{a}^2 = \overline{b}^2$$

Veremos que $\sim$ es una relación de equivalencia

Es *Refleja*: $\overline{a}^2 = \overline{a}^2 \ \Leftrightarrow\ \overline{a} \sim \overline{a}$

Es *Simétrica*: $\overline{a} \sim \overline{b} \ \Leftrightarrow\ \overline{a}^2 = \overline{b}^2 \ \Leftrightarrow\ \overline{b}^2 = \overline{a}^2 \ \Leftrightarrow \overline{b} \sim \overline{a}$

Es *Transitiva*: Si $\overline{a} \sim \overline{b} \ \wedge\ \overline{b} \sim \overline{c}$, entonces $\overline{a}^2 = \overline{b}^2 \ \wedge\ \overline{b}^2 = \overline{c}^2$, de lo cual se obtiene $\overline{a}^2 = \overline{c}^2$, es decir, $\overline{a} \sim \overline{c}$.

Luego $\sim$ es una relación de equivalencia, ahora nos interesa determinar la cardinalidad de cada clase

$$\overline{a} \sim \overline{b} \Leftrightarrow \overline{a}^2 = \overline{b}^2 \Leftrightarrow \overline{a}^2 - \overline{b}^2 = \overline{0} \Leftrightarrow (\overline{a} - \overline{b})(\overline{a} + \overline{b}) = \overline{0} \Leftrightarrow (\overline{b} = \overline{a} \ \vee\ \overline{b} = -\overline{a})$$

Luego la clase de $\overline{a}$, denotada por

$$[\overline{a}] = \{\overline{a}, -\overline{a}\},$$

contiene dos elemento siempre, ya que p es un primo impar.

Ahora bien, sea r el número de clases de equivalencia, por lo tanto $2r = p-1$, es decir, $r = \frac{p-1}{2}$.

De lo cual obtenemos que

$$\begin{array}{rccc} f: & \mathcal{U}(\mathbb{Z}_p)/\sim & \to & \square_p \\ & [\overline{a}] & \to & \overline{a}^2 \end{array}$$

es una función biyectiva, luego $|\square_p| = \frac{p-1}{2}$ □

Teorema 122 *Sea p un número primo impar y $a \in \mathbb{Z}$ tal que $(a,p) = 1$ entonces*

$$a^{\frac{p-1}{2}} \equiv 1(\mathtt{mod}\ p) \quad \vee\ a^{\frac{p-1}{2}} \equiv -1(\mathtt{mod}\ p)$$

Demostración: Por Teorema de Fermat, tenemos que

$$\begin{array}{rcl} a^{p-1} & \equiv & 1(\mathtt{mod}\ p) \\ (a^{\frac{p-1}{2}})^2 & \equiv & 1(\mathtt{mod}\ p) \\ (a^{\frac{p-1}{2}})^2 - 1 & \equiv & 0(\mathtt{mod}\ p) \\ (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) & \equiv & 0(\mathtt{mod}\ p) \end{array}$$

Por lo tanto

$$a^{\frac{p-1}{2}} \equiv 1(\mathtt{mod}\ p) \quad \vee\ a^{\frac{p-1}{2}} \equiv -1(\mathtt{mod}\ p)$$

□

Teorema 123 *Sea p un número primo impar y $a \in \mathbb{Z}$ entonces*

$$\overline{a} \in \square_p \quad \Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv 1(\mathtt{mod}\ p)$$

Demostración: Sea $\overline{a} \in \square_p$ entonces existe $b \in \mathbb{Z}$, tal que $\overline{a} = \overline{b}^2$ de lo cual obtenemos

$$\begin{array}{rcl} a^{\frac{p-1}{2}} & \equiv & (b^2)^{\frac{p-1}{2}}(\mathtt{mod}\ p) \\ & \equiv & b^{p-1} \equiv 1(\mathtt{mod}\ p) \end{array}$$

En la otra dirección, sabemos $\mathbb{Z}_p$ es cuerpo y $\mathcal{U}(\mathbb{Z}_p)$, es cíclico, luego todo los elemento de $\square_p$ son $\frac{p-1}{2}$ y son raíces del polinomio $a^{\frac{p-1}{2}} \equiv 1(\mathtt{mod}\ p)$ y este polinomio tiene a lo más $\frac{p-1}{2}$, luego son las únicas las que pertenecen a $\square_p$ □

Propiedad 124 *Sean p un número primo impar y $a \in \mathbb{Z}$ tal que $a \notin \mathcal{U}(\mathbb{Z}_p) - \square_p$ entonces*

$$a^{\frac{p-1}{2}} \equiv -1(\mathtt{mod}\ p)$$

Definición 38 (Símbolo de Legendre) *Sea p un número primo impar y $a \in \mathbb{Z}$ tal que $(a,p)=1$.*

Se define

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad \overline{a} \in \square_p \\ -1 & si \quad \overline{a} \notin \square_p \end{cases}$$

Ejemplo 67 *En en el ejemplo 66 tenemos que*

$$\square_7 = \{\overline{1},\ \overline{2},\ \overline{4}\} \quad \not\square_7 = \{\overline{3},\ \overline{5},\ \overline{6}\}$$

De lo anterior tenemos que

$$\left(\frac{1}{7}\right)=1;\ \left(\frac{2}{7}\right)=1;\ \left(\frac{4}{7}\right)=1;\ \left(\frac{3}{7}\right)=-1;\ \left(\frac{5}{7}\right)=-1;\ \left(\frac{6}{7}\right)=-1$$

Propiedad 125 *Sean p un número primo impar y $a,b \in \mathbb{Z}$ tales que $(a,p)=(b,p)=1$.*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathtt{mod}\ p)$
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. *Si* $a \equiv b (\mathtt{mod}\ p)$ *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Demostración: La demostración de (1), se obtiene por el teorema 122, (2) es inmediata, la demostración de (3) por caso:

- Si $a^{\frac{p-1}{2}} \equiv 1 (\mathtt{mod}\ p)$ y $b^{\frac{p-1}{2}} \equiv 1 (\mathtt{mod}\ p)$ luego tenemos

  $$1 \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} (\mathtt{mod}\ p)$$

  Luego se cumple

  $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

- Si $a^{\frac{p-1}{2}} \equiv 1 (\mathtt{mod}\ p)$ y $b^{\frac{p-1}{2}} \equiv -1 (\mathtt{mod}\ p)$ luego tenemos

  $$-1 \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} (\mathtt{mod}\ p)$$

  Luego se cumple

  $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

- Si $a^{\frac{p-1}{2}} \equiv -1(\mathtt{mod}\ p)$ y $b^{\frac{p-1}{2}} \equiv -1(\mathtt{mod}\ p)$ luego tenemos

$$1 \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} (\mathtt{mod}\ p)$$

Luego se cumple

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Ejemplo 68 *Calcular*

$$\left(\frac{1785}{13}\right)$$

Solución: Usando el algoritmo de la división tenemos $1785 = 13 \cdot 137 + 4$, luego

$$\left(\frac{1785}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$$

Propiedad 126 *Sea p un número primo impar entonces*

1. $p \equiv 1(\mathtt{mod}\ 4) \Leftrightarrow \overline{-1} \in \square_p$
2. $p \equiv 3(\mathtt{mod}\ 4) \Leftrightarrow \overline{-1} \in \not\square_p$

Demostración: Sea $p \equiv 1(\mathtt{mod}\ 4)$, luego tenemos $\frac{p-1}{4} \in \mathbb{Z}$.

Por la propiedad 124 tenemos $-1 \equiv ((a)^{\frac{p-1}{2}}) \equiv ((a)^{\frac{p-1}{4}})^2$, luego $\overline{-1} \in \square_p$.

En el otro sentido tenemos $\overline{-1} \in \square_p$, por lo tanto $(-1)^{\frac{p-1}{2}} = 1$, luego $\frac{p-1}{2}$ debe ser un número par, de lo cual $4|(p-1)$ es decir, $p \equiv 1(\mathtt{mod}\ 4)$.

Ejemplo 69 *Resolver*

$$x^2 \equiv -1(\mathtt{mod}\ 31)$$

Solución: Como $31 \equiv 3(\mathtt{mod}\ 4)$, luego $\overline{-1} \in \not\square_{31}$, es decir, el conjunto solución es vació.

Teorema 127 *Sea p un número primo impar entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Ejemplo 70 *Resolver*

$$x^2 \equiv 2(\mathtt{mod}\ 11)$$

Solución: Como $\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$, luego $\overline{-1} \in \not\square_{11}$, es decir, el conjunto solución es vació.

