Aritmética

Daniel Jiménez

Tercera Versión
2013

Índice general

Introducción

La primera versión del presente apunte, corresponde a un trabajo de recopilación realizado por los alumnos Victor Bravo, Ada Ramos y Ambar Toledo de la Carrera de Matemáticas de nuestra Universidad, durante el año 2008. Toda esta selección de material, se obtuvo de diferentes años en que dictó la asignatura de Aritmética el profesor Jorge León, quien nos permitió usar los apuntes de sus alumnos para dar forma a este proyecto, del mismo modo, los apuntes de la ayudante de la asignatura señorita Ada Ramos.

Capítulo 1

Números Naturales

1.1. Nociones de Estructura Algebraica

1.1.1. Grupos

Definición 1 *Se dice que $(G, *)$ es un **grupo**, si y sólo si, G es un conjunto no vacío, provisto de una función*

$$\begin{array}{rccc} * & : & G \times G & \longrightarrow & G \\ & & (a, b) & \longmapsto & a * b, \end{array}$$

también llamada operación binaria $*$ y que cumple con

Asociatividad

Para todo a, b, c en G, se cumple

$$a * (b * c) = (a * b) * c.$$

Existencia del elemento neutro

Existe e elemento neutro de G, tal que para todo a en G, se cumple

$$a * e = a = e * a.$$

Existencia del elemento inverso

Para todo a en G, existe b en G, tal que

$$a * b = e = b * a,$$

en tal caso el elemento b se denota por a^{-1}, llamado el inverso de a. Es fácil demostrar que el inverso es único, cuando existe.

Diremos que $(G, *)$ es un grupo, para indicar que G bajo la operación $*$ es un grupo.

Algunos grupos cumplen una propiedad adicional dada por:

Conmutatividad

Para todo $a, b \in G$ se cumple

$$a * b = b * a$$

En tal caso, se dice que G es un grupo abeliano o conmutativo

Definición 2 *Sea H un subconjunto no vacío de un grupo G.*

Se dice que H es un ***subgrupo*** *de G, si y sólo si H es un grupo con la misma operación de G. En tal caso se denota por $H \leq G$.*

Propiedad 1 *Sea H un subconjunto no vacío de un grupo $(G, *)$.*

H es un subgrupo de G, si y sólo si cumple:

1. *Para todo $x, y \in H$, se tiene que $x * y \in H$.*
2. *Para todo $x \in H$, se tiene que $x^{-1} \in H$.*

Ejemplo 1 *Algunos ejemplo de grupos*

1. *$G = \{e\}$ es el grupo trivial, $e * e = e$*
2. *$G = \{e, a\}$, es un grupo con la operación*

$*$	e	a
e	e	a
a	a	e

3. *$G = \{e, a, b\}$, es un grupo con la operación y $b = a^2$*

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. *$G = \{e, a, b, c\}$, es un grupo, llamado grupo de Klein con la operación*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5. *$G = \{e, a, b, c\}$, es un grupo, con la operación*

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Ejemplo 2 *Algunos ejemplos de grupos no conmutativo, se obtiene al considerar los movimientos rígidos de los n-agonos regulares, con la operación de realizar consecutivamente la respectiva simetrías respectivamente de otra manera la composición.*

1. *Los movimiento rígido del triángulo equilátero son seis, las rotaciones en 120,240 y 360 grados, y las reflexiones o simetría respecto a las bisectriz del triángulo*

$$Sim(T) = \{r_0, r_{120}, r_{240}, s_1, s_2, s_3\}$$

Construir la tabla del grupo $Sim(T)$

2. *Los movimiento rígido del cuadrado son ocho, las rotaciones en 90,180,270,360 y las reflexiones o simetría respecto a las diagonales y a la recta que une los puntos medio de los lados paralelos.*

1.1.2. Anillo y Cuerpo

Definición 3 *Se dice que $(A, +, \cdot)$ es un anillo, si y sólo si, A es un conjunto no vacío, provisto de dos operaciones $+$ y $\cdot$, tales que:*

1. *$(A, +)$ es un grupo abeliano.*

2. ***Asociatividad***

   Para todo $x, y, z \in A$ se tiene que

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

3. ***Neutro***

   Existe $1 \in A - \{0\}$, tal que para todo $x \in A$ se cumple

$$x \cdot 1 = 1 \cdot x = x.$$

4. ***Distributiva***

   Para todo $x, y, z \in A$ se tiene que

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Además se dice que A es una anillo conmutativo si la operación " $\cdot$ " lo es.

Notación: Habitualmente el neutro con la primera operación se denota con el símbolo 0 y el neutro de la segunda operación con el símbolo 1. Además el inverso aditivo por $-a$ y el multiplicativo cuando existe por a^{-1}.

Ejemplo 3 *El conjunto de las matrices*

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

es un anillo no conmutativo, con las siguientes operaciones
Suma:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

Producto:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

Además note que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Observación: no todas la matrices tiene inverso multiplicativo o con el producto.

Sea $A \in M_2(\mathbb{R})$, se dice que A es invertible si y sólo si existe $B \in M_2(\mathbb{R})$ tal que

$$AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Ejercicio 4 *En* $(M_2(\mathbb{R}), +, \cdot)$

1. *Demostrar que* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *es invertible si y sólo si* $ad - bc \neq 0$
2. *Si* $B = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix}$. *Determine* B^{-1}
3. *Si* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 0 \\ 1 & 4 \end{pmatrix}$. *Determine* $X \in M_2(\mathbb{R})$, *tal que*

$$A \cdot X \cdot B = I$$

Definición 4 *Sea* $(A, +, \cdot)$ *un anillo.*

Se define el conjunto de los elementos invertibles

$$\mathcal{U}(A) = \{x \in A \mid \text{ existe el inverso multiplicativo de } x \}$$

Ejercicio 5 *Sea* $(A, +, \cdot)$ *un anillo.*

Demuestre que

1. $(\forall a \in A)(a \cdot 0 = 0)$
2. $(-1)(-1) = 1$
3. $(\forall a, b \in A)(\ (-a)b = -(ab)\ )$

Definición 5 *Se dice que un anillo* $(K, +, \cdot)$ *es un* ***cuerpo*** *si y sólo si* $(K^*, \cdot)$ *es un grupo abeliano, donde* $K^* = K - \{0\}$.

Es decir $(K, +, \cdot)$ *es un cuerpo si y solo si,* $(K, +, \cdot)$ *es un anillo conmutativo, tal que* $\mathcal{U}(A) = K^*$

1.2. Números Naturales $\mathbb{N}$

La más conocida presentación de los números naturales, es la que presentó el matemático italiano Giuseppe Peano (1858-1932) por primera vez en 1889 en un pequeño libro publicado en Turin, titulado "Arithmetices Principia Nova Methodo Exposita"Traducido al inglés: Van Heijenoort. The Principles of Arithmetic, presented by a new method. Este texto incluye sus famosos axiomas, pero más que un texto de aritmética, este documento contiene una introducción a la lógica en la cual se presentan por primera vez los símbolos actuales para representar la pertenencia, la existencia, la unión y la intersección, algunas otras presentaciones son:

On the Logic of Number, de **Charles S. Pierce**, fue publicado en 1881 en las páginas 85 a 95 del volumen 4 de la revista The American Journal of Mathematics.

An Elementary Theory of the Category of Sets.**Lawvere, F. William.** Proc. Nat. Acad. Sci. 52 (1964): 1506-1511.

Ahora veremos la construcción de los números naturales a través de los llamados axiomas de **Peano**. Estos son:

Axioma 1 *Existe un conjunto denotado por* $\mathbb{N}$*, cuyos elementos se llaman* ***números naturales*** *y existe número natural llamado "cero" e indicado por el símbolo* 0*.*

$$0 \in \mathbb{N}.$$

Axioma 2 *Existe una relación simbolizada por "suc", tal que se escriba* $suc(x)$ *debe leerse sucesor de* x*.*

$$(\forall x \in \mathbb{N})(\exists! y \in \mathbb{N})(y = suc(x)).$$

Axioma 3

$$(\forall x \in \mathbb{N})(suc(x) \neq 0).$$

Axioma 4

$$(\forall x, y \in \mathbb{N})(suc(x) = suc(y) \Rightarrow x = y).$$

Axioma 5 *Si $I \subseteq \mathbb{N}$ y se verifican:*

1. $0 \in I$.
2. $(\forall x \in I)(suc(x) \in I)$.

Entonces $I = \mathbb{N}$.

Teorema 2 *Ningún número natural es sucesor de si mismo, es decir,*

$$(\forall x \in \mathbb{N})(suc(x) \neq x).$$

Demostración: Definamos el conjunto $M = \{x \in \mathbb{N} \mid suc(x) \neq x\}$, y demostraremos que $M = \mathbb{N}$.

Para lo anterior usaremos el Axioma (5), lo que significa que demos verificar cada una las hipótesis:

En primer lugar es claro que $M \subseteq \mathbb{N}$.

La segunda condición se obtiene del Axiomas (1), ya que $0 \in \mathbb{N}$ y cumple con $suc(0) \neq 0$, luego $0 \in M$.

Por último, consideremos $x \in M$, luego se tiene que

$$x \in \mathbb{N} \text{ y } suc(x) \neq x.$$

Por el Axioma (4), se obtiene tenemos que $suc(suc(x)) \neq suc(x)$, luego $suc(x) \in M$.

Por lo tanto M cumples las todas las hipótesis del Axioma (5), de lo cual se obtiene $M = \mathbb{N}$. □

Teorema 3 *Todo número natural no nulo es sucesor de uno y sólo un número natural, es decir,*

$$(\forall x \in \mathbb{N} - \{0\})(\exists! y \in \mathbb{N})(x = suc(y)).$$

Demostración: Definamos el conjunto

$$M = \{x \in \mathbb{N} - \{0\} \quad | \quad (\exists! y \in \mathbb{N})(x = suc(y))\} \cup \{0\}$$

y demostremos que $M = \mathbb{N}$ usando el Axioma (5).

Notemos primero que: $M \subseteq \mathbb{N}$ y $0 \in M$ por definición del conjunto M.

Para la segunda parte, sea $x \in M$, luego se tiene que

$$x \in \mathbb{N} \text{ y existe } y \in \mathbb{N} \text{ tal que } suc(y) = x.$$

por el Axioma (2) se tiene que $suc(x) \in \mathbb{N}$ y por el Axioma (3) se tiene que $suc(x) \neq 0$, como se tiene que $x = suc(y)$, luego $suc(x) = suc(suc(y))$.