Teorema 128 (Reciprocidad Cuadrática) *Sean p, q dos números primos impares distintos*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

o bien

$$\left(\frac{p}{q}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}\left(\frac{q}{p}\right)$$

Ejemplo 71 *Calcular*

$$\left(\frac{31}{1009}\right)$$

Solución: Usando reciprocidad cuadrática tenemos

$$\begin{aligned}\left(\frac{31}{1009}\right) &= (-1)^{\left(\frac{31-1}{2}\right)\left(\frac{1009-1}{2}\right)}\left(\frac{1009}{31}\right)\\ \left(\frac{31}{1009}\right) &= (-1)^{(15)(504)}\left(\frac{31\cdot 32+17}{31}\right)\\ \left(\frac{31}{1009}\right) &= ((-1)^{504})^{15}\left(\frac{17}{31}\right)=\left(\frac{17}{31}\right)\end{aligned}$$

Aplicando nuevamente

$$\begin{aligned}\left(\frac{17}{31}\right) &= (-1)^{\left(\frac{17-1}{2}\right)\left(\frac{31-1}{2}\right)}\left(\frac{31}{17}\right)\\ \left(\frac{17}{31}\right) &= (-1)^{(8)(15)}\left(\frac{17\cdot 1+14}{17}\right)\\ \left(\frac{17}{31}\right) &= ((-1)^{8})^{15}\left(\frac{14}{17}\right)=\left(\frac{2\cdot 7}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)\end{aligned}$$

Pero

$$\left(\frac{7}{17}\right) = (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{17-1}{2}\right)}\left(\frac{17}{7}\right)=\left(\frac{3}{7}\right)$$

Pero tenemos

$$\left(\frac{3}{7}\right)=-1\ ;\ \left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=(-1)^{36}=1$$

de esta manera obtenemos

$$\left(\frac{31}{1009}\right)=\left(\frac{17}{31}\right)=\left(\frac{14}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{7}\right)=-1$$

3.6. Ejercicios Desarrollados

Ejemplo 72 *Resolver en* $\mathbb{Z}_{25}$*:*

$$\overline{x}+\overline{41}=\overline{17}$$

Solución:

$$\begin{aligned}\overline{x}+\overline{41} &= \overline{17}\\ \overline{x} &= \overline{17}-\overline{41}\\ \overline{x} &= -\overline{24};\quad -24+25=1\\ \overline{x} &= \overline{1}\end{aligned}$$

Ejemplo 73 *Resolver:*

$$\begin{array}{rcl} 2x+3y+z & \equiv & 8(\mathtt{mod}\ 17) \\ x+4y+5z & \equiv & 5(\mathtt{mod}\ 17) \\ 3x+8y-z & \equiv & 0(\mathtt{mod}\ 17) \end{array}$$

Solución: Despejando z en la primera congruencia tenemos

$$z \equiv 8-2x-3y(\mathtt{mod}\ 17)$$

reemplazando en la segunda congruencia tenemos

$$\begin{array}{rcll} x+4y+5\cdot(8-2x-3y) & \equiv & 5(\mathtt{mod}\ 17) & \\ x+4y+40-10x-15y & \equiv & 5(\mathtt{mod}\ 17) & \\ -9x & \equiv & -35+11y(\mathtt{mod}\ 17) & \\ 8x & \equiv & 16+11y(\mathtt{mod}\ 17) & /\cdot -2 \\ -16x & \equiv & -32-22y(\mathtt{mod}\ 17) & \\ x & \equiv & 2+12y(\mathtt{mod}\ 17) & \end{array}$$

Ahora reemplazando x en $z \equiv 8-2x-3y(\mathtt{mod}\ 17)$

$$\begin{array}{rcl} z & \equiv & 8-2\cdot(2+12y)-3y(\mathtt{mod}\ 17) \\ z & \equiv & 8-4-24y-3y(\mathtt{mod}\ 17) \\ z & \equiv & 4-27y(\mathtt{mod}\ 17) \\ z & \equiv & 4+7y(\mathtt{mod}\ 17) \end{array}$$

Ahora reemplazamos $x \equiv 2+12y(\mathtt{mod}\ 17)$ y $z \equiv 4+7y(\mathtt{mod}\ 17)$ en la tercera congruencia, y obtenemos

$$\begin{array}{rcl} 3x+8y-z & \equiv & 0(\mathtt{mod}\ 17) \\ 3\cdot(2+12z)+8y-(4+7y) & \equiv & 0(\mathtt{mod}\ 17) \\ 6+36y+8y-4-7y & \equiv & 0(\mathtt{mod}\ 17) \\ 37y & \equiv & -2(\mathtt{mod}\ 17) \\ 3y & \equiv & 15(\mathtt{mod}\ 17) \\ y & \equiv & 5(\mathtt{mod}\ 17) \end{array}$$

$$\begin{array}{rcl} x & \equiv & 2+12y(\mathtt{mod}\ 17) \\ x & \equiv & 2+12\cdot 5(\mathtt{mod}\ 17) \\ x & \equiv & 62(\mathtt{mod}\ 17) \\ x & \equiv & 11(\mathtt{mod}\ 17) \end{array} \qquad \begin{array}{rcl} z & \equiv & 4+7y(\mathtt{mod}\ 17) \\ z & \equiv & 4+7\cdot 5(\mathtt{mod}\ 17) \\ z & \equiv & 39(\mathtt{mod}\ 17) \\ z & \equiv & 5(\mathtt{mod}\ 17) \end{array}$$

De esta manera se tiene que

$$x \equiv 11(\mathtt{mod}\ 17) \qquad y \equiv 5(\mathtt{mod}\ 17) \qquad z \equiv 5(\mathtt{mod}\ 17)$$

Ejemplo 74 *Hacer la tabla de los grupos:*

a) $(\mathbb{Z}_7, +)$

Solución:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

b) $(\mathbb{Z}_{13}, +)$

Solución:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{9}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{10}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{11}$	$\overline{11}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{12}$	$\overline{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$

c) $(\mathcal{U}(\mathbb{Z}_7), \cdot)$

Solución:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ejemplo 75 *Calcular el reticulado de los subgrupos de* $(\mathbb{Z}_{12}, +)$

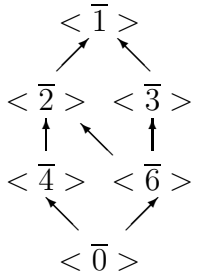
Solución: $\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{12}, +) \Leftrightarrow |\mathcal{H}|/|\mathcal{G}| = 12$ luego $|\mathcal{H}| \in \{1, 2, 3, 4, 6, 12\}$

$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$
$< \overline{0} >= \{\overline{0}\}$
$< \overline{1} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$
$< \overline{2} >= \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{0}\}$
$< \overline{3} >= \{\overline{3}, \overline{6}, \overline{9}, \overline{0}\}$
$< \overline{4} >= \{\overline{4}, \overline{8}, \overline{0}\}$
$< \overline{5} >= \{\overline{5}, \overline{10}, \overline{3}, \overline{8}, \overline{1}, \overline{6}, \overline{11}, \overline{4}, \overline{9}, \overline{2}, \overline{7}, \overline{0}\}$
$< \overline{6} > \{\overline{6}, \overline{0}\}$
$< \overline{7} >= \{\overline{7}, \overline{2}, \overline{9}, \overline{4}, \overline{11}, \overline{6}, \overline{1}, \overline{8}, \overline{3}, \overline{10}, \overline{5}, \overline{0}\}$
$< \overline{8} >= \{\overline{8}, \overline{4}, \overline{0}\}$
$< \overline{9} >= \{\overline{9}, \overline{6}, \overline{3}, \overline{0}\}$
$< \overline{10} >= \{\overline{10}, \overline{8}, \overline{6}, \overline{4}, \overline{2}, \overline{0}\}$
$< \overline{11} > \{\overline{11}, \overline{10}, \overline{9}, \overline{8}, \overline{7}, \overline{6}, \overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}, \overline{0}\}$

orden	subgrupo
1	$< \overline{0} >$
2	$< \overline{6} >$
3	$< \overline{4} >, < \overline{8} >$
4	$< \overline{3} >, < \overline{9} >$
6	$< \overline{2} >, < \overline{10} >$
12	$< \overline{1} >, < \overline{5} >, < \overline{7} >, < \overline{11} >$

$< \overline{0} > \subset < \overline{6} > \subset < \overline{3} > \subset < \overline{1} >$
$< \overline{0} > \subset < \overline{4} > \subset < \overline{2} > \subset < \overline{1} >$
$< \overline{0} > \subset < \overline{6} > \subset < \overline{2} > \subset < \overline{1} >$

Reticulado:



Ejemplo 76 *Calcular el reticulado de los subgrupos de* $(\mathbb{Z}_{10}, +)$

Solución: $\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{10}, +) \Leftrightarrow |\mathcal{H}|/|\mathcal{G}| = 10$, luego $|\mathcal{H}| \in \{1, 2, 5, 10\}$,
$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$.

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

orden	subgrupo
1	$< \overline{0} >$
2	$< \overline{5} >$
5	$< \overline{2} >, < \overline{4} >, < \overline{6} >, < \overline{8} >$
10	$< \overline{1} >, < \overline{3} >, < \overline{7} >, < \overline{9} >$

$$<\overline{0}>\subset<\overline{5}>\subset<\overline{2}>\subset<\overline{1}>$$

Reticulado:

$$<\overline{0}> \rightarrow <\overline{5}> \rightarrow <\overline{2}> \rightarrow <\overline{1}>$$

Ejemplo 77 *Determinar subgrupos de* $(\mathcal{U}(\mathbb{Z}_{13}), \cdot)$

Solución: $\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{13}^*, \cdot) \Leftrightarrow |\mathcal{H}|/|\mathcal{G}| = 12$ luego $|\mathcal{H}| \in \{1,2,3,4,6,12\}$,
$\mathbb{Z}_{13}^* = \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12}\}$

$<\overline{1}>=\{\overline{1}\}$
$<\overline{2}>=\{\overline{2},\overline{4},\overline{8},\overline{3},\overline{6},\overline{12},\overline{11},\overline{9},\overline{5},\overline{10},\overline{7},\overline{1}\}$
$<\overline{3}>=\{\overline{3},,\overline{9},\overline{1}\}$
$<\overline{4}>=\{\overline{4},\overline{3},\overline{12},\overline{9},\overline{10},\overline{1}\}$
$<\overline{5}>=\{\overline{5},\overline{12},\overline{8},\overline{1}\}$
$<\overline{6}>=\{\overline{6},\overline{10},\overline{8},\overline{9},\overline{212},\overline{7},\overline{3},\overline{5},\overline{4},\overline{11},\overline{1}\}$
$<\overline{7}>=\{\overline{7},\overline{10},\overline{5},\overline{9},\overline{11},\overline{12},\overline{6},\overline{3},\overline{8},\overline{4},\overline{2},\overline{1}\}$
$<\overline{8}>=\{\overline{8},\overline{12},\overline{5},\overline{1}\}$
$<\overline{9}>=\{\overline{9},\overline{3},\overline{1}\}$
$<\overline{10}>=\{\overline{10},\overline{9},\overline{12},\overline{3},\overline{4},\overline{1}\}$
$<\overline{11}>=\{\overline{11},\overline{4},\overline{5},\overline{3},\overline{7},\overline{12},\overline{2},\overline{9},\overline{8},\overline{10},\overline{6},\overline{1}\}$
$<\overline{12}>=\{\overline{12},\overline{1}\}$

orden	subgrupo
1	$<\overline{1}>$
2	$<\overline{12}>$
3	$<\overline{3}>,<\overline{9}>$
4	$<\overline{5}>,<\overline{8}>$
6	$<\overline{4}>,<\overline{10}>$
12	$<\overline{2}>,<\overline{6}>,<\overline{7}>,<\overline{11}>$

Ejemplo 78 *Hacer la tabla de:*

a) $\square_{15} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{15})\}$ Como

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{15}) &= \{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\} \\ \square_{15} &= \{\overline{1},\overline{4}\} \end{aligned}$$

$\cdot$	$\overline{1}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$

b) $\square_{13} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{13})\}$

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{13}) &= \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12}\} \\ \square_{13} &= \{\overline{1},\overline{4},\overline{9},\overline{3},\overline{12},\overline{10}\} \end{aligned}$$

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{9}$	$\overline{10}$	$\overline{12}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{4}$	$\overline{9}$	$\overline{10}$	$\overline{12}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{12}$	$\overline{1}$	$\overline{4}$	$\overline{10}$
$\overline{4}$	$\overline{4}$	$\overline{12}$	$\overline{3}$	$\overline{10}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{1}$	$\overline{10}$	$\overline{3}$	$\overline{12}$	$\overline{4}$
$\overline{10}$	$\overline{10}$	$\overline{4}$	$\overline{1}$	$\overline{12}$	$\overline{9}$	$\overline{3}$
$\overline{12}$	$\overline{12}$	$\overline{10}$	$\overline{9}$	$\overline{4}$	$\overline{3}$	$\overline{1}$

Ejemplo 79 *Calcular los elementos, generadores y hacer la tabla de:*

a) $\square_{16} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{16})\}$

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{16}) &= \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\} \\ \square_{16} &= \{\overline{1}, \overline{9}\} \end{aligned}$$

$$< \overline{1} >= \{\overline{1}\} \qquad < \overline{9} >= \{\overline{9}, \overline{1}\}$$

El generador del grupo $\square_{16}$ es $\overline{9}$.

$\cdot$	$\overline{1}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{1}$

b) $\square_{26} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{26})\}$

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{26}) &= \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{21}, \overline{23}, \overline{25}\} \\ \square_{26} &= \{\overline{1}, \overline{9}, \overline{25}, \overline{23}, \overline{3}, \overline{17}\} \end{aligned}$$

$$\begin{aligned} < \overline{1} > &= \{\overline{1}\}; & < \overline{9} > &= \{\overline{9}, \overline{3}, \overline{1}\} \\ < \overline{25} > &= \{\overline{25}, \overline{1}\}; & < \overline{23} > &= \{\overline{23}, \overline{9}, \overline{25}, \overline{3}, \overline{17}, \overline{1}\} \\ < \overline{3} > &= \{\overline{3}, \overline{9}, \overline{1}\}; & < \overline{17} > &= \{\overline{17}, \overline{3}, \overline{25}, \overline{9}, \overline{23}, \overline{1}\} \end{aligned}$$

Generadores del grupo de los $\square_{26}$ son $\overline{17}, \overline{23}$.

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{9}$	$\overline{17}$	$\overline{23}$	$\overline{25}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{9}$	$\overline{17}$	$\overline{23}$	$\overline{25}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{25}$	$\overline{17}$	$\overline{23}$
$\overline{9}$	$\overline{9}$	$\overline{1}$	$\overline{3}$	$\overline{23}$	$\overline{25}$	$\overline{17}$
$\overline{17}$	$\overline{17}$	$\overline{25}$	$\overline{23}$	$\overline{3}$	$\overline{1}$	$\overline{9}$
$\overline{23}$	$\overline{23}$	$\overline{17}$	$\overline{25}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{25}$	$\overline{25}$	$\overline{23}$	$\overline{17}$	$\overline{9}$	$\overline{3}$	$\overline{1}$

Ejemplo 80 *Hacer la tabla y determinar raíces primitivas de* $\mathcal{U}(\mathbb{Z}_{18})$

Solución: $18 = 2 \cdot 3^2$, por lo tanto cumple el teorema 110, es decir $\mathcal{U}(\mathbb{Z}_{18})$ es un grupo cíclico.

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{18}) &= \{\overline{a} \in \mathbb{Z}_{18} \quad | \quad (\overline{a}, 18) = 1\}, \quad |\mathcal{U}(\mathbb{Z}_{18})| = \phi(18) \\ \mathcal{U}(\mathbb{Z}_{18}) &= \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\} \end{aligned}$$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{17}$	$\overline{1}$	$\overline{11}$	$\overline{13}$
$\overline{7}$	$\overline{7}$	$\overline{17}$	$\overline{13}$	$\overline{5}$	$\overline{1}$	$\overline{11}$
$\overline{11}$	$\overline{11}$	$\overline{1}$	$\overline{5}$	$\overline{13}$	$\overline{17}$	$\overline{7}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{1}$	$\overline{17}$	$\overline{7}$	$\overline{5}$
$\overline{17}$	$\overline{17}$	$\overline{13}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Como $\mathcal{U}(\mathbb{Z}_{18})$ es cíclico, las raíces primitivas es lo mismo que los generadores.

$$\begin{aligned}\phi(\phi(18)) &= \phi(6) \quad 6 = 2\cdot 3\\ \phi(\phi(18)) &= 2\cdot 3\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\\ \phi(\phi(18)) &= 2\cdot 3\cdot\frac{1}{2}\cdot\frac{2}{3}=2\end{aligned}$$

Por lo tanto $\mathcal{U}(\mathbb{Z}_{18})$ tiene dos raíces primitivas. Ahora buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{18})$.

$$\begin{aligned}<\overline{1}> &= \{\overline{1}\}\\ <\overline{5}> &= \{\overline{5},\overline{7},\overline{17},\overline{13},\overline{11},\overline{1}\}\end{aligned}$$

Luego, buscamos los primos relativos con $\phi(18)$ que son: $1, 5$
Por lo tanto las raíces primitivas de $\mathcal{U}(\mathbb{Z}_{18})$ son:

$$\overline{5}^1=\overline{5},\quad \overline{5}^5=\overline{11}$$

Ejemplo 81 *Sea $\mathcal{G}$ grupo cíclico. Demostrar que $\mathcal{G}$ es abeliano.*

Solución: $\mathcal{G}$ es cíclico existe $g\in\mathcal{G}$ tal que $\mathcal{G}=<g>$
Sean $a, b\in\mathcal{G}$ luego existe i, j tales que $a=g^i,\ b=g^j$

$$a\cdot b=g^i\cdot g^j=g^{i+j}=g^{j+i}=g^j\cdot g^i=b\cdot a$$

Por lo tanto $\mathcal{G}$ es un grupo abeliano.

Ejemplo 82 *Determinar todos los $\overline{x}\in\mathbb{Z}_5$ tal que $\overline{x}^3+\overline{2}\overline{x}^2+\overline{2}=\overline{0}$*

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

$$\begin{array}{rcccl}\overline{x} &=& \overline{0} &:& \overline{0}^3+\overline{2}\cdot\overline{0}^2+\overline{2} = \overline{2}\neq\overline{0}\\ \overline{x} &=& \overline{1} &:& \overline{1}^3+\overline{2}\cdot\overline{1}^2+\overline{2} = \overline{5}=\overline{0}\\ \overline{x} &=& \overline{2} &:& \overline{2}^3+\overline{2}\cdot\overline{2}^2+\overline{2} = \overline{18}=\overline{3}\neq\overline{0}\\ \overline{x} &=& \overline{3} &:& \overline{3}^3+\overline{2}\cdot\overline{3}^2+\overline{2} = \overline{47}=\overline{2}\neq\overline{0}\\ \overline{x} &=& \overline{4} &:& \overline{4}^3+\overline{2}\cdot\overline{4}^2+\overline{2} = \overline{98}=\overline{3}\neq\overline{0}\end{array}$$

Por lo tanto la única solución de en $\mathbb{Z}_5$ tal que $\overline{x}^3+\overline{2}\overline{x}^2+\overline{2}=\overline{0}$ es $\overline{x}=\overline{1}$

Ejemplo 83 *Calcular el orden de:*

a) $\overline{2}\in(\mathbb{Z}_{14},+)$, recordemos que $|\overline{x}|=\frac{n}{(n,x)}$

$$|\overline{2}| = \frac{14}{(14,2)}=7$$

ya que $(14,2)=2$. Por lo tanto el orden de $\overline{2}$ es 7.

b) $\overline{12} \in (\mathbb{Z}_{58}, +)$ recordemos que $|\overline{x}| = \frac{n}{(n,x)}$ Calculemos $(12, 58)$

$$\begin{aligned} 58 &= 12 \cdot 4 + 10 \\ 12 &= 10 \cdot 1 + 2 \\ 10 &= 2 \cdot 5 \end{aligned}$$

Luego $(12, 58) = 2$, de lo cual

$$|\overline{12}| = \frac{58}{(58, 2)} = \frac{58}{2} = 29$$

Por lo tanto el orden de $\overline{12}$ es 29.