Para la unicidad, el Axioma 4, no puede haber dos antecesores, luego $suc(y) = x$, es el único elemento en los naturales tal que

$$suc(x) = suc(suc(y)).$$

es decir, dado $x \in M$, existe un único $z \in \mathbb{N}$ tal que $suc(x) = suc(z)$

Por lo tanto, $M = \mathbb{N}$, concluyendo así la demostración. □

1.2.1. Suma en $\mathbb{N}$

En el conjunto de los números Naturales se puede definir una operación binaria, dada por el teorema .

Propiedad 4 *Sea $x \in \mathbb{N}$ fijo, se define la siguiente relación por recurrencia*

$$x + 0 \;:=\; x$$

Si $x + y$ esta definido, entonces

$$x + suc(y) \;:=\; suc(x + y).$$

entonces la anterior relación define la función

$$\begin{array}{rccc} + \;:\; & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & y & \longmapsto & x + y, \end{array}$$

Demostración: Sea $x \in \mathbb{N}$ fijo, definimos el conjunto

$$J = \{y \in \mathbb{N} \;\mid x + y \;\text{ esta bien definido }\}$$

Claramente $0 \in \mathbb{N}$, no tiene un antecesor y además se tiene $x + 0 = x$. Luego $0 \in J$.

Supongamos que $y \in J$, luego $x + y \in \mathbb{N}$ y esta bien definido, por lo tanto, tenemos que $suc(x + y) \in \mathbb{N}$ es único, es decir $x + suc(y)$ esta bien definido, por ende $suc(y) \in J$, luego por Axioma (5), tenemos que $J = \mathbb{N}$.

De este modo, $+$ es una función con x esta fijo. □

Observación: Notemos que el lema anterior nos permite definir, para cualquier par de números naturales la suma de ellos

Teorema 5 *En el conjunto de los números naturales, existe una operación suma $(+)$ que cumple:*

1. $(\forall x \in \mathbb{N})(\, x + 0 = x\,)$.
2. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\, x + suc(y) = suc(x + y)\,)$.

Notación: Denotemos $suc(0) = 1$ y reemplazando $y = 0$ en Teorema 5.2, obtenemos

$$suc(x) \;=\; x + 1. \tag{1.1}$$

Ahora bien, a partir de (1.1) tomando $x = 1$, obtenemos $suc(1) = 1+1$, lo que anotaremos como $suc(1) = 2$ siguiendo del mismo modo

$$\begin{array}{rcl} suc(0) & = & 1 \\ suc(1) & = & 2 \\ suc(2) & = & 3 \\ & \vdots & \\ suc(n) & = & n + 1. \end{array}$$

La siguiente propiedad completa la demostración del neutro

Propiedad 6

$$(\forall y \in \mathbb{N})(0 + y = y). \tag{1.2}$$

Demostración: Se define el conjunto

$$J = \{y \in \mathbb{N} \mid 0 + y = y\}$$

y demostremos que $J = \mathbb{N}$.

Para la primera parte, tenemos que $0 \in \mathbb{N}$ y por la propiedad 4 tenemos que $0 + 0 = 0$, de este modo concluimos que $0 \in J$.

Supongamos $y \in J$, es decir, $y \in \mathbb{N}$ y $0 + y = y$, ahora bien como $y \in \mathbb{N}$ por Axioma (2), se tiene que $suc(y) \in \mathbb{N}$, por la Propiedad 4, se tiene que

$$0 + suc(y) = suc(0 + y) = suc(y),$$

es decir $suc(y) \in J$.

Luego en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Teorema 7 (Conmutatividad) *La suma en* $\mathbb{N}$ *es conmutativa, esto es*

$$(\forall x, y \in \mathbb{N})(x + y = y + x).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})(x + y = y + x)\}$$

y demostremos que $M = \mathbb{N}$.

Por definición de suma y la Propiedad (6), tenemos se cumple

$$(\forall y \in \mathbb{N})(0 + y = y = y + 0),$$

así $0 \in M$.

Ahora veremos la segunda parte del axioma 5, es decir,

$$(\forall x \in M)(suc(x) \in M)$$

Supongamos $x \in M$, es decir, $x \in \mathbb{N}$ y para todo $y \in \mathbb{N}$ se tiene $x + y = y + x$.

Como $x \in \mathbb{N}$ por Axioma (2)tenemos que $suc(x) \in \mathbb{N}$, para ello debemos demostrar que $suc(x) \in M$, es decir

$$(\forall y \in \mathbb{N})(suc(x) + y = y + suc(x)).$$

Para demostrar lo anterior definimos el conjunto

$$I = \{y \in \mathbb{N} \mid suc(x) + y = y + suc(x)\}$$

y demostremos que $I = \mathbb{N}$, para ello recurrimos al axioma 5.

Sabemos que $suc(x) + 0 = 0 + suc(x)$, luego se tiene que $0 \in I$, primera hipótesis del axioma.

Supongamos $y \in I$, es decir, $y \in \mathbb{N}$ y

$$suc(x) + y = y + suc(x).$$

Como $y \in \mathbb{N}$, se tiene que $suc(y) \in \mathbb{N}$, ahora bien

$$\begin{aligned} suc(x) + suc(y) &= suc(suc(x) + y) \\ &= suc(y + suc(x)) \\ &= suc(suc(y + x)) \\ &= suc(suc(x + y)) \\ &= suc(x + suc(y)) \\ &= suc(suc(y) + x) \\ &= suc(y) + suc(x). \end{aligned}$$

Por lo tanto $suc(y) \in I$, Así tenemos en virtud del Axioma (5) que $I = \mathbb{N}$, con lo cual, se concluye que M también cumple las hipótesis del axioma 5, por lo tanto $M = \mathbb{N}$. □

Corolario 8 *Sean* $x, y \in \mathbb{N}$

$$suc(x) + y = suc(x + y) = suc(y) + x.$$

Teorema 9 (Asociatividad) *La suma* $(+)$ *en* $\mathbb{N}$ *es asociativa, en símbolos*

$$(\forall x, y, z \in \mathbb{N})((x + y) + z = x + (y + z)).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y, z \in \mathbb{N})((x + y) + z = x + (y + z))\}$$

y demostremos que $M = \mathbb{N}$.

Por propiedad 6 tenemos que

$$(\forall y, z \in \mathbb{N})((0 + y) + z = 0 + (y + z)) \Leftrightarrow (\forall y, z \in \mathbb{N})(y + z = y + z)$$

es decir, $0 \in M$.

Para la segunda parte, suponemos que $x \in M$, esto es

$$(\forall y, z \in \mathbb{N})((x + y) + z = x + (y + z)),$$

y queremos demostrar que $suc(x) \in M$, es decir

$$(\forall y, z \in \mathbb{N})((suc(x) + y) + z = suc(x) + (y + z)),$$

Para lo cual usaremos hipótesis y corolario anterior,

$$\begin{aligned}(suc(x)+y)+z &= suc(y+x)+z\\ &= suc((x+y)+z)\\ &= suc((x+y)+z)\\ &= suc(x+(y+z))\\ &= suc(x)+(y+z)\end{aligned}$$

lo cual es verdadero, por lo tanto $M=\mathbb{N}$, es decir,

$$(\forall x,y,z\in\mathbb{N})((x+y)+z=x+(y+z)).$$

□

Teorema 10 (Cancelación) *En* $\mathbb{N}$ *existe la ley de cancelación, es decir*

$$(\forall x,y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)).$$

Demostración: Considere el conjunto

$$M=\{x\in\mathbb{N}\mid(\forall y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z))\ \}$$

y demostremos que $M=\mathbb{N}$.

Para la primera parte, debemos verificar

$$(\forall y,z\in\mathbb{N})(0+y=0+z))\Leftrightarrow y=z)$$

es decir, propiedad 6, del neutro

$$(\forall y,z\in\mathbb{N})(y=z\Leftrightarrow y=z)$$

esto es, $0\in M$.

Para la segunda parte, suponemos que $x\in M$, esto es

$$(\forall y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)),$$

y queremos demostrar que $suc(x)\in M$, es decir

$$(\forall y,z\in\mathbb{N})((suc(x)+y=suc(x)+z)\Leftrightarrow(y=z)).$$

Para lo cual usaremos hipótesis y corolario anterior,

$$\begin{aligned}& suc(x)+y=suc(x)+z\\ \Leftrightarrow\ & suc(x+y)=suc(x+z)\\ \Leftrightarrow\ & x+y=x+z\\ \Leftrightarrow\ & y=z\end{aligned}$$

lo cual es verdadero, por lo tanto $M=\mathbb{N}$, es decir,

$$(\forall x,y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)).$$

□

1.2.2. Producto en $\mathbb{N}$

Propiedad 11 *Sea $x \in \mathbb{N}$ fijo, se define la siguiente relación por recurrencia*

$$x \cdot 0 \;:=\; 0$$

Si $x \cdot y$ esta definido, entonces

$$x \cdot suc(y) \;:=\; x \cdot y + x.$$

entendiendo que primeros multiplicamos y luego sumamos, entonces la anterior relación define la función

$$\begin{array}{rccc} \cdot \;:\; & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & y & \longmapsto & x \cdot y, \end{array}$$

Demostración: Sea $x \in \mathbb{N}$ fijo, definimos el conjunto

$$J = \{\; y \in \mathbb{N} \;\mid x \cdot y \;\text{ esta bien definido }\}$$

Claramente $0 \in \mathbb{N}$, ya que $x \cdot 0 = 0$ y además 0 no tiene un antecesor.

Ahora supongamos que $y \in J$, luego $x \cdot y \in \mathbb{N}$ esta bien definido, por lo tanto, tenemos que $x \cdot y + x \in \mathbb{N}$ es único, es decir $x \cdot suc(y)$ esta bien definido, por ende $suc(y) \in J$, luego por axioma 5, tenemos que $J = \mathbb{N}$, con lo cual, $\cdot$ es una operación binaria con x fijo. □

Observación: La anterior propiedad nos define de el producto de dos números naturales

Teorema 12 *En el conjunto de los números naturales, existe una operación producto " $\cdot$ " que cumple:*

1. $(\forall x \in \mathbb{N})(\, x \cdot 0 = 0\,)$.
2. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\, x \cdot suc(y) = x \cdot y + x\,)$.

Observación: Con las notaciones anteriores tenemos que

$$x \cdot 1 = x \cdot suc(0) = x \cdot 0 + x = x$$

y también

$$x \cdot 2 = x \cdot suc(1) = x \cdot 1 + x = x + x$$

La siguiente propiedad completa la demostración del neutro

Propiedad 13

$$(\forall y \in \mathbb{N})(1 \cdot y = y). \tag{1.3}$$

Demostración: Se define el conjunto

$$J = \{y \in \mathbb{N} \mid 1 \cdot y = y\}$$

y demostremos que $J = \mathbb{N}$.