Ejemplo 84 *Calcular el orden de:*

a) $\overline{12} \in (\mathcal{U}(\mathbb{Z}_{13}), \cdot)$

$$< \overline{12} > \;=\; \{\overline{12}, \overline{1}\}$$

Por lo tanto el orden de $\overline{12}$ es 2

b) $\overline{3} \in (\mathbb{Z}_{31}^*, \cdot)$

$$< \overline{3} > \;=\; \{\overline{3}, \overline{9}, \overline{27}, \overline{19}, \overline{26}, \overline{16}, \overline{17}, \overline{20}, \overline{29}, \overline{25}, \overline{13}, \overline{8}, \overline{24}, \overline{10}, \overline{-1}, \ldots\}$$

Note que $-1 \in < \overline{3} >$, luego en las próximas potencia estarán los inversos de todos los anteriores. Por lo tanto el orden de $\overline{3}$ es 30

Ejemplo 85 *Calcular los generadores de:* $(\mathbb{Z}_{18}, +)$

Solución: Como $18 = 2 \cdot 3^2$

$$\phi(18) \;=\; 2 \cdot 3^2 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2 \cdot 3^2 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6$$

Por lo tanto $(\mathbb{Z}_{18}, +)$ tiene 6 generadores, que van a hacer los primos relativos con 18.
Luego, los generadores de $(\mathbb{Z}_{18}, +)$ son: $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}$

Ejemplo 86 *Calcular el número de generadores de:* $(\mathbb{Z}_{500}, +)$

Solución: Como $500 = 2^2 \cdot 5^3$

$$\phi(500) \;=\; 2^3 \cdot 5^3 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 2^3 \cdot 5^3 \cdot \frac{1}{2} \cdot \frac{4}{5} = 200$$

Por lo tanto $(\mathbb{Z}_{500}, +)$ tiene 200 generadores.

Ejemplo 87 *Determinar los generadores de:*

a) $(\mathcal{U}(\mathbb{Z}_{19}),\cdot)$

Como el 19 es primo y el teorema 110 entonces $(\mathcal{U}(\mathbb{Z}_{19}),\cdot)$ es un grupo cíclico y el número de generadores esta determinado por la función de Euler aplicada al cardinal del grupo:

$$\phi(19) = 18 = 2\cdot 3^2$$

$$\phi(\phi(19)) = \phi(18) \;=\; 2\cdot 3^2\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right) = 2\cdot 3^2\cdot\frac{1}{2}\cdot\frac{2}{3} = 6$$

Por lo tanto $(\mathbb{Z}_{19}^*,\cdot)$ tiene 6 generadores. Buscamos el primer generador:

$$\begin{aligned} <\overline{1}> &= \{\overline{1}\}\\ <\overline{2}> &= \{\overline{2},\overline{4},\overline{8},\overline{16},\overline{13},\overline{7},\overline{14},\overline{9},\overline{18},\overline{17},\overline{15},\overline{11},\overline{3},\overline{6},\overline{12},\overline{5},\overline{10},\overline{1}\}\end{aligned}$$

Ahora necesitamos los primos relativos con 18 que son: $1,5,7,11,13,17$.

Por lo tanto los generadores de $(\mathcal{U}(\mathbb{Z}_{19}),\cdot)$ son:

$$\overline{2}^1=\overline{2},\quad \overline{2}^5=\overline{16},\quad \overline{2}^7=\overline{7},\quad \overline{2}^{11}=\overline{17},\quad \overline{2}^{13}=\overline{11},\quad \overline{2}^{17}=\overline{10}$$

b) $(\mathcal{U}(\mathbb{Z}_{24}),\cdot)$

Como 24 no cumple el teorema 110, luego no es cíclico, es decir no tiene generadores.

En forma directa podemos verificar que todos los elementos $\mathcal{U}(\mathbb{Z}_{24})$ tiene orden 2 o 1.

Ejemplo 88 *Determinar las raíces primitivas módulo* 31

Solución: 31 es primo luego $\mathcal{U}(\mathbb{Z}_{31})$ es cíclico.

$$\begin{aligned}\mathcal{U}(\mathbb{Z}_{31}) \;=\; \{&\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16},\overline{17},\overline{18},\overline{19},\overline{20},\overline{21},\overline{22},\overline{23},\overline{24},..\\ &\overline{25},\overline{26},\overline{27},\overline{28},\overline{29},\overline{30}\}\end{aligned}$$

$$\begin{aligned}\phi(\phi(31)) &= \phi(30);\quad 30 = 2\cdot 3\cdot 5\\ \phi(\phi(31)) &= 2\cdot 3\cdot 5\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\\ \phi(\phi(31)) &= 2\cdot 3\cdot 5\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 8\end{aligned}$$

Por lo tanto $\mathbb{Z}_{31}$ tiene 8 raíces primitivas. Buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{31})$.

$$\begin{aligned} <\overline{1}> &= \{\overline{1}\}\\ <\overline{2}> &= \{\overline{2},\overline{4},\overline{8},\overline{16},\overline{1}\}\\ <\overline{3}> &= \{\overline{3},\overline{9},\overline{27},\overline{19},\overline{26},\overline{16},\overline{17},\overline{20},\overline{29},\overline{25},\overline{13},\overline{8},\overline{24},\overline{10},\overline{30},\overline{28},\\ &\quad \overline{22},\overline{4},\overline{12},\overline{5},\overline{15},\overline{14},\overline{11},\overline{2},\overline{6},\overline{18},\overline{23},\overline{7},\overline{21},\overline{1}\}\end{aligned}$$

Luego, buscamos los primos relativos con $\phi(31)$ que son: $1,7,11,13,17,19,23,29$. Por lo tanto las raíces primitivas módulo 31 son:

$$\overline{3}^1=\overline{3},\quad \overline{3}^7=\overline{17},\quad \overline{3}^{11}=\overline{13},\quad \overline{3}^{13}=\overline{24},\quad \overline{3}^{17}=\overline{22},\quad \overline{3}^{19}=\overline{12},\quad \overline{3}^{23}=\overline{11},\quad \overline{3}^{29}=\overline{21}$$

Ejemplo 89 *Determinar el resto al dividir* $(100^{40}+8)^{78}$ *por* 19

Solución: $100 \equiv 5(\texttt{mod } 19)$ y $(5,19)=1$ por lo tanto $5^{\phi(19)} \equiv 5^{18} \equiv 1(\texttt{mod } 19)$, además $40 = 18\cdot 2+4$

$$5^{40}+8 \equiv 5^{18\cdot 2+4}+8 \equiv (5^{18})^2\cdot 5^4+8 \equiv 5^4+8 \equiv (25)^2+8 \equiv 36+8 \equiv 6(\texttt{mod } 19)$$

Además $(6,19)=1$, luego tenemos $6^{\phi(19)} \equiv 6^{18} \equiv 1(\texttt{mod } 19)$

$$6^{78} \equiv 6^{18\cdot 4+6} \equiv (6^{18})^4\cdot 6^6 \equiv 6^6 \equiv (36)^3 \equiv (17)^3 \equiv 11(\texttt{mod } 19)$$

Luego hemos demostrado que

$$(100^{40}+8)^{78} \equiv 6^{78} \equiv 11(\texttt{mod } 19)$$

Por lo tanto el resto al dividir $(100^{40}+8)^{78}$ por 19 es 11

Ejemplo 90 *Determinar el resto al dividir* $3^{251}+2^{501}+5^{61}$ *por* 7

Solución: Sabemos que $(2,7)=(3,7)=(5,7)=1$, además $\phi(7)=6$, luego tenemos

$$\begin{aligned} 3^{251} &\equiv 3^{6\cdot 41+5} \equiv 3^5 \equiv 5(\texttt{mod } 7)\\ 2^{501} &\equiv 2^{6\cdot 83+3} \equiv 2^3 \equiv 1(\texttt{mod } 7)\\ 5^{61} &\equiv 5^{6\cdot 10+1} \equiv 5^1 \equiv 5(\texttt{mod } 7)\end{aligned}$$

Ahora tenemos

$$3^{251}+2^{501}+5^{61} \equiv 5+1+5 \equiv 11 \equiv 4(\texttt{mod } 7)$$

Por lo tanto el resto al dividir $3^{251}+2^{501}+5^{61}$ por 7 es 4

Ejemplo 91 *Probar que si* n *y* 7 *son primos relativos entonces* $7|n^6-1$

Solución: Como $(n,7)=1$, luego tenemos que $n^{\phi(7)} \equiv 1(\texttt{mod } 7)$

$$\begin{aligned} n^6 &\equiv 1(\texttt{mod } 7)\\ n^6 &= 1+7\cdot q \quad q\in\mathbb{Z}\\ n^6-1 &= 7\cdot q\end{aligned}$$

Por lo tanto se tiene que $7|n^6-1$

Ejemplo 92 *Si* $(a,p)=1$. *Calcular* $\overline{1+a+a^2+\cdots+a^{p-1}}$ *en* $\mathbb{Z}_p$

Solución: Si $a=1 \quad \overline{1+a+a^2+\cdots+a^{p-1}} = \overline{1+1+\cdots+1} = \overline{p\cdot 1} = \overline{0}$

Si $a\neq 1$ podemos amplificar por $\left(\frac{1-a}{1-a}\right)$ la expresión

$$1+a+a^2+\cdots+a^{p-1} = 1 \ / \cdot \left(\frac{1-a}{1-a}\right)$$

de lo cual obtenemos

$$\frac{1-a^p}{1-a} = 1$$

Pero $(a,p)=1$ luego se tiene que $a^p \equiv a(\texttt{mod } p)$, por lo tanto

$$\overline{1+a+a^2+\cdots+a^{p-1}} = \frac{\overline{1-a}}{1-a} = \overline{1}$$