Para la primera parte, tenemos que $0 \in \mathbb{N}$ y por la propiedad 4 tenemos que $1 \cdot 0 = 0$, de este modo concluimos que $0 \in J$.

Supongamos $y \in J$, es decir, $y \in \mathbb{N}$ y $1 \cdot y = y$, ahora bien como $y \in \mathbb{N}$, se tiene que $suc(y) \in \mathbb{N}$, por la Propiedad 4, se tiene que

$$1 \cdot suc(y) = 1 \cdot y + 1 = y + 1 = suc(y),$$

es decir $suc(y) \in J$.

Luego en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Propiedad 14

$$(\forall x \in \mathbb{N})(0 \cdot x = 0).$$

Demostración: Dado el conjunto

$$J = \{x \in \mathbb{N} \mid 0 \cdot x = 0\},$$

por demostrar que $J = \mathbb{N}$.

Por definición de " $\cdot$ ", se tiene $0 \cdot 0 = 0$ por lo tanto $0 \in J$.

Supongamos $x \in J$, es decir, $x \in \mathbb{N}$ y $0 \cdot x = 0$, ahora bien como $x \in \mathbb{N}$ por Axioma (2) $suc(x) \in \mathbb{N}$, además como

$$0 \cdot suc(x) = 0 \cdot x + 0 = 0 + 0 = 0$$

Luego se tiene que $suc(x) \in J$. Por lo tanto y en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Teorema 15 *El producto " $\cdot$ " en $\mathbb{N}$ es conmutativo, es decir*

$$(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})(x \cdot y = y \cdot x)\}$$

y demostremos que $M = \mathbb{N}$.

Sabemos que $0 \in \mathbb{N}$ y también que $0 \cdot y = y \cdot 0$ es verdadero, luego se tiene que $0 \in M$.

Supongamos $x \in M$, es decir $x \in \mathbb{N}$ y $x \cdot y = y \cdot x$ para todo $y \in \mathbb{N}$. Como $x \in \mathbb{N}$ se tiene que $suc(x) \in \mathbb{N}$, ahora debemos demostrar que $suc(x) \in M$ para esto consideremos el conjunto

$$I = \{y \in \mathbb{N} \mid suc(x) \cdot y = y \cdot suc(x)\}$$

y demostremos que $I = \mathbb{N}$.

Ya que $0 \in \mathbb{N}$ por Axioma (1) y que $suc(x) \cdot 0 = 0 \cdot suc(x)$ tenemos que $0 \in I$. Supongamos $y \in I$, es decir $y \in \mathbb{N}$ y $suc(x) \cdot y = y \cdot suc(x)$.

Como $y \in \mathbb{N}$ por Axioma (2) se tiene que $suc(y) \in \mathbb{N}$, ahora bien

$$\begin{aligned} suc(x) \cdot suc(y) &= suc(x) \cdot y + suc(x) \\ &= y \cdot suc(x) + suc(x) \\ &= (y \cdot x + y) + suc(x) \\ &= (x \cdot y + y) + suc(x) \\ &= suc((x \cdot y + y) + x) \\ &= suc((x \cdot y + x) + y) \\ &= x \cdot y + x + suc(y) \\ &= x \cdot suc(y) + suc(y) \\ &= suc(y) \cdot x + suc(y) \\ &= suc(y) \cdot suc(x). \end{aligned}$$

Así tenemos en virtud del Axioma (5) que $I = \mathbb{N}$, con lo cual $M = \mathbb{N}$. □

Teorema 16 *En $\mathbb{N}$ se cumple la propiedad distributiva, esto es*

$$(\forall x, y, z \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z).$$

Demostración: Sea

$$M = \{z \in \mathbb{N} \mid (\forall x, y \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z)\}$$

y demostremos que $M = \mathbb{N}$.

Veamos que $0 \in M$

$$(x + y) \cdot 0 = x \cdot 0 + y \cdot 0$$

es verdadero, luego se tiene que $0 \in M$.

Supongamos $z \in M$, es decir, $(\forall x, y \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z)$.

Por demostrar que $suc(x) \in M$, debemos justificar que,

$$(\forall x, y \in \mathbb{N})((x + y) \cdot suc(z) = x \cdot suc(z) + y \cdot suc(z)),$$

para ello

$$\begin{aligned} (x + y) \cdot suc(z) &= (x + y) \cdot z + (x + y) && \text{definición del producto} \\ &= (x \cdot z + y \cdot z) + (x + y) && \text{Hipótesis} \\ &= (x \cdot z + x) + (y \cdot z + y) && \text{Asociatividad y Conmutatividad} \\ &= x \cdot suc(z) + y \cdot suc(z) \end{aligned}$$

Así tenemos que $suc(z) \in M$, y en virtud del Axioma (5) se tiene $M = \mathbb{N}$. □

Corolario 17 *En $\mathbb{N}$ es válida también la siguiente ley distributiva*

$$(\forall x, y, z \in \mathbb{N})(x \cdot (y + z) = x \cdot y + x \cdot z)$$

Demostración: Sean $x, y, z \in \mathbb{N}$ cualesquiera, entonces

$$\begin{aligned} x \cdot (y+z) &= (y+z) \cdot x && \text{Teorema (15)} \\ &= y \cdot x + z \cdot x && \text{Teorema (16)} \\ &= x \cdot y + x \cdot z && \text{Teorema (15)} \end{aligned}$$

□

Teorema 18 *En* $\mathbb{N}$ *se cumple la propiedad asociativa, esto es*

$$(\forall x, y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z))\}$$

y demostremos que $M = \mathbb{N}$.

Por propiedad 14 tenemos que

$$(\forall y, z \in \mathbb{N})((0 \cdot y) \cdot z = 0 \cdot (y \cdot z)) \Leftrightarrow (\forall y, z \in \mathbb{N})(0 \cdot z = 0)$$

así $0 \in M$.

Supongamos ahora $x \in M$, esto es

$$(\forall y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)),$$

queremos demostrar que $suc(x) \in M$, esto es,

$$(\forall y, z \in \mathbb{N})((suc(x) \cdot y) \cdot z = suc(x) \cdot (y \cdot z)),$$

lo cual se obtiene de

$$\begin{aligned} (suc(x) \cdot y) \cdot z &= (y \cdot x + y) \cdot z \\ &= (y \cdot x) \cdot z + y \cdot z \\ &= (x \cdot y) \cdot z + y \cdot z \\ &= x \cdot (y \cdot z) + 1 \cdot (y \cdot z) \\ &= (x+1) \cdot (y \cdot z) \\ &= suc(x) \cdot (y \cdot z) \end{aligned}$$

por lo tanto $M = \mathbb{N}$, es decir,

$$(\forall x, y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

□

Observación: $(\mathbb{N}, +, \cdot)$, no es un anillo, ya que no cumple la propiedad de inverso aditivo.

1.2.3. Orden en $\mathbb{N}$

En esta sección definiremos un orden total en $\mathbb{N}$, para ello veremos la siguiente propiedad de los números naturales.
Notación: $\mathbb{N}^* = \mathbb{N} - \{0\}$.

Teorema 19 *Dados $x, y \in \mathbb{N}$ se presenta uno y sólo uno de los siguientes casos:*

1. $x = y$.
2. *Existe* $u \in \mathbb{N}, u \neq 0$ *tal que* $x + u = y$.
3. *Existe* $v \in \mathbb{N}, v \neq 0$ *tal que* $y + v = x$.

Demostración: Notemos que las tres proposiciones no pueden ser verdadera al mismo tiempo, ya que por el teorema 10 de cancelación $u = v = 0$ lo cual es una contradicción, luego definimos el conjunto

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})[(x = y) \veebar (\exists u \in \mathbb{N}^*,\, x + u = y) \veebar (\exists v \in \mathbb{N}^*,\, y + v = x)]\}$$

y demostremos que $M = \mathbb{N}$.

Para demostrar que $0 \in M$, debemos justificar la siguiente proposición

$$(\forall y \in \mathbb{N})[(0 = y) \veebar (\exists u \in \mathbb{N}^*,\, u = y) \veebar (\exists v \in \mathbb{N}^*,\, y + v = 0)]$$

Veamos que la tercera condición es falsa, para ello $y + v = 0$ con $v \neq 0$, es decir, existe $z \in \mathbb{N}$, tal que $v = suc(z)$, luego

$$0 = y + v = y + suc(z) = suc(y + z),$$

lo cual contradice el Axioma (3).

Por lo tanto, $0 \in M$ es equivale a

$$(\forall y \in \mathbb{N})[(y = 0) \veebar (y \neq 0) \veebar F]$$

lo cual es verdadero.

Ahora demostraremos $(\forall x \in M)(suc(x) \in M)$, esto es:

Suponemos que

$$(\forall y \in \mathbb{N})[(x = y) \veebar (\exists u \in \mathbb{N}^*, x + u = y) \veebar (\exists \in \mathbb{N}^*, y + v = x)]$$

Queremos demostrar que

$$(\forall y \in \mathbb{N})[(suc(x) = y) \veebar (\exists u \in \mathbb{N}^*, suc(x) + u = y) \veebar (\exists v \in \mathbb{N}^*, y + v = suc(x))],$$

Sea $x \in M$, tal que cumpla una de las siguientes proposiciones

I. $y = x$.

II. $x + u = y$ para algún $u \neq 0$.

III. $x = y + v$ para algún $v \neq 0$.

Prime Caso: Si $x = y$ entonces se aplicando el sucesor obtenemos

$$suc(x) = y + 1$$

a. $y = suc(x)$.

b. $suc(x) + u = y$ para algún $u \neq 0$.

c. $suc(x) = y + v$ para algún $v \neq 0$.

Claramente Cumple (c), y al reemplazar en las otras dos obtenemos

$$y = y + 1 \qquad y + 1 + u = y$$

ambas son imposibles.

Segundo Caso: Si existe $u \in \mathbb{N}^*$ tal que $x+u = y$, luego existe $w \in \mathbb{N}$ tal que $suc(w) = u$ entonces se tiene

$$\begin{aligned} suc(x) + u &= suc(y), \\ suc(x) + suc(w) &= suc(y) \\ suc(suc(x) + w) &= suc(y) \\ suc(x) + w &= y \end{aligned}$$

Claramente se cumple una de las siguientes proposiciones

$$suc(x) = y) \veebar (\exists u \in \mathbb{N}^*, suc(x) + u = y)$$

Además reemplazando en la otra, la proposición

$$suc(x) = suc(x) + w + v$$

es falsa.