Ejemplo 93 *Resolver:*

a) $x^{20} + x^{13} + x^7 + x \equiv 0(\mathtt{mod}\ 7)$

Solución: Como 7 es un número primo tenemos que

$$x^{20} + x^{13} + x^7 + x \equiv 0(\mathtt{mod}\ 7) \Leftrightarrow x(x^{19} + x^{12} + x^6 + 1) \equiv 0(\mathtt{mod}\ 7)$$

Luego

$$x^{19} + x^{12} + x^6 + 1 \equiv 0(\mathtt{mod}\ 7) \quad \vee \quad x \equiv 0(\mathtt{mod}\ 7)$$

Sea x tal que $(x, 7) = 1$ entonces tenemos que $x^6 \equiv 1(\mathtt{mod}\ 7)$, de lo cual tenemos

$$x^{6q+r} \equiv x^r(\mathtt{mod}\ 7),$$

Reemplazando se tiene

$$\begin{aligned} x^{19} + x^{12} + x^6 + 1 &\equiv 0(\mathtt{mod}\ 7) \\ x + 1 + 1 + 1 &\equiv 0(\mathtt{mod}\ 7) \\ x &\equiv 4(\mathtt{mod}\ 7) \end{aligned}$$

Por lo tanto las soluciones de $x^{20} + x^{13} + x^7 + x \equiv 0(\mathtt{mod}\ 7)$ son

$$x \equiv 0(\mathtt{mod}\ 7), \quad x \equiv 4(\mathtt{mod}\ 7)$$

b) $x^{11} + x^8 + 5 \equiv 0(\mathtt{mod}\ 7)$

Solución: cero no es solución, luego

$$\begin{aligned} x^{11} + x^8 + 5 &\equiv 0(\mathtt{mod}\ 7) \\ x^5 + x^2 + 5 &\equiv 0(\mathtt{mod}\ 7) \end{aligned}$$

Evaluando tenemos

$$\begin{array}{rcrcll} x & = & 0 & : & 0^5 + 0^2 + 5 & = & 5 \not\equiv 0(\mathtt{mod}\ 7) \\ x & = & 1 & : & 1^5 + 1^2 + 5 & = & 7 \equiv 0(\mathtt{mod}\ 7) \\ x & = & 2 & : & 2^5 + 2^2 + 5 & = & 41 = 6 \not\equiv 0(\mathtt{mod}\ 7) \\ x & = & 3 & : & 3^5 + 3^2 + 5 & = & 257 = 5 \not\equiv 0(\mathtt{mod}\ 7) \\ x & = & 4 & : & 4^5 + 4^2 + 5 & = & 1045 = 2 \not\equiv 0(\mathtt{mod}\ 7) \\ x & = & 5 & : & 5^5 + 5^2 + 5 & = & 3155 = 5 \not\equiv 0(\mathtt{mod}\ 7) \\ x & = & 6 & : & 6^5 + 6^2 + 5 & = & 7817 = 5 \not\equiv 0(\mathtt{mod}\ 7) \end{array}$$

Por lo tanto la solución de $x^{11} + x^8 + 5 \equiv 0(\mathtt{mod}\ 7)$ es

$$x \equiv 1(\mathtt{mod}\ 7)$$

Ejemplo 94 *Resolver:*

$$\begin{array}{rcl} 5x & \equiv & 2(\mathtt{mod}\ 7) \\ 8x & \equiv & 4(\mathtt{mod}\ 9) \\ 2x & \equiv & 3(\mathtt{mod}\ 11) \end{array}$$

Solución: Son primos relativos, ya que $(9,11)=1, \quad (9,7)=1, \quad (11,7)=1$

$$\begin{array}{rcl} 5x & \equiv & 2(\mathtt{mod}\ 7)\ /\cdot 3 \\ 15x & \equiv & 6(\mathtt{mod}\ 7) \\ x & \equiv & 6(\mathtt{mod}\ 7) \end{array} \qquad \begin{array}{rcl} 8x & \equiv & 4(\mathtt{mod}\ 9) \\ -x & \equiv & 4(\mathtt{mod}\ 9)\ /\cdot -1 \\ x & \equiv & 5(\mathtt{mod}\ 9) \end{array} \qquad \begin{array}{rcl} 2x & \equiv & 3(\mathtt{mod}\ 11)\ /\cdot 6 \\ 12x & \equiv & 18(\mathtt{mod}\ 11) \\ x & \equiv & 7(\mathtt{mod}\ 11) \end{array}$$

Por lo tanto hay que resolver

$$\begin{array}{rcl} x & \equiv & 6(\mathtt{mod}\ 7) \\ x & \equiv & 5(\mathtt{mod}\ 9) \\ x & \equiv & 7(\mathtt{mod}\ 11) \end{array}$$

Para ello aplicamos el teorema chino de los resto

$$a_1=6, a_2=5, a_3=7, m_1=7, m_2=9, m_3=11, m=m_1\cdot m_2\cdot m_3=693$$

$$\begin{array}{rcl} \frac{m}{m_1}\cdot b_1 & \equiv & 1(\mathtt{mod}\ m_1) \\ 99\cdot b_1 & \equiv & 1(\mathtt{mod}\ 7) \\ b_1 & \equiv & 1(\mathtt{mod}\ 7) \end{array} \qquad \begin{array}{rcl} \frac{m}{m_2}\cdot b_2 & \equiv & 1(\mathtt{mod}\ m_2) \\ 77\cdot b_2 & \equiv & 1(\mathtt{mod}\ 9) \\ 5\cdot b_2 & \equiv & 1(\mathtt{mod}\ 9)\ /\cdot 2 \\ b_2 & \equiv & 2(\mathtt{mod}\ 9) \end{array} \qquad \begin{array}{rcl} \frac{m}{m_3}\cdot b_3 & \equiv & 1(\mathtt{mod}\ m_3) \\ 63\cdot b_3 & \equiv & 1(\mathtt{mod}\ 11) \\ 8b_3 & \equiv & 1(\mathtt{mod}\ 11)\ /\cdot 7 \\ b_3 & \equiv & 7(\mathtt{mod}\ 11) \end{array}$$

$$\begin{array}{rcl} x_0 & = & a_1\cdot b_1\cdot\dfrac{m}{m_1}+a_2\cdot b_2\cdot\dfrac{m}{m_2}+a_3\cdot b_3\cdot\dfrac{m}{m_3} \\ x_0 & = & 6\cdot 1\cdot 99+15\cdot 2\cdot 77+7\cdot 7\cdot 63 \\ x_0 & = & 4451 \\ x & \equiv & x_0(\mathtt{mod}\ m) \\ x & \equiv & 4451(\mathtt{mod}\ 252) \\ x & \equiv & 293(\mathtt{mod}\ 252) \end{array}$$

Ejemplo 95 *Sea p primo impar, $\overline{a}\in\mathbb{Z}_p$. Si el orden multiplicativo de $\overline{a}$ es 3.*
Demostrar $a^2+a+1\equiv 0(\mathtt{mod}\ p)$ y $\overline{a+1}$ tiene orden multiplicativo 6.

Solución: Como se tiene que $|\overline{a}|=3$, luego $\overline{a}^3=1$.

$$\begin{array}{rcl} a^3 & \equiv & 1(\mathtt{mod}\ p) \\ a^3-1 & \equiv & 0(\mathtt{mod}\ p) \\ (a-1)\cdot(a^2+a+1) & \equiv & 0(\mathtt{mod}\ p) \end{array}$$

Pero $a\not\equiv 1(\mathtt{mod}\ p)$, ya que $|\overline{a}|=3$. Luego

$$a^2+a+1\equiv 0(\mathtt{mod}\ p)$$

Calculemos el orden de $\overline{a+1}$.

$$\begin{aligned}(a+1)^2 &= a^2+2a+1 \equiv a(\mathtt{mod}\ p)\\ ((a+1)^2)^3 &\equiv a^3(\mathtt{mod}\ p)\\ (a+1)^6 &\equiv 1(\mathtt{mod}\ p)\end{aligned}$$

Nos falta verificar que no es otro divisor de 6. Para ello vemos que $(a+1)^2 \equiv a(\mathtt{mod}\ p)$, por lo tanto $(a+1)^2 \not\equiv 1(\mathtt{mod}\ p)$, además si multiplicamos por $a+1$ obtenemos que $(a+1)^3 \equiv a^2+a \equiv -1(\mathtt{mod}\ p)$, es decir, $(a+1)^3 \not\equiv 1(\mathtt{mod}\ p)$

Por lo tanto $|\overline{a+1}| = 6$.