Tercer Caso: Si existe $v \in \mathbb{N}^*$ tal que $x = y + v$, aplicando el sucesor se tiene $suc(x) = y + suc(v)$, luego se cumple (c)

$$suc(x) = y + w \text{ para algún } w \neq 0.$$

Las otras proposición son falsas (a), (b), ya que al reemplazar obtenemos

$$y = y + suc(v) \quad y + suc(v) + u = y \text{ para algún } u \neq 0.$$

Cancelando

$$0 = suc(v) \quad suc(v) + u = 0 \text{ para algún } u \neq 0.$$

De este modo se tiene que $suc(x) \in M$, de lo cual obtenemos $M = \mathbb{N}$. □

Definición 6 *Sean $x, y \in \mathbb{N}$. Se dice que*

1. *x es **menor o igual** a y (o y es **mayor o igual** que x) si y sólo si existe $u \in \mathbb{N}$ de modo que $x + u = y$, este hecho lo anotaremos indistintamente por*

$$x \leq y \quad \vee \quad y \geq x.$$

Es decir,

$$x \leq y \Leftrightarrow (\exists u \in \mathbb{N})(x + u = y).$$

2. *x es **menor que** y (o y es **mayor que** x) si y sólo si existe $u \in \mathbb{N}^*$ de modo que $x + u = y$, este hecho lo anotaremos indistintamente por*

$$x < y \quad \vee \quad y > x.$$

Es decir,

$$x < y \Leftrightarrow (\exists u \in \mathbb{N}^*)(x + u = y).$$

Propiedad 20 *Sean $x, y \in \mathbb{N}$, entonces se tiene*

$$[x < y \Leftrightarrow (x \leq y) \wedge (x \neq y)]$$

o bien

$$[y > x \Leftrightarrow (y \geq x) \wedge (y \neq x)].$$

Notación: En adelante usaremos las siguientes notaciones:

1. $x \ngeq y$, quiere decir que x no es mayor o igual a y.
2. $x \nleq y$, quiere decir que x no es menor o igual a y.
3. $x \not< y$, quiere decir que x no es mayor que y.
4. $x \not> y$, quiere decir que x no es menor que y.

Propiedad 21 *Notemos que*

$$x \ngeq y \Leftrightarrow x < y.$$

Teorema 22 *La relación $\leq$ es una relación de orden en $\mathbb{N}$, es decir la relación es refleja, antisimétrica y transitiva.*

Demostración:
Refleja: Por la definición de suma se tiene que $x + 0 = x$, definición de $\leq$ se tiene que

$$x \leq x \quad \forall x \in \mathbb{N}.$$

Antisimétrica: Supongamos que $x \leq y \ \wedge \ y \leq x$. Luego existen $u, v \in \mathbb{N}$ tales que

$$x + u = y \quad \wedge \quad y + v = x$$

Si u, v uno de ellos es nulo, esta listo.

Supongamos que u, v son no nulo, luego

$$y = x + u = (y + v) + u = y + (v + u)$$

tenemos entonces que

$$y + 0 = y + (v + u)$$

cancelando tenemos que

$$u + v = 0.$$

Ahora bien, como $u \neq 0$ entonces $u = suc(z)$ para algún $z \in \mathbb{N}$ pero

$$0 = v + u = v + suc(z) = suc(v + z)$$

lo cual es una contradicción con el Axioma (2).Luego $u = 0 \vee v = 0$ entonces se cumple

$$x = y.$$

Transitiva: Supongamos $x \leq y \wedge y \leq z$. Luego existen $u, v \in \mathbb{N}$ tales que

$$x + u = y \quad \wedge \quad y + v = z$$

de esto es claro que

$$x + u + v = z$$

es decir

$$x + (u + v) = z$$

por lo tanto

$$x \leq z.$$

□

Observación: La transitividad se mantiene al cambiar $\leq$ por $<$, es decir, dados $x, y, z \in \mathbb{N}$

$$[(x < y) \wedge (y < z)] \Rightarrow (x < z).$$

Teorema 23 (Totalidad) *Dados x e $y \in \mathbb{N}$ se cumple una y sólo una de las siguientes proposición*

1. $x = y$.
2. $x < y$.
3. $y < x$.

Demostración: Inmediata a partir del Teorema (19) y la definición del símbolo $<$.

□

Teorema 24 *La suma en $\mathbb{N}$ es monótona, es decir*

$$(\forall x, y, z \in \mathbb{N})(x \leq y \Rightarrow (x + z \leq y + z)).$$

Demostración: Supongamos $x \leq y$, luego existe $u \in \mathbb{N}$ tal que $x + u = y$ de donde

$$\begin{array}{rrcl} & (x+u)+z & = & y+z, \quad \forall z \in \mathbb{N} \\ \Leftrightarrow & x+(u+z) & = & y+z \\ \Leftrightarrow & x+(z+u) & = & y+z \\ \Leftrightarrow & (x+z)+u & = & y+z \end{array}$$

de esto es claro que

$$x + z \leq y + z.$$

□

Corolario 25 *Sea $x \in \mathbb{N}$, entonces*

$$x \leq suc(x).$$

Teorema 26 *Para todo $x \in \mathbb{N}$ se tiene que $x \geq 0$.*

Demostración: Por Propiedad (6) tenemos que $0 + x = x$, $\forall x \in \mathbb{N}$, es decir existe $u = x$ tal que $0 + u = x$, y por definición de mayor o igual se tiene que $x \geq 0$ □

Corolario 27 *Si $x \in \mathbb{N}^*$ entonces $x \geq 1$.*

Demostración: Supongamos $x \neq 0$.

Entonces $x = suc(y)$ para algún $y \in \mathbb{N}$, luego como $suc(y) = y + 1$ se tiene que

$$x = y + 1 = 1 + y,$$

de donde

$$x \geq 1.$$

Corolario 28 *Sean $x, y \in \mathbb{N}$, tal que $x < y$ entonces,*

$$suc(x) \leq y$$

Demostración: Supongamos $y > x$. Luego existe $u \in \mathbb{N}, u \neq 0$ tal que $x + u = y$, ahora bien como $u \neq 0$ entonces $u = suc(v)$ para algún $v \in \mathbb{N}$, luego

$$y = x + suc(v) = suc(x + v) = suc(v + x) = v + suc(x),$$

de donde obtenemos que

$$y \geq suc(x) \quad \forall x, y \in \mathbb{N}.$$

□

Teorema 29 *Sean $x, y \in \mathbb{N}$.*

$$Si\ x > 0\ e\ y > 0\ entonces\ xy > 0.$$

Demostración: Como $y > 0$ es decir $y \neq 0$ tenemos que existe $u \in \mathbb{N}$ tal que $y = suc(u)$, ahora

$$xy = xsuc(u)$$

luego existe xu tal que

$$xy = xu + x$$

es decir

$$xy \geq x$$

además $x > 0$, así tenemos que

$$xy \geq x > 0.$$

A partir de esto, tenemos los siguientes casos:

1. $xy > x$, es decir $xy > x > 0$, luego por transitividad obtenemos que

$$xy > 0.$$

2. $xy = x$, es decir $xy = x > 0$ de donde

$$xy > 0.$$

□

Teorema 30 *El producto en* $\mathbb{N}$ *es monótono.*
Sean $x, y, z \in \mathbb{N}$

$$(x < y) \wedge (z > 0) \Rightarrow (xz < yz).$$

Demostración: Supongamos $(x < y) \wedge (z > 0)$. Luego como

$$x < y \Leftrightarrow (\exists u \in \mathbb{N}, u \neq 0)(x + u = y)$$

tenemos que

$$(x + u)z = yz$$

de esto

$$xz + uz \;\; = \;\; yz. \tag{1.4}$$

Ahora bien como $u \in \mathbb{N} \wedge u \neq 0$ se tiene que $u > 0$, y $z > 0$ (por hipótesis), tenemos que $uz > 0$ teorema anterior, por lo tanto, de la relación (1.4) se obtiene que $xz \leq yz$ pero como $uz > 0$, tenemos que $uz \neq 0$ entonces podemos concluir que

$$xz < yz.$$

□

Teorema 31 *Si* $x \neq 0$ *e* $y \neq 0$ *entonces* $xy \neq 0$ *para todo* $x, y \in \mathbb{N}$.

Demostración: Supongamos $x \neq 0$ e $y \neq 0$. además como todo número natural es mayor o igual a cero tenemos en particular que $x \geq 0$, luego se obtiene que $x > 0$. Del mismo modo podemos se concluye que $y > 0$.

Así tenemos que $x > 0 \wedge y > 0$ con lo cual $xy > 0$, por la definición de mayor que se tiene que

$$xy \neq 0$$

□

Teorema 32 *Sean $x, y, z \in \mathbb{N}$ tales que $z \neq 0$ entonces se cumple.*

$$[(x \neq y) \Rightarrow (zx \neq zy)]$$

Demostración: Sean $x, y, z \in \mathbb{N}$ tales que $z \neq 0$ $x \neq y$

Por el teorema 23 consideremos entonces los siguientes casos:

1. Supongamos $x > y$, luego existe $u \in \mathbb{N}, u \neq 0$ de modo que $y + u = x$ de esto

$$zx = z(y + u) = zy + zu. \tag{1.5}$$

   Ahora bien como $z \neq 0$ y $u \neq 0$ tenemos que $zu \neq 0$, este hecho y la igualdad en (1.5) implican que $zx > zy$ con lo cual

$$zx \neq zy.$$

2. Análogo al caso anterior suponiendo $x < y$.

□

Teorema 33 (Principio del Buen Orden)

Todo subconjunto no vacío de $\mathbb{N}$ tiene un menor elemento, en símbolos

$$(\forall A \subseteq \mathbb{N}, A \neq \emptyset)(\exists a \in A)(\forall x \in A)(a \leq x).$$

Demostración: Sea $\emptyset \neq A \subseteq \mathbb{N}$ y consideremos el conjunto

$$B = \{x \in \mathbb{N} \mid (\forall y \in A)(\, x \leq y \,)\}.$$

En primer lugar notemos que el conjunto B verifica las siguientes propiedades:

1. $0 \in B$ pues como $x \geq 0$ para todo $x \in \mathbb{N}$ en particular

$$(\forall y \in A)(\, y \geq 0 \,)$$

2. Como $A \neq \emptyset$, luego existe $x \in A$ y además $x < suc(x)$, luego $suc(x) \notin B$, luego $B \neq \mathbb{N}$, por lo tanto B no puede cumplir la condición

$$(\forall x \in B)(\, suc(x) \in B \,)$$

   Por ello, existe $u \in B$, tal que $u + 1 \notin B$,

   Ahora bien para probar el teorema basta probar que $u \in A$.