Ejemplo 96 *Determine el número de soluciones de:*

a) $x^2 \equiv 2(\mathtt{mod}\ 31)$

Necesitamos saber si 2 es un cuadrado o no

$$\left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = 1$$

Por lo tanto $2 \in \square_{31}$ luego $x^2 \equiv 2(\mathtt{mod}\ 31)$ tiene dos soluciones.

b) $x^2 \equiv 3(\mathtt{mod}\ 31)$

$$\begin{aligned}\left(\frac{3}{31}\right)\cdot\left(\frac{31}{3}\right) &= (-1)^{\frac{31-1}{2}\cdot\frac{3-1}{2}};\quad 31 \equiv 1(\mathtt{mod}\ 3)\\ \left(\frac{3}{31}\right)\cdot\left(\frac{1}{3}\right) &= -1\end{aligned}$$

Como $\left(\frac{1}{3}\right) = 1$ implica que $\left(\frac{3}{31}\right) = -1$

Por lo tanto $3 \notin \square_{31}$, es decir $x^2 \equiv 3(\mathtt{mod}\ 31)$ tiene solución vacía.

c) $x^2 \equiv 429(\mathtt{mod}\ 563)$

429 se descompone como producto de primo en $3 \cdot 11 \cdot 13$

$$\left(\frac{429}{563}\right) = \left(\frac{3}{563}\right)\cdot\left(\frac{11}{563}\right)\cdot\left(\frac{13}{563}\right)$$

Veremos cada una por separado

$$\begin{aligned}\left(\frac{3}{563}\right)\cdot\left(\frac{563}{3}\right) &= (-1)^{\frac{563-1}{2}\cdot\frac{3-1}{2}};\quad 563 \equiv 2(\mathtt{mod}\ 3)\\ \left(\frac{3}{563}\right)\cdot\left(\frac{2}{3}\right) &= -1\end{aligned}$$

Pero $\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$, de donde se tiene que $\left(\frac{3}{563}\right) = 1$

$$\begin{aligned}\left(\frac{11}{563}\right)\cdot\left(\frac{563}{11}\right) &= (-1)^{\frac{563-1}{2}\cdot\frac{11-1}{2}}; \quad 563 \equiv 2(\texttt{mod } 11)\\ \left(\frac{11}{563}\right)\cdot\left(\frac{2}{11}\right) &= -1\end{aligned}$$

Pero $\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1$, luego tenemos $\left(\frac{11}{563}\right) = 1$

$$\begin{aligned}\left(\frac{13}{563}\right)\cdot\left(\frac{563}{13}\right) &= (-1)^{\frac{563-1}{2}\cdot\frac{13-1}{2}}; \quad 563 \equiv 4(\texttt{mod } 13)\\ \left(\frac{13}{563}\right)\cdot\left(\frac{4}{13}\right) &= 1\end{aligned}$$

Como $\left(\frac{4}{13}\right) = 1$ entonces $\left(\frac{13}{563}\right) = 1$

Reemplazando tenemos

$$\left(\frac{429}{563}\right) = \left(\frac{3}{563}\right)\cdot\left(\frac{11}{563}\right)\cdot\left(\frac{13}{563}\right) = 1\cdot 1\cdot 1 = 1$$

Por lo tanto $429 \in \square_{563}$, luego $x^2 \equiv 429(\texttt{mod } 563)$ tiene dos soluciones.

d) $2x^2 + 4x + 3 \equiv 0(\texttt{mod } 17)$

El Discriminante de la ecuación $ax^2 + bx + c \equiv 0(\texttt{mod } p)$ es $\Delta = b^2 - 4\cdot a\cdot c$

Luego tenemos que

$$\Delta = 4^2 - 4\cdot 3\cdot 2 = 16 - 24 = -8 = (-1)\cdot 2^3$$

Notemos que $2^3 \in \square_{17}$ si y sólo si $2 \in \square_{17}$

$$\left(\frac{-8}{17}\right) = \left(\frac{-1}{17}\right)\cdot\left(\frac{2^3}{17}\right) = (-1)^{\frac{17-1}{2}}\cdot(-1)^{\frac{17^2-1}{8}} = 1\cdot 1$$

Por lo tanto

$$\left(\frac{-8}{17}\right) = \left(\frac{-1}{17}\right)\cdot\left(\frac{2^3}{17}\right) = 1$$

de lo cual tenemos que $-8 \in \square_{17}$ y por lo tanto $2x^2 + 4x + 3 \equiv 0(\texttt{mod } 17)$ tiene dos soluciones.

Ejemplo 97 *Resolver las siguientes ecuaciones*

Solución: Sea $x \in \mathbb{Z}$, tales que

a) $x^2 \equiv 2(\mathtt{mod}\ 311)$

Veamos si 2 es un cuadrado o no.

$$\left(\frac{2}{311}\right) = (-1)^{\frac{311^2-1}{8}} = 1$$

Luego $2 \in \square_{311}$, por lo tanto $x^2 \equiv 2(\mathtt{mod}\ 311)$ tiene dos soluciones.

Veremos ahora cuales son, para ello notemos que $2 \equiv 4356 \equiv 66^2(\mathtt{mod}\ 311)$

$$\begin{aligned} x^2 &\equiv 2(\mathtt{mod}\ 311) \\ x^2 &\equiv 66^2(\mathtt{mod}\ 311) \\ x^2 - 66^2 &\equiv 0(\mathtt{mod}\ 311) \\ (x-66)\cdot(x+66) &\equiv 0(\mathtt{mod}\ 311) \end{aligned}$$

Como 311 es un número primo, entonces tenemos

$$\begin{aligned} x - 66 \equiv 0(\mathtt{mod}\ 311) &\quad \vee \quad x + 66 \equiv 0(\mathtt{mod}\ 311) \\ x \equiv 66(\mathtt{mod}\ 311) &\quad \vee \quad x \equiv -66(\mathtt{mod}\ 311) \\ x \equiv 66(\mathtt{mod}\ 311) &\quad \vee \quad x \equiv 245(\mathtt{mod}\ 311) \end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 2(\mathtt{mod}\ 311)$ son:

$$x \equiv 66(\mathtt{mod}\ 311), \quad x \equiv 245(\mathtt{mod}\ 311)$$

b) $x^2 \equiv 5(\mathtt{mod}\ 19)$

Veamos si 5 es un cuadrado o no

$$\left(\frac{5}{19}\right)\cdot\left(\frac{19}{5}\right) = (-1)^{\frac{19-1}{2}\cdot\frac{5-1}{2}} = 1$$

pero $19 \equiv 4 \equiv 2^2(\mathtt{mod}\ 5)$, de lo cual obtenemos

$$1 = \left(\frac{5}{19}\right)\cdot\left(\frac{19}{5}\right) = \left(\frac{5}{19}\right)\cdot\left(\frac{2^2}{5}\right) = \left(\frac{5}{19}\right)$$

Luego $5 \in \square_{19}$, por lo tanto $x^2 \equiv 5(\mathtt{mod}\ 19)$ tiene dos soluciones.

Veremos ahora cuales son, para ello notemos que $5 \equiv 81 \equiv 9^2(\mathtt{mod}\ 19)$

$$\begin{aligned} x^2 &\equiv 5(\mathtt{mod}\ 19) \\ x^2 &\equiv 9^2(\mathtt{mod}\ 19) \\ x^2 - 9^2 &\equiv 0(\mathtt{mod}\ 19) \\ (x-9)\cdot(x+9) &\equiv 0(\mathtt{mod}\ 19) \end{aligned}$$

Como 19 es un número primo, entonces tenemos

$$\begin{aligned} x - 9 \equiv 0(\mathtt{mod}\ 19) &\quad \vee \quad x + 9 \equiv 0(\mathtt{mod}\ 19) \\ x \equiv 9(\mathtt{mod}\ 19) &\quad \vee \quad x \equiv -9(\mathtt{mod}\ 19) \end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 5(\mathtt{mod}\ 19)$ son:

$$x \equiv 9(\mathtt{mod}\ 19), \quad x \equiv 10(\mathtt{mod}\ 19)$$

c) $3x^2 + 4x + 5 \equiv 0(\mathtt{mod}\ 31)$

Calculemos el discriminante

$$\Delta = 4^2 - 4 \cdot 3 \cdot 5 = 16 - 60 = -44 \equiv 18(\mathtt{mod}\ 31)$$

Veremos si es un cuadrado.

$$\left(\frac{18}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{3^2}{31}\right) = (-1)^{\frac{31^2-1}{8}} \cdot 1 = 1$$

Luego $18 = -44 \in \square_{31}$, por lo tanto $3x^2 + 4x + 5 \equiv 0(\mathtt{mod}\ 31)$ tiene dos soluciones.

Como p es impar, sabemos que,

$$ax^2 + bx + c = 0(\mathtt{mod}\ p) \Leftrightarrow (2ax + b)^2 = \Delta(\mathtt{mod}\ p)$$

Reemplazando obtenemos

$$\begin{aligned}
3x^2 + 4x + 5 &\equiv 0(\mathtt{mod}\ 31) \\
(6x + 4)^2 &\equiv \Delta(\mathtt{mod}\ 31) \\
z^2 &\equiv -44(\mathtt{mod}\ 31) \quad -44 \equiv 49(\mathtt{mod}\ 31) \\
z^2 &\equiv 49(\mathtt{mod}\ 31) \\
z^2 - 49 &\equiv 0(\mathtt{mod}\ 31) \\
z^2 - 7^2 &\equiv 0(\mathtt{mod}\ 31) \\
(z - 7) \cdot (z + 7) &\equiv 0(\mathtt{mod}\ 31)
\end{aligned}$$

Como 31 es un número primo entonces tenemos

$$\begin{aligned}
z \equiv 7(\mathtt{mod}\ 31) &\ \vee\ z \equiv -7(\mathtt{mod}\ 31) \\
6x + 4 \equiv 7(\mathtt{mod}\ 31) &\ \vee\ 6x + 4 \equiv -7(\mathtt{mod}\ 31) \\
6x \equiv 3(\mathtt{mod}\ 31)\ /26 &\ \vee\ 6x \equiv -11(\mathtt{mod}\ 31)\ /26 \\
x \equiv 78(\mathtt{mod}\ 31) &\ \vee\ x \equiv -286(\mathtt{mod}\ 31) \\
x \equiv 16(\mathtt{mod}\ 31) &\ \vee\ x \equiv 24(\mathtt{mod}\ 31)
\end{aligned}$$