   Supongamos lo contrario, esto es $u \in B \wedge u \notin A$. Luego $(\forall y \in A)(\, u < y \,)$, por corolario 28 tenemos que $(\forall y \in A)(\, u + 1 \leq y \,)$ lo cual implica que $u + 1 \in B$ y esto es una contradicción.

   Por lo tanto $u \in A$, es decir, $(\exists u \in A)(\forall y \in A)(\, u \leq y \,)$. □

Teorema 34 (Principio de Inducción)
Sea $n \in \mathbb{N}$ y $p(n)$ una proposición en la variable n. Si se cumple

1. *$p(0)$ es verdadera.*

2. *$(\forall n \in \mathbb{N})(p(n) \Rightarrow p(suc(n))$ es verdadera.*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

Demostración: Sea

$$M = \{n \in \mathbb{N} \mid p(n) \text{ es verdadera}\}$$

y demostremos que $M = \mathbb{N}$.

Por hipótesis tenemos que $p(0)$ es verdadera, luego $0 \in M$.

Supongamos $n \in M$, es decir, $p(n)$ es verdadera, pero por hipótesis si $p(n)$ es verdadera entonces $p(suc(n))$ es verdadera, luego se tiene que $suc(n) \in M$, ahora bien en virtud del Axioma (5)tenemos que $M = \mathbb{N}$ lo cual concluye la demostración.

□

Observación: Sabemos que $suc(n) = n + 1$, luego el teorema precedente se puede escribir como sigue:

Corolario 35 (Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$p(0)$ y*

2. *$(\forall n \in \mathbb{N})(p(n) \Rightarrow p(n+1))$*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

Corolario 36 (Segundo Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$(\exists k_0 \in \mathbb{N})(p(k_0))$ y*

2. *$(\forall n \in \mathbb{N})((n \geq k_0 \wedge p(n)) \Rightarrow p(n+1))$*

Entonces la proposición $n \geq k_0 \Rightarrow p(n)$ es válida para todo $n \in \mathbb{N}$.

Corolario 37 (Tercer Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$p(0)$ y*

2. *$(\forall n \in \mathbb{N})((p(0) \wedge p(1) \wedge \cdots \wedge p(n)) \Rightarrow p(n+1))$*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

1.3. Ejercicios Desarrollados

Ejemplo 6 *Sea A un subconjunto de números reales que cumple las siguientes propiedades:*

$Ax.$I. $4 \in A \ \wedge \ 7 \notin A$.

$Ax.$II. $(\forall x \in A)(3x + 1 \in A)$.

$Ax.$III. $(\forall x, y \in A)(x + y \in A)$.

Demuestre las siguientes propiedades

a. $3 \in A \Rightarrow 14 \in A$.

b. $9 \in A \Rightarrow (21 \in A \vee 31 \notin A)$.

c. $(\forall x, y \in A)(-3x - 2y \notin A)$.

Demostración:

a. Si $3 \in A$, implica que $3 \cdot 3 + 1 = 10 \in A$.
Pero $4 \in A \wedge 10 \in A$, por lo tanto $10 + 4 = 14 \in A$.
De esta manera se tiene que, si $3 \in A$ entonces $14 \in A$.

b. Supongamos que $9 \in A, 4 \in A$, por propiedad Ax.III se tiene que $9 + 4 = 13 \in A$.
Análogamente $13 \in A, 4 \in A$, por propiedad Ax.III se tiene que $13 + 4 = 17 \in A$.
Finalmente $17 \in A, 4 \in A$, por propiedad Ax.III se tiene que $17 + 4 = 21 \in A$.
Como $21 \in A$, luego la proposición $21 \in A \vee 31 \notin A$ es verdadera.
De esta manera se obtiene que, $9 \in A \Rightarrow (21 \in A \vee 31 \notin A)$.

c. Por absurdo, supongamos $(\forall x, y \in A)(-3x - 2y \notin A)$ es falso, es decir,

$$(\exists x, y \in A)(-3x - 2y \in A) \text{ es verdadero.}$$

Sean $x, y \in A$ tal que $-3x - 2y \in A$, luego

$$\begin{aligned} x \in A &\Rightarrow 3x + 1 \in A \quad \text{Prop Ax.II} \\ -3x - 2y \in A \wedge 3x + 1 \in A &\Rightarrow -2y + 1 \in A \quad \text{Prop Ax.III} \end{aligned}$$

$$\begin{aligned} -2y + 1 \in A \wedge y \in A &\Rightarrow -y + 1 \in A \\ -y + 1 \in A \wedge y \in A &\Rightarrow 1 \in A \\ 1 \in A \wedge 4 \in A &\Rightarrow 5 \in A \\ 1 \in A \wedge 5 \in A &\Rightarrow 6 \in A \\ 1 \in A \wedge 4 \in A &\Rightarrow 7 \in A \end{aligned}$$

Lo cual es una contradicción, por lo tanto

$$(\forall x, y \in A)(-3x - 2y \notin A), \quad \text{es Verdadero}$$

□

Ejemplo 7 *Demostrar por inducción*

$$(\forall n \in \mathbb{N} - \{0\})(\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)]$$

Demostración: Sea

$$p(n) : (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)]$$

Veamos

$$\begin{aligned} p(1) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^2 - a^2 - 2a - 1)] \\ &: (\forall a \in \mathbb{Z})[a(2a+1) \mid 0] \equiv V \end{aligned}$$

Supongamos $p(n)$ y demostremos $p(n+1)$

$$\begin{aligned} p(n) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)] \\ p(n+1) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n+2} - a^{2n+2} - 2a - 1)] \end{aligned}$$

Dado $a \in \mathbb{Z}$, existe $k \in \mathbb{Z}$ tal que $((a+1)^{2n} - a^{2n} - 2a - 1) = a(2a+1)k$ o bien $(a+1)^{2n} = a^{2n} + 2a + 1 + a(2a+1)k$

$$\begin{aligned} & (a+1)^{2n+2} - a^{2n+2} - 2a - 1 \\ = \; & (a+1)^{2n}(a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & [a^{2n} + 2a + 1 + a(2a+1)k](a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & a^{2n}(a+1)^2 + (2a+1)(a+1)^2 + a(2a+1)k(a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & a^{2n}(a+1)^2 - a^{2n+2} + (2a+1)(a+1)^2 - (2a+1) + a(2a+1)k(a+1)^2 \\ = \; & a^{2n}((a+1)^2 - a^2) + (2a+1)((a+1)^2 - 1) + a(2a+1)k(a+1)^2 \\ = \; & a^{2n}(2a+1) + (2a+1)(a^2 + 2a) + a(2a+1)k(a+1)^2 \\ = \; & a(2a+1)a^{2n-1} + a(2a+1)(a+2) + a(2a+1)k(a+1)^2 \\ = \; & a(2a+1)[a^{2n-1} + (a+2) + k(a+1)^2] = a(2a+1)k' \end{aligned}$$

Luego

$$(\forall n \in \mathbb{N}^*))(p(n) \Rightarrow p(n+1))$$

es verdadera. Por teorema de inducción se concluye.

Ejemplo 8 *Demostrar*

$$(\forall n, m \in \mathbb{N})(n + m = 0 \Rightarrow (n = 0 \wedge m = 0)).$$

Demostración: Notemos que la proposición es equivalente a

$$(\forall n, m \in \mathbb{N})((n \neq 0 \vee m \neq 0) \Rightarrow n + m \neq 0).$$

Luego supongamos que $n \neq 0 \vee m \neq 0$
Primer Caso: Si $n \neq 0$ existe $n' \in \mathbb{N}$ tal que $suc(n') = n$

$$n + m = suc(n') + m = suc(n' + m) \in \mathbb{N}^*$$

Por lo tanto $n + m \neq 0$

Segundo Caso: Si $m \neq 0$ existe $m' \in \mathbb{N}$ tal que $suc(m') = m$

$$n + m = n + suc(m') = suc(n + m') \in \mathbb{N}^*$$

Por lo tanto $n + m \neq 0$.

De Primer y Segundo Caso, se tiene que

$$(\forall n, m \in \mathbb{N})((n \neq 0 \vee m \neq 0) \Rightarrow n + m \neq 0).$$

Ejercicio 9 *Sea A un subconjunto de números reales que cumple las siguientes propiedades (axiomas):*

$Ax.$I. $5 \in A \ \wedge \ 7 \notin A.$

$Ax.$II. $(\forall x \in A)(3x + 2 \in A).$

$Ax.$III. $(\forall x, y \in A)(x + y \in A).$

Demuestre los siguientes propiedades

a. $3 \in A \Rightarrow 16 \in A.$

b. $4 \in A \Rightarrow 23 \in A.$

c. $11 \in A \Rightarrow (28 \in A \vee 31 \notin A).$

d. $24 \notin A \Rightarrow (4 \notin A \vee 12 \in A).$

e. $2 \notin A.$

f. $(\forall x, y \in A)(3x + 2y + 17 \in A).$

g. $(\forall x, y \in A)(7x + 3y + 16 \in A).$

h. $(\forall x, y \in A)(-3 - 3x - y \notin A).$

i. $(\forall y, z \in \mathbb{R})((3y + z + 7) \notin A \Rightarrow (y \notin A \vee \frac{z}{2} \notin A)).$

j. $(\forall y, z \in \mathbb{R})((3y \notin A \wedge (z + 10) \notin A) \Rightarrow (y \notin A \vee z \notin A)).$

Ejercicio 10 *Dado el conjunto*

$$A = \{0\} \cup \left\{ n + \frac{1}{m} \mid n \in \mathbb{N}, m \in \mathbb{N}^* \right\}.$$

Determine que Axiomas de Peano satisface el conjunto A.

Ejercicio 11 *Demostrar directamente*

a. $(\forall n \in \mathbb{N})(suc(n) = n + suc(0)).$

b. $(\forall n \in \mathbb{N})(suc(n) + m = suc(m + n))$.

c. $(\forall n \in \mathbb{N})(suc(suc(n)) \neq 1)$.

d. $(\forall n, m \in \mathbb{N})(m + suc(n) \neq m)$.

e. $(\forall n, m \in \mathbb{N})(n + m = 0 \Rightarrow (n = 0 \wedge m = 0))$.

f. $(\forall n, m \in \mathbb{N})(n \cdot m = 0 \Rightarrow (n = 0 \vee m = 0))$.

g. $(\forall r \in \mathbb{N}^*)(\forall n, m \in \mathbb{N})(r \cdot n = r \cdot m \Rightarrow (n = m))$.