Por lo tanto las soluciones de $3x^2 + 4x + 5 \equiv 0(\mathtt{mod}\ 31)$ son:

$$x \equiv 16(\mathtt{mod}\ 31), \quad x \equiv 24(\mathtt{mod}\ 31)$$

d) $x^{32} + 4x + 2 \equiv 0(\mathtt{mod}\ 31)$

Notemos que 0 no es solución, luego las soluciones deben cumplir con $x^{30} \equiv 1(\mathtt{mod}\ 31)$, por lo tanto

$$x^{32} + 4x + 2 \equiv x^2 + 4x + 2(\mathtt{mod}\ 31)$$

Veamos el discriminante

$$\Delta = 4^2 - 4 \cdot 1 \cdot 2 = 16 - 8 = 8 = 2^3$$

Notemos que $2^3 \in \square_{31}$ si y sólo si $2 \in \square_{31}$

$$\left(\frac{8}{31}\right) = \left(\frac{2}{31}\right) = (-1)^{\frac{31^2-1}{8}} = 1$$

Luego tenemos $2^3 \in \square_{31}$, por lo tanto $x^2 + 4x + 2 \equiv 0(\mathtt{mod}\ 31)$ tiene dos soluciones.
Sabemos que

$$ax^2 + bx + c = 0(\mathtt{mod}\ p) \Leftrightarrow (2ax + b)^2 = \Delta(\mathtt{mod}\ p)$$

$$\begin{aligned} x^2 + 4x + 2 &\equiv 0(\mathtt{mod}\ 31) \\ (2x+4)^2 &\equiv 8(\mathtt{mod}\ 31) \\ z^2 &\equiv 8(\mathtt{mod}\ 31) \quad 8 \equiv 225 \equiv 15^2(\mathtt{mod}\ 31) \\ z^2 &\equiv 15^2(\mathtt{mod}\ 31) \\ z^2 - 15^2 &\equiv 0(\mathtt{mod}\ 31) \\ (z-15)\cdot(z+15) &\equiv 0(\mathtt{mod}\ 31) \end{aligned}$$

Como 31 es un número primo entonces tenemos

$$\begin{aligned} z \equiv 15(\mathtt{mod}\ 31) &\quad \vee \quad z \equiv -15(\mathtt{mod}\ 31) \\ 2x + 4 \equiv 15(\mathtt{mod}\ 31) &\quad \vee \quad 2x + 4 \equiv -15(\mathtt{mod}\ 31) \\ 2x \equiv 11(\mathtt{mod}\ 31)\ /16 &\quad \vee \quad 2x \equiv -19(\mathtt{mod}\ 31)\ /16 \\ x \equiv 176(\mathtt{mod}\ 31) &\quad \vee \quad x \equiv -304(\mathtt{mod}\ 31) \\ x \equiv 21(\mathtt{mod}\ 31) &\quad \vee \quad x \equiv 6(\mathtt{mod}\ 31) \end{aligned}$$

Por lo tanto las soluciones de $x^{32} + 4x + 2 \equiv 0(\mathtt{mod}\ 31)$ son:

$$x \equiv 21(\mathtt{mod}\ 31), \quad x \equiv 6(\mathtt{mod}\ 31)$$

e) $x^4 \equiv 1(\mathtt{mod}\ 23)$

$$\begin{aligned} x^4 &\equiv 1(\mathtt{mod}\ 23) \\ x^4 - 1 &\equiv 0(\mathtt{mod}\ 23) \\ x^4 - 1^4 &\equiv 0(\mathtt{mod}\ 23) \\ (x^2 - 1^2)\cdot(x^2 + 1^2) &\equiv 0(\mathtt{mod}\ 23) \\ (x-1)\cdot(x+1)\cdot(x^2+1) &\equiv 0(\mathtt{mod}\ 23) \end{aligned}$$

Ya que 23 es un número primo entonces se tiene que

$$\begin{array}{lll} x - 1 \equiv 0(\mathtt{mod}\ 23) & x + 1 \equiv 0(\mathtt{mod}\ 23) & x^2 + 1 \equiv 0(\mathtt{mod}\ 23) \\ x \equiv 1(\mathtt{mod}\ 23) & x \equiv -1(\mathtt{mod}\ 23) & x^2 \equiv -1(\mathtt{mod}\ 23) \\ & x \equiv 22(\mathtt{mod}\ 23) & \end{array}$$

Determinemos si -1 es un cuadrado o no

$$\left(\frac{-1}{23}\right) = (-1)^{\frac{23-1}{2}} = -1$$

Luego $-1 \notin \square_{23}$, por lo tanto $x^2 + 1 \equiv 0(\texttt{mod}\ 23)$ no tiene solución.

De este modo tenemos que las soluciones de $x^4 \equiv 1(\texttt{mod}\ 23)$ son:

$$x \equiv 1(\texttt{mod}\ 23), \quad x \equiv 22(\texttt{mod}\ 23)$$

f) Resolver $x^4 + x^2 + 1 \equiv 0(\texttt{mod}\ 11)$

Consideremos el cambio de variable $u = x^2$ luego la tenemos

$$x^4 + x^2 + 1 \equiv 0(\texttt{mod}\ 11) \Leftrightarrow u^2 + u + 1 \equiv 0(\texttt{mod}\ 11)$$

El discriminante

$$\Delta = 1^2 - 4 = -3 \equiv 8(\texttt{mod}\ 11)$$

Notemos que $2^3 \in \square_{11}$ si y sólo si $2 \in \square_{11}$

$$\left(\frac{8}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1$$

Por lo tanto $x^4 + x^2 + 1 \equiv 0(\texttt{mod}\ 11)$ no tiene solución.

Ejemplo 98 *Determinar todos los números primos impares p tal que $p \leq 30$ y $\left(\frac{3}{p}\right) = -1$*

Solución: Por reciprocidad cuadrática tenemos

$$\left(\frac{3}{p}\right) \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

Luego

$$\left(\frac{p}{3}\right) = (-1)^{\frac{p+1}{2}}$$

i) $p \equiv 1(\texttt{mod}\ 3)$

$$1 = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = (-1)^{\frac{p+1}{2}}$$

Luego $\frac{p+1}{2}$ es par, es decir, $\frac{p+1}{2} = 2 \cdot t \quad t \in \mathbb{Z}$, por ende tenemos que $p = 4 \cdot t - 1$.

Pero $p \equiv 1(\texttt{mod}\ 3)$, luego reemplazando obtenemos $4t - 1 \equiv 1(\texttt{mod}\ 3)$, al simplificar se tiene $t \equiv 2(\texttt{mod}\ 3)$, de este modo $p = 4(3s + 2) - 1 = 12s + 7$

Por lo tanto $p \in \{7, 19\}$

ii) $p \equiv 2(\texttt{mod}\ 3)$

$$-1 = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{p+1}{2}}$$

Luego $\frac{p+1}{2}$ es impar, es decir, $\frac{p+1}{2} = 2 \cdot t + 1 \quad t \in \mathbb{Z}$, así $p = 4 \cdot t + 1$.

Pero $p \equiv 2(\texttt{mod}\ 3)$, luego $4t+1 \equiv 2(\texttt{mod}\ 3)$, es decir, $t \equiv 1(\texttt{mod}\ 3)$, de lo cual obtenemos $p = 4(3s+1)+1 = 12s+5$

Por lo tanto $p \in \{5, 17, 29\}$

Por lo tanto todos los p primos tal que $\left(\frac{3}{p}\right) = -1$ y $p \leq 30$ son $\{5, 7, 17, 19, 29\}$

Ejemplo 99 *Determinar todos los $\alpha \in \mathbb{Z}_{11}$ tal que*

$$\begin{array}{|rcl} x - y & = & \alpha \\ x \cdot y & = & 1 \end{array}$$

el sistema en $\mathbb{Z}_{11}$ no tenga solución.

Solución: Despejando de la primera ecuación tenemos $y = x - \alpha$ y reemplazar tenemos

$$\begin{aligned} x \cdot (x - \alpha) &= 1 \\ x^2 - \alpha x &= 1 \\ x^2 - \alpha \cdot x - 1 &= 0 \end{aligned}$$

El discriminante es $\Delta = \alpha^2 + 4$, para que el sistema no tenga solución, es decir,

$$\Delta = \not\in \square_{11} = \{\overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}\}$$

$$\begin{array}{rcl:rcl} \alpha & = & 0 & 0^2 + 4 & = & 4 \in \square_{11} \\ \alpha & = & 1 & 1^2 + 4 & = & 5 \in \square_{11} \\ \alpha & = & 2 & 2^2 + 4 & = & 8 \not\in \square_{11} \\ \alpha & = & 3 & 3^2 + 4 & = & 13 = 2 \not\in \square_{11} \\ \alpha & = & 4 & 4^2 + 4 & = & 20 = 9 \in \square_{11} \\ \alpha & = & 5 & 5^2 + 4 & = & 29 = 7 \not\in \square_{11} \\ \alpha & = & 6 & 6^2 + 4 & = & 40 = 7 \not\in \square_{11} \\ \alpha & = & 7 & 7^2 + 4 & = & 53 = 9 \in \square_{11} \\ \alpha & = & 8 & 8^2 + 4 & = & 68 = 2 \not\in \square_{11} \\ \alpha & = & 9 & 9^2 + 4 & = & 85 = 8 \not\in \square_{11} \\ \alpha & = & 10 & 10^2 + 4 & = & 104 = 5 \in \square_{11} \end{array}$$

Por lo tanto $\alpha \in \{\overline{2}, \overline{3}, \overline{5}, \overline{6}, \overline{8}, \overline{9}\}$

Ejemplo 100 *Determinar condiciones sobre el primo p tal que $x^4 \equiv 16(\texttt{mod}\ p)$*

a) Tenga dos soluciones.

b) Tenga cuatro soluciones.