Ejercicio 12 *Demostrar usando las propiedades*

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

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

Ejercicio 13 *Sea* $\{a_n\}$ *una sucesión definida por recurrencia, tal que*

$$f(0) = 0;\ f(1) = 1;\ a_n = a_{n-1} + a_{n-2},\ \textit{con } n \leq> 1.$$

Demostrar que

1. $(\forall n \in \mathbb{N})(f(n) < \left(\frac{7}{4}\right)^n)$.
2. $(\forall 4 < n \in \mathbb{N})(\left(\frac{4}{3}\right)^n < f(n))$.
3. $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N}^*)(f(n + m) = f(m - 1)f(n) + f(m)f(n + 1))$.
4. $$(\forall n \in \mathbb{N})\left(f(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]\right).$$

Capítulo 2

Números Enteros

Notemos que las ecuaciones del tipo $a + x = b$, con $a, b \in \mathbb{N}$, pueden tener solución vacía en el conjunto de los numeros naturales. Para que este tipo de ecuación siempre tenga solución no vacía, es necesario construir un conjunto $\mathbb{Z}$ llamado de los números enteros.

Definición 7 *Sean $x, y, z \in \mathbb{N}$.*

Se dice que la diferencia o resta entre x e y es z si y sólo si x es igual a $y + z$, es decir,

$$x - y = z \text{ si y sólo si } x = y + z$$

Observación: El símbolo "$x - y$"se lee x menos y.

Propiedad 38 *Sean $x, y, z \in \mathbb{N}$.*

1. *Si $x - y = p,\ p \in \mathbb{N}$ entonces se tiene*
$$(x - y)z = xz - yz.$$
2. *Si $x - y = p,\ p \in \mathbb{N}$ entonces se tiene*
$$(x - y) + z = (x + z) - y.$$

Demostración:

1. Sea $x - y = p,\ p \in \mathbb{N}$, luego tenemos que $x = y + p$ de este modo
$$xz = (y + p)z = yz + pz$$
y por lo tanto
$$xz - yz = pz = (x - y)z.$$
2. Sean $x - y = p,\ p \in \mathbb{N}$
Luego tenemos que
$$x = y + p$$
de donde
$$x + z = y + p + z$$
Por lo tanto
$$(x + z) - y = p + z = (x - y) + z$$

□

Definición 8 *En el conjunto* $\mathbb{N} \times \mathbb{N}$ *se define la siguiente relación*[1]*:*

Sean $a, b, c, d \in \mathbb{N}$*, entonces diremos que los pares ordenados* (a, b) *y* (c, d) *están relacionados, lo que denotaremos por*

$$(a, b) \sim (c, d) \quad \textit{si y sólo si } a + d = b + c.$$

Teorema 39 *La relación* $\sim$ *es una relación de equivalencia en* $\mathbb{N} \times \mathbb{N}$*.*

Demostración: Sean $a, b, c, d, e, f \in \mathbb{N}$

Refleja: Como $a + b = b + a$ se tiene que $(a, b) \sim (b, a)$
Simétrica: Supongamos $(a, b) \sim (c, d)$, luego tenemos que

$$\begin{array}{rrcl} & a+d & = & b+c \\ \Rightarrow & b+c & = & a+d \\ \Rightarrow & c+b & = & d+a \\ \Rightarrow & (c,d) & \sim & (a,b) \end{array}$$

Transitiva: Supongamos $(a, b) \sim (c, d) \wedge (c, d) \sim (e, f)$, d lo cual se obtiene que

$$\begin{array}{rccccl} & (a+d=b+c) & \wedge & (c+f=d+e) & & \\ \Rightarrow & a+d+f=b+c+f & \wedge & c+f=d+e & & \text{Reemplazando} \\ \Rightarrow & a+f+d & = & b+d+e & & \text{Cancelado} \\ \Rightarrow & a+f & = & b+e & & \\ \Rightarrow & (a,b) & \sim & (e,f) & & \end{array}$$

□

Definición 9 *Sean* $(a, b) \in \mathbb{N} \times \mathbb{N}$*.*

Se define la clase de equivalencia de (a, b) *como el conjunto de todos los pares ordenados de* $\mathbb{N} \times \mathbb{N}$ *que están relacionados con el par ordenado* (a, b)*, y la denotaremos por* $\overline{(a, b)}$*. El par* (a, b) *se llama representante de la clase de equivalencia de* (a, b)*.*

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid (x, y) \sim (a, b)\}.$$

Ejemplo 14

$$\begin{array}{rcl} \overline{(1,0)} & = & \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid (x,y) \sim (1,0)\} \\ & = & \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x+0 = y+1\} \\ & = & \{(1,0),(2,1),(3,2),\ldots\}. \end{array}$$

Definición 10 *El conjunto formado por todas las clases de equivalencia definidas sobre el conjunto* $\mathbb{N} \times \mathbb{N}$*, es llamado conjunto de los números enteros y a cada clase de equivalencia número entero.*

El conjunto de los números enteros se anota

$$\mathbb{Z} = \{\overline{(a, b)} \mid a, b \in \mathbb{N}\}.$$

[1]Para más detalles ver el capítulo de **Relaciones** del curso de Matemáticas Generales.

Sistema de Representante

Por teorema (23) tenemos que, dado $a, b \in \mathbb{N}$ se tiene que $a \geq b \ \veebar \ a < b$.
Luego $(a, b) \in \overline{(a-b, 0)}$, cuando $a \geq b$ y en el otro caso tenemos que $(a, b) \in \overline{(0, b-a)}$.
Es decir,

$$\overline{(a,b)} = \begin{cases} \overline{(a-b,0)} & \text{si} \quad a \geq b \\ \\ \overline{(0,b-a)} & \text{si} \quad a < b \end{cases}$$

Además se tiene que

$$\begin{array}{rcl} \overline{(n,0)} = \overline{(m,0)} & \Rightarrow & n = m \\ \overline{(0,n)} = \overline{(0,m)} & \Rightarrow & n = m \\ \overline{(n,0)} = \overline{(0,m)} & \Rightarrow & n = m = 0 \end{array}$$

Así tenemos que cada elemento $\overline{(a,b)} \in \mathbb{Z}$ admite una único elemento de las siguientes formas

$$\overline{(n,0)} \quad \vee \quad \overline{(0,m)}$$

donde $n \in \mathbb{N}, m \in \mathbb{N}^*$.

De este modo tenemos que

$$\{\overline{(n,0)}, \overline{(0,m)} \mid n \in \mathbb{N}, m \in \mathbb{N}^*\}$$

es un sistema de representante

2.1. Suma y Producto en $\mathbb{Z}$

Teorema 40 *Sean $(a,b),(c,d),(e,f),(g,h) \in \mathbb{N} \times \mathbb{N}$ tales que $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces tenemos*

$$\begin{array}{rcl} (a+e \ , \ b+f) & \sim & (c+g \ , \ d+h) \\ (a \cdot e + b \cdot f \ , \ a \cdot f + b \cdot e) & \sim & (c \cdot g + d \cdot h \ , \ c \cdot h + d \cdot g) \end{array}$$

Demostración:

1. **Suma**

   Supongamos $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces

$$\begin{array}{rcccc} & a+d = b+c & \wedge & e+h = f+g \\ \Rightarrow & (a+d)+(e+h) & = & (b+c)+(f+g) \\ \Rightarrow & (a+e)+(d+h) & = & (b+f)+(c+g) \\ \Rightarrow & (a+e, b+f) & \sim & (c+g, d+h) \\ \Rightarrow & \overline{(a+e, b+f)} & = & \overline{(c+g, d+h)}. \end{array}$$

2. Producto

   Supongamos $(a,b) \sim (c,d)$ y $(e,f) \sim (g,h)$ entonces

   $$(1) \quad a+d = b+c \ \wedge \ (2) \quad e+h = f+g$$

   La primera ecuación amplificamos por e, f, y la segunda ecuación por c, d

   $$\begin{array}{rcl} ae+de & = & be+ce \\ bf+cf & = & af+df \\ ce+ch & = & cf+cg \\ df+dg & = & de+dh \end{array}$$

   Sumando las ecuaciones resultantes obtenemos

   $$ae+\underline{de}+bf+\underline{cf}+\underline{ce}+ch+\underline{df}+dg = be+\underline{ce}+af+\underline{df}+\underline{cf}+cg+\underline{de}+dh$$

   Cancelando se tiene

   $$(ae+bf)+(ch+dg) = (be+af)+(cg+dh)$$

   de lo cual tenemos

   $$(a\cdot e+b\cdot f \ , \ a\cdot f+b\cdot e) \sim (c\cdot g+d\cdot h \ , \ c\cdot h+d\cdot g)$$

□

Observación: El teorema anterior nos permite definir la suma y el producto en $\mathbb{Z}$ del siguiente modo:

Definición 11 *Sean $\overline{(a,b)}$ y $\overline{(c,d)} \in \mathbb{Z}$, se definen*

1. **Suma**
   $$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$
2. **Producto**
   $$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}.$$

Teorema 41 *El conjunto de los números enteros con la suma y el producto definido tiene la estructura de un anillo conmutativo. De otro modo $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, es decir*

1. *Propiedades de la suma en $\mathbb{Z}$*

   i) Asociatividad
   $$(\forall x,y,z \in \mathbb{Z})((x+y)+z = x+(y+z)).$$

   ii) Existencia de elemento neutro
   $$(\exists! e \in \mathbb{Z})(\forall x \in \mathbb{Z})(x+e = e+x = x).$$

   iii) Existencia de elemento inverso
   $$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y = y+x = e).$$

   iv) Conmutatividad
   $$(\forall x,y \in \mathbb{Z})(x+y = y+x).$$

2. *Propiedades del producto en* $\mathbb{Z}$

   i) Asociatividad

   $$(\forall x, y, z \in \mathbb{Z})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

   ii) Existencia de elemento neutro

   $$(\exists! e \in \mathbb{Z})(\forall x \in \mathbb{Z})(x \cdot e = e \cdot x = x).$$

   iii) Conmutatividad

   $$(\forall x, y \in \mathbb{Z})(x \cdot y = y \cdot x).$$

3. *El producto en* $\mathbb{Z}$ *es distributivo respecto a la suma*

   $$x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall x, y, z \in \mathbb{Z}.$$

Demostración:

1. Propiedades de la suma en $\mathbb{Z}$

   i) Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

   Entonces

   $$\begin{aligned}
   (x+y)+z &= [\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} \\
   &= \overline{(a+c, b+d)} + \overline{(e,f)} \\
   &= \overline{((a+c)+e, (b+d)+f)} \\
   &= \overline{(a+(c+e), b+(d+f))} \\
   &= \overline{(a,b)} + \overline{(c+e, d+f)} \\
   &= \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}] \\
   &= x + (y+z).
   \end{aligned}$$

   ii) Sean $x = \overline{(a,b)}$ cualquiera y determinemos $e = \overline{(u,v)}$ de modo que

   $$\begin{aligned}
   & \overline{(a,b)} + \overline{(u,v)} = \overline{(a,b)} \\
   \Leftrightarrow\ & \overline{(a+u, b+v)} = \overline{(a,b)} \\
   \Leftrightarrow\ & (a+u, b+v) \sim (a,b) \\
   \Leftrightarrow\ & (a+u)+b = (b+v)+a \\
   \Leftrightarrow\ & a+u = v+a \\
   \Leftrightarrow\ & u = v.
   \end{aligned}$$

   Por lo tanto existe $e = \overline{(u,u)}$, el cual por comodidad lo denotaremos por $\overline{(0,0)}$.

iii) Sea $x = \overline{(a,b)}$, queremos encontrar un elemento $y = \overline{(c,d)}$ de modo que se verifique la siguiente relación

$$\begin{array}{rrcl} & x+y & = & e \\ \Leftrightarrow & \overline{(a,b)} + \overline{(c,d)} & = & \overline{(0,0)} \\ \Leftrightarrow & \overline{(a+c,b+d)} & = & \overline{(0,0)} \\ \Leftrightarrow & (a+c,b+d) & \sim & (0,0) \\ \Leftrightarrow & a+c & = & b+d \\ \Leftrightarrow & c+a & = & d+b \\ \Leftrightarrow & (c,d) & \sim & (b,a) \\ \Leftrightarrow & \overline{(c,d)} & = & \overline{(b,a)}. \end{array}$$

Por lo tanto tenemos que $y = \overline{(b,a)}$.

Notación: De acuerdo a lo anterior cada elemento en $\mathbb{Z}$ tiene un inverso. En adelante anotaremos como $-x$ el inverso de $x \in \mathbb{Z}$. Según esto $-\overline{(a,b)} = \overline{(b,a)}$ y siempre tendremos que $x + (-x) = e$, además naturalmente $-(-x) = x, \forall x \in \mathbb{Z}$.

iv) La conmutatividad queda como ejercicio

2. Propiedades del producto en $\mathbb{Z}$

i) Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$. Entonces

$$\begin{array}{rcl} (x \cdot y) \cdot z & = & [\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} \\ & = & \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\ & = & \overline{((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)} \\ & = & \overline{((ac)e + (bd)e + (ad)f + (bc)f, (ac)f + (bd)f + (ad)e + (bc)e)} \\ & = & \overline{(a(ce) + b(de) + a(df) + b(cf), a(cf) + b(df) + a(de) + b(ce))} \\ & = & \overline{(a(ce) + a(df) + b(cf) + b(de), a(cf) + a(de) + b(ce) + b(df))} \\ & = & \overline{a(ce+df) + b(cf+de), a(cf+de) + b(ce+df)} \\ & = & \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\ & = & \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}] \\ & = & x \cdot (y \cdot z). \end{array}$$

ii) Sean $x = \overline{(a,b)}$,

$$\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)} = \overline{(a,b)}.$$

Además

$$\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(1 \cdot a + 0 \cdot b, 0 \cdot a + 1 \cdot b)} = \overline{(a,b)}.$$

iii) Sea $x = \overline{(a,b)}, y = \overline{(c,d)}$

Luego

$$\begin{array}{rcl} x \cdot y & = & \overline{(a,b)} \cdot \overline{(c,d)} \\ & = & \overline{(ac+bd, ad+bc)} \\ & = & \overline{(ca+db, cb+da)} \\ & = & \overline{(c,d)} \cdot \overline{(a,b)} \\ & = & y \cdot x. \end{array}$$

3. Distributividad

   Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)}$

   Entonces

$$\begin{aligned} x \cdot (y+z) &= \overline{(a,b)} \cdot (\overline{(c,d)} + \overline{(e,f)}) \\ &= \overline{(a,b)} \cdot \overline{(c+e, d+f)} \\ &= \overline{(a(c+e)+b(d+f), a(d+f)+b(c+e))} \\ &= \overline{(ac+ae+bd+bf, ad+af+bc+be)} \\ &= \overline{((ac+bd)+(ae+bf), (ad+bc)+(af+be))} \\ &= \overline{(ac+bd, ad+bc)} + \overline{(ae+bf, af+be)} \\ &= \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} \\ &= x \cdot y + x \cdot z. \end{aligned}$$

□

Teorema 42 *Ley de cancelación para la suma en $\mathbb{Z}$, es decir*

$$(\forall x, y, z \in \mathbb{Z})((x + y = x + z) \Rightarrow y = z).$$

Demostración: Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

Luego

$$\begin{aligned} & \overline{(a,b)} + \overline{(c,d)} = \overline{(a,b)} + \overline{(e,f)} \\ \Rightarrow\ & \overline{(a+c, b+d)} = \overline{(a+e, b+f)} \\ \Rightarrow\ & a+c+b+f = b+d++a+e \\ \Rightarrow\ & c+f = d+e \quad \text{(Ley de cancelación en } \mathbb{N}) \\ \Rightarrow\ & \overline{(c,d)} = \overline{(e,f)}. \end{aligned}$$

□

Teorema 43 *Ley de cancelación para el producto en $\mathbb{Z}$, es decir*

$$(\forall x \in \mathbb{Z} - \{0\})(\forall y, z \in \mathbb{Z})((x \cdot y = x \cdot z) \Rightarrow y = z).$$

o bien

$$(\forall x, y, z \in \mathbb{Z})((x \cdot y = x \cdot z \wedge x \neq 0) \Rightarrow y = z).$$

Demostración: Sean $x = \overline{(a,b)}, y = \overline{(c,d)}, z = \overline{(e,f)} \in \mathbb{Z}$.

Luego

$$\begin{aligned} & \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a,b)} \cdot \overline{(e,f)} \\ \Rightarrow\ & \overline{(ac+bd, ad+bc)} = \overline{(ae+bf, af+be)} \\ \Rightarrow\ & ac+bd+af+be = ad+bc+ae+bf \\ \Rightarrow\ & a(c+f)+b(d+e) = a(d+e)+b(c+f) \\ \Rightarrow\ & a(c+f)-b(c+f) = a(d+e)-b(d+e) \quad (a > b, \text{ es decir, } a-b \in \mathbb{N}) \\ \Rightarrow\ & (a-b)(c+f) = (a-b)(d+e) \\ \Rightarrow\ & c+f = d+e \\ \Rightarrow\ & \overline{(c,d)} = \overline{(e,f)} \\ \Rightarrow\ & y = z. \end{aligned}$$

□

Observación: ¿En que casos $\overline{(a,b)}$ admite un inverso multiplicativo?
Consideremos $\overline{(a,b)}$ y sea $\overline{(c,d)}$ tal que

$$\begin{array}{rrcl} & \overline{(a,b)}\cdot\overline{(c,d)} & = & \overline{(1,0)} \\ \Leftrightarrow & \overline{(ac+bd,ad+bc)} & = & \overline{(1,0)} \\ \Leftrightarrow & ac+bd & = & ad+bc+1 \\ \Leftrightarrow & ac+bd-ad-bc & = & 1 \\ \Leftrightarrow & a(c-d)-b(c-d)=1 & \vee & b(d-c)-a(d-c)=1 \\ \Leftrightarrow & (a-b)(c-d)=1 & \vee & (b-a)(d-c)=1. \end{array}$$

Ahora bien, tenemos tres casos:

1. $a>b$, entendiendo $a-b\in\mathbb{N}$ luego

$$\begin{array}{rrcl} & (a-b)(c-d) & = & 1 \\ \Rightarrow & a-b=1 & \vee & c-d=1 \\ \Rightarrow & a=b+1 & \vee & c=d+1. \end{array}$$

   Por lo tanto $\overline{(a,b)}=\overline{(b+1,b)}=\overline{(1,0)}$ admite inverso multiplicativo y este es

$$\overline{(c,d)}=\overline{(d+1,d)}=\overline{(1,0)}.$$

2. $a<b$ entonces $b-a\in\mathbb{N}$ luego $(b-a)(d-c)=1$ y en este caso

$$\overline{(a,b)}=\overline{(0,1)}$$

   admite inverso multiplicativo el cual esta dado por

$$\overline{(0,1)}.$$

3. $a=b$ entonces $0=1$ y por lo tanto $\overline{(a,a)}$ con $a\in\mathbb{N}$ no tiene inverso multiplicativo.

Resumiendo tenemos que $\overline{(a,b)}$ admite inverso multiplicativo si

$$\overline{(a,b)}=\overline{(1,0)} \quad \vee \quad \overline{(a,b)}=\overline{(0,1)}.$$

La unidades de $\mathbb{Z}$ es

$$\mathcal{U}(\mathbb{Z})=\{\overline{(1,0)}\ ,\ \overline{(0,1)}\}$$

Identificación con el Sistema de Representante

Con el sistema de representante, se tiene que

$$\begin{array}{rcl} \overline{(n,0)}+\overline{(m,0)} & = & \overline{(n+m,0)} \\ \overline{(n,0)}\cdot\overline{(m,0)} & = & \overline{(n\cdot m,0)} \end{array}$$

Y para los otros tenemos

$$\begin{aligned} \overline{(0,n)} + \overline{(0,m)} &= \overline{(0,n+m)} \\ \overline{(0,n)} \cdot \overline{(0,m)} &= \overline{(n \cdot m, 0)} \end{aligned}$$

Usando lo anterior podemos identificar

$$\overline{(n,0)} = n; \qquad \overline{(0,m)} = -m$$

Con esta identificación se tiene que compatible con la suma y el producto de los números naturales.

A partir de esto, podemos considerar la siguiente correspondencia o contención

$$\begin{aligned} \mathbb{N} &\subset \mathbb{Z} \\ n &\equiv \overline{(n,0)} \end{aligned}$$

Notación: $\mathbb{Z}^+ = \mathbb{N}^*; \quad -\mathbb{N} = \{-n \mid n \in \mathbb{N}\}; \quad \mathbb{Z}^- = -\mathbb{Z}^+.$

Con las notaciones anteriores tenemos

$$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+,$$

además $\mathbb{N} \cap -\mathbb{N} = \{0\}$.