Solución: Busquemos los Factores de la expresión

$$\begin{aligned} x^4 &\equiv 16(\mathtt{mod}\ p) \\ x^4-16 &\equiv 0(\mathtt{mod}\ p) \\ x^4-4^2 &\equiv 0(\mathtt{mod}\ p) \\ (x^2-4)\cdot(x^2+4) &\equiv 0(\mathtt{mod}\ p) \\ (x-2)\cdot(x+2)\cdot(x^2+4) &\equiv 0(\mathtt{mod}\ p) \end{aligned}$$

Como p es primo tenemos

$$x \equiv 2(\mathtt{mod}\ p) \ \vee \ x \equiv -2(\mathtt{mod}\ p) \ \vee \ x^2 \equiv -4(\mathtt{mod}\ p)$$

a) Tenga dos soluciones.

El primo debe ser impar y $-4 \notin \square_p$ de lo cual $\left(\frac{-4}{p}\right) = -1$

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{4}{p}\right) = (-1)^{\frac{p-1}{2}}\cdot 1 = (-1)^{\frac{p-1}{2}} = -1$$

Luego $\frac{p-1}{2}$ es impar, es decir, $\frac{p-1}{2} = 2\cdot t+1 \quad t \in \mathbb{Z}$, de lo cual tenemos $p = 4\cdot t+3$.

La ecuación tiene dos soluciones si y sólo si $p \equiv 3(\mathtt{mod}\ 4)$

b) Tenga cuatro soluciones.

El primo debe ser impar y $-4 \in \square_p$, es decir, $\left(\frac{-4}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$

Luego $\frac{p-1}{2}$ es par, es decir, $\frac{p-1}{2} = 2\cdot t \quad t \in \mathbb{Z}$, de lo cual tenemos $p = 4\cdot t+1$.

La ecuación tiene dos soluciones si y sólo si $p \equiv 1(\mathtt{mod}\ 4)$

Ejemplo 101 *Determine número de solución de*

$$\begin{array}{|rcl} x^2+y^2 &\equiv& 1(\mathtt{mod}\ 43) \\ x-y &\equiv& 2(\mathtt{mod}\ 43) \end{array}$$

Solución: Despejando de la segunda ecuación $x \equiv 2+y(\mathtt{mod}\ 43)$ y reemplazando en la primera obtenemos

$$\begin{aligned} (2+y)^2+y^2 &\equiv 1(\mathtt{mod}\ 43) \\ 4+4y+y^2+y^2-1 &\equiv 0(\mathtt{mod}\ 43) \\ 2y^2+4y+3 &\equiv 0(\mathtt{mod}\ 43) \end{aligned}$$

El discriminante

$$\Delta = 4^2-4\cdot 2\cdot 3 = 16-24 = -8 = -1\cdot 2^3$$

$$\left(\frac{-8}{43}\right) = \left(\frac{-1}{43}\right)\cdot\left(\frac{2^3}{43}\right) = (-1)^{\frac{43-1}{2}}\cdot\left(\frac{2}{43}\right) = (-1)\cdot(-1)^{\frac{43^2-1}{8}}(-1)\cdot(-1) = 1$$

Por lo tanto

$$\begin{array}{|rcl} x^2+y^2 & \equiv & 1(\texttt{mod } 43) \\ x-y & \equiv & 2(\texttt{mod } 43) \end{array}$$

tiene dos soluciones.

Ejemplo 102 *Sea p un primo impar. Demostrar que si $\delta \in \not\square_p$ entonces*

$$\not\square_p = \delta\square_p$$

Demostración: Recuerde que ambos conjunto tiene igual cardinal, luego basta demostrar una contención

Supongamos que $\overline{x}^2\cdot\delta$ es un cuadrado, luego

$$\begin{array}{rcl} \delta\cdot\overline{x}^2 & = & \overline{a}^2 \quad / \cdot \overline{x}^{-2} \\ \delta & = & \overline{a}^2\cdot\overline{x}^{-2} \\ \delta & = & (\overline{a}\cdot\overline{x}^{-1})^2 \end{array}$$

De lo cual tenemos que $\delta \in \square_p$, lo que es una contradicción

Por lo tanto

$$\not\square_p = \{\overline{x}^2\cdot\delta \quad | \quad \overline{x}\in\mathbb{Z}_p^*\}$$

Ejemplo 103 *Determine número de solución de $x^6+x^3-2\equiv 0(\texttt{mod } 37)$*

Solución: Realizando el cambio de variable $u=x^3$, obtenemos que

$$x^6+x^3-2\equiv 0(\texttt{mod } 37) \Leftrightarrow u^2+u-2\equiv 0(\texttt{mod } 37)$$

Pero $u^2+u-2=(u-1)\cdot(u+2)$. Luego

$$\begin{array}{rcl} x^6+x^3-2 & \equiv & 0(\texttt{mod } 37) \\ (x^3-1)\cdot(x^3+2) & \equiv & 0(\texttt{mod } 37) \\ (x-1)\cdot(x^2+x+1)\cdot(x^3-2) & \equiv & 0(\texttt{mod } 37) \end{array}$$

Como 37 es primo veamos primero la ecuación de segundo grado $x^2+x+1\equiv 0(\texttt{mod } 37)$, para ello $\Delta = 1-4=-3=-1\cdot 3$

$$\left(\frac{-3}{37}\right) = \left(\frac{-1}{37}\right)\cdot\left(\frac{3}{37}\right) = (-1)^{\frac{37-1}{2}}\cdot\left(\frac{3}{37}\right) = -\left(\frac{3}{37}\right)$$

Aplicando reciprocidad cuadrática tenemos

$$\left(\frac{-3}{37}\right) = -\left(\frac{3}{37}\right) = (-1)(-1)^{\frac{37-1}{2}\cdot\frac{3-1}{2}}\left(\frac{37}{3}\right) = (-1)(-1)\left(\frac{1}{3}\right) = 1$$

Por lo tanto $-3\in\square_{37}$ luego la ecuación tiene soluciones distinta de 1.

Ya que 2 no es un cubo, por lo cual $x^3-2\equiv 0(\texttt{mod } 37)$ no tiene solución.

De este modo obtenemos que el número de soluciones de $x^6+x^3-2\equiv 0(\texttt{mod } 37)$ es 3.

Ejemplo 104 *Determinar todos los $\alpha \in \mathbb{Z}_{13}$, para los cuales la ecuación $x^2+2x+\alpha-1=0$ no tiene solución en $\mathbb{Z}_{13}$*

Solución: Calculando el discriminante $\Delta = 4-4(\alpha-1) = 4-4\alpha+4 = 8-4\alpha$, luego la ecuación no tiene solución si y sólo si $8-4\alpha \notin \square_{13} = \{\overline{1}, \overline{4}, \overline{9}, \overline{3}, \overline{12}, \overline{10}\}$

Evaluando todo los α posible obtenemos:

$$\begin{array}{rcrcll}
\alpha & = & 0 & : & 8-4\cdot 0 & = & 8 \notin \square_{13} \\
\alpha & = & 1 & : & 8-4\cdot 1 & = & 4 \in \square_{13} \\
\alpha & = & 2 & : & 8-4\cdot 2 & = & 0 \notin \square_{13} \\
\alpha & = & 3 & : & 8-4\cdot 3 & = & -4 = 9 \in \square_{13} \\
\alpha & = & 4 & : & 8-4\cdot 4 & = & -8 = 5 \notin \square_{13} \\
\alpha & = & 5 & : & 8-4\cdot 5 & = & -12 = 1 \in \square_{13} \\
\alpha & = & 6 & : & 8-4\cdot 6 & = & -16 = 10 \in \square_{13} \\
\alpha & = & 7 & : & 8-4\cdot 7 & = & -20 = 6 \notin \square_{13} \\
\alpha & = & 8 & : & 8-4\cdot 8 & = & -24 = 2 \notin \square_{13} \\
\alpha & = & 9 & : & 8-4\cdot 9 & = & -28 = 11 \notin \square_{13} \\
\alpha & = & 10 & : & 8-4\cdot 10 & = & -32 = 7 \notin \square_{13} \\
\alpha & = & 11 & : & 8-4\cdot 11 & = & -36 = 3 \in \square_{13} \\
\alpha & = & 12 & : & 8-4\cdot 12 & = & -40 = 12 \in \square_{13}
\end{array}$$

Por lo tanto $\alpha \in \{\overline{0}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$

Ejemplo 105 *Determinar generadores y subgrupos de: $\mathcal{C}_{19}$*

$\mathcal{C}_{19} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{19})\}$

$$\begin{array}{rcl}
\mathcal{C}_{19} & = & \{\overline{1}, \overline{8}, \overline{7}, \overline{11}, \overline{18}, \overline{12}\} \\
< \overline{1} > & = & \{\overline{1}\} \\
< \overline{8} > & = & \{\overline{8}, \overline{7}, \overline{18}, \overline{11}, \overline{12}, \overline{1}\} \\
< \overline{7} > & = & \{\overline{7}, \overline{11}, \overline{1}\} \\
< \overline{11} > & = & \{\overline{11}, \overline{7}, \overline{1}\} \\
< \overline{18} > & = & \{\overline{18}, \overline{1}\} \\
< \overline{12} > & = & \{\overline{12}, \overline{11}, \overline{18}, \overline{7}, \overline{8}, \overline{1}\}
\end{array}$$

Por lo tanto los generadores de $\mathcal{C}_{19}$ son $\overline{8}, \overline{12}$

orden	subgrupo
1	$< \overline{1} >$
2	$< \overline{18} >$
3	$< \overline{7} >, < \overline{11} >$
6	$< \overline{8} >, < \overline{12} >$