Propiedad 44 *Sean $x \in \mathbb{Z}$ entonces se tiene*

$$x \cdot 0 = 0.$$

Demostración: Sea $x \in \mathbb{Z}$, entonces

$$\begin{aligned} x \cdot 0 &= x \cdot (0+0) \\ x \cdot 0 &= x \cdot 0 + x \cdot 0 \\ 0 &= x \cdot 0 \quad \text{(sumando inverso aditivo de } x \cdot 0). \end{aligned}$$

□

Teorema 45 *Para todo $x, y, z \in \mathbb{Z}$ se verifica:*

1. $x \cdot (-y) = -(x \cdot y)$.
2. $(-x) \cdot y = -(x \cdot y)$.
3. $(-x) \cdot (-y) = x \cdot y$.

Demostración: Sean $x, y, z \in \mathbb{Z}$

1. Consideremos
$$x \cdot y + x \cdot (-y) = x \cdot (y + (-y)) = x \cdot 0 = 0,$$
así tenemos que $x \cdot (-y)$ es el inverso aditivo de $x \cdot y$, lo cual es equivalente a demostrar (1).

2. Análogo al caso (1).

3. De acuerdo a (1) y (2) tenemos (3) como sigue

$$(-x)\cdot(-y) \underbrace{=}_{\text{por (2)}} -(x\cdot(-y)) \underbrace{=}_{\text{por (1)}} -(-(x\cdot y)) = x\cdot y.$$

para la última igualdad, tenga presente que el inverso aditivo de a es $-a$, de otro modo el inverso de $-a$ es a y también $-(-a)$, luego son iguales

Notación: Para $a, b \in \mathbb{Z}$ anotaremos $a+(-b)$ como $a-b$, cuya notación es compatible con la dada anteriormente para el conjunto $\mathbb{N}$.

Teorema 46 *La ecuación $a+x=b$ con $a, b \in \mathbb{Z}$ tiene única solución. La cual esta dada por $x=b-a$.*

Demostración: Sea

$$\begin{array}{rrcll} & a+x & = & b & \\ \Leftrightarrow & (a+x)+(-a) & = & b+(-a) & \text{(sumando el inverso aditivo de } a) \\ \Leftrightarrow & (a+(-a))+x & = & b-a & \\ \Leftrightarrow & 0+x & = & b-a & \\ \Leftrightarrow & x & = & b-a. & \end{array}$$

□

Definición 12 *Sea A un anillo, $x \in A,\ x \neq 0$.*

Se dice que x es un divisor de cero derecho si y sólo si existe $y \in A,\ y \neq 0$ tal que $yx = 0$

Se dice que x es un divisor de cero izquierdo si y sólo si existe $y \in A,\ y \neq 0$ tal que $xy = 0$

Teorema 47 *El anillo $\mathbb{Z}$ no tiene divisores de cero, es decir,*

$$(\forall x, y \in \mathbb{Z})(\ xy = 0 \Rightarrow (x = 0 \vee y = 0)\ )$$

Demostración: Si $x, y \in \mathbb{N}$, por teorema 31, la propiedad se cumple.

Supongamos ahora $x \in \mathbb{N}, y \in -\mathbb{N}$, luego tenemos $-y = z \in \mathbb{N}$.

$$xz = x(-y) = -(xy) = -0 = 0$$

Por la primera parte tenemos que $x = 0 \vee z = 0$, como $-y = z = 0$ entonces $y = 0$. Por lo tanto

$$x = 0 \vee y = 0$$

Los otros caso son similares. □

2.2. Orden en $\mathbb{Z}$

Definición 13 *Sean $x, y \in \mathbb{Z}$*

Se dice que x es menor o igual que y si y sólo si existe $n \in \mathbb{N}$ tales que $x + n = y$, es decir,

$$(x \leq y) \Leftrightarrow (\exists n \in \mathbb{N})(x + n = y)$$

de modo equivalente

$$(x \leq y) \Leftrightarrow (y - x \in \mathbb{N}).$$

Teorema 48 *La relación "$\leq$" es una relación de orden en $\mathbb{Z}$.*

Demostración: Sean $x, y, z \in \mathbb{Z}$
Refleja:

$$x \leq x \text{ pues } x - x = 0 \in \mathbb{N}.$$

Antisimétrica: Supongamos $x \leq y$ e $y \leq x$, es decir $y - x \in \mathbb{N}$ y $x - y \in \mathbb{N}$, puesto que

$$(x - y) + (y - x) = x + ((-y) + y) + (-x) = 0$$

tenemos que

$$x - y = -(y - x)$$

de esto

$$y - x \in \mathbb{N} \quad \wedge \quad y - x \in -\mathbb{N}$$

es decir,

$$y - x \in (\mathbb{N} \cap -\mathbb{N}),$$

pero

$$\mathbb{N} \cap -\mathbb{N} = \{0\},$$

de otro modo

$$y - x \in \{0\},$$

esto es

$$y - x = 0 \Leftrightarrow x = y.$$

Transitiva: Supongamos $x \leq y$ e $y \leq z$, es decir, $y - x \in \mathbb{N}$ y $z - y \in \mathbb{N}$, ahora bien como

$$(y - x) + (z - y) \in \mathbb{N}$$

pero

$$(y - x) + (z - y) = z - x$$

tenemos entonces que

$$z - x \in \mathbb{N}$$

con lo cual

$$x \leq z.$$

□

Teorema 49 *La relación "$\leq$" es compatible con la suma $(+)$ y el producto $(\cdot)$ en $\mathbb{Z}$, esto es:*

1. $(\forall x, y \in \mathbb{Z})(\forall z \in \mathbb{Z})(\, x \leq y \;\Rightarrow\; x + z \leq y + z\,)$.
2. $(\forall x, y \in \mathbb{Z})(\forall z \in \mathbb{N})(\, x \leq y \;\Rightarrow\; x \cdot z \leq y \cdot z\,)$.
3. $(\forall x, y \in \mathbb{Z})(\forall z \in -\mathbb{N})(\, x \leq y \;\Rightarrow\; x \cdot z \geq y \cdot z\,)$.

Demostración: Sea $x, y, z \in \mathbb{Z}$

1. Supongamos $x \leq y$, ahora bien

$$\begin{array}{ll} & x \leq y \\ \Rightarrow & y - x \in \mathbb{N} \\ \Rightarrow & (y - x) + (z - z) \in \mathbb{N} \\ \Rightarrow & (y + z) - (x + z) \in \mathbb{N} \\ \Rightarrow & x + z \leq y + z. \end{array}$$

2. Supongamos $x \leq y$ e $z \in \mathbb{N}$

$$\begin{array}{ll} & x \leq y \;\wedge\; z \in \mathbb{N} \\ \Rightarrow & y - x \in \mathbb{N} \;\wedge\; z \in \mathbb{N} \\ \Rightarrow & (y - x) \cdot z \in \mathbb{N} \\ \Rightarrow & y \cdot z - x \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z \leq y \cdot z. \end{array}$$

3. Supongamos $x \leq y$ e $z \in -\mathbb{N}$

$$\begin{array}{ll} & x \leq y \;\wedge\; z \in -\mathbb{N} \\ \Rightarrow & y - x \in \mathbb{N} \;\wedge\; (-z) \in \mathbb{N} \\ \Rightarrow & (y - x) \cdot (-z) \in \mathbb{N} \\ \Rightarrow & -y \cdot z + x \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z - y \cdot z \in \mathbb{N} \\ \Rightarrow & x \cdot z \geq y \cdot z. \end{array}$$

□

2.3. Divisibilidad

Dada dos rueda dentada, una con 54 diente y la otra con 28 diente, inicia su giro después de ¿cuántas vueltas como mínimo debe girar de modo que vuelva a la posición origina o de partida?

En esta sección debemos tener presente en forma especial el Principio de Inducción Teorema 34 y Principio del Buen Orden Teorema 33

Definición 14 *Sean $a, b \in \mathbb{Z}$, $a \neq 0$.*
Diremos que "a" divide a "b", si existe $q \in \mathbb{Z}$ tal que

$$b = aq.$$

Notación: a divide a b, se denota por $a|b$, y cuando a no divide a b, se denota por $a \nmid b$.

Teorema 50 *Sean $a, b, c \in \mathbb{Z}$*

1. *Si $a|b$ entonces $(\forall c \in \mathbb{Z})(a|bc)$.*
2. *Si $(a|b \wedge b|c)$ entonces $a|c$.*
3. *Si $(a|b \wedge a|c)$ entonces $(\forall m, n \in \mathbb{Z})(a|(mb + nc))$.*
4. *Si $(a|b \wedge b|a)$ entonces $(a = b \vee a = -b)$.*
5. *Si $(a|b \wedge a > 0 \wedge b > 0)$ entonces $a \leq b$.*

Notación: La expresión $a = \pm b$ significa $(a = b \vee a = -b)$.

Demostración: Demostraremos sólo (3) y (5), quedando las demás como ejercicio.

(3) Si $a|b$ y $a|c$ entonces existen $q, q' \in \mathbb{Z}$ tal que

$$b = aq \quad \wedge \quad c = aq'. \tag{2.1}$$

Sean $n, m \in \mathbb{Z}$ y notemos que por (2.1)

$$\begin{aligned} mb + nc &= m(aq) + n(aq') \\ &= a(mq + nq'), \end{aligned}$$

ahora bien, definiendo $s = mq + nq' \in \mathbb{Z}$, tenemos que $mb + nc = as$, es decir, $a|(mb + nc)$.

(5) Si $a|b$ entonces existe $q \in \mathbb{Z}$ tal que

$$b = aq.$$

Ahora como $a > 0$ y $b > 0$, se tiene que q es positivo, más aún $q \geq 1$, luego

$$b - a = aq - a = a(q - 1) \geq 0,$$

es decir,

$$b - a \geq 0 \Leftrightarrow b \geq a.$$

Ejemplo 15 *Demostrar que*

$$(\forall n \in \mathbb{N})(6|(n^3 - n))$$

Solución: La demostración la realizaremos usando el principio de inducción.

Definamos la función proposicional $p(n) = 6|(n^3 - n)$

Primer paso: $p(0) = 6|0$, verdadero.

Segundo paso: Supongamos $p(n) = 6|(n^3 - n)$ es verdadero, es decir, existe $k \in \mathbb{Z}$, tal que $n^3 - n = 6k$.

Por demostrar que $p(n+1)$ es verdadero. Lo cual significa que $6|((n+1)^3 - (n+1))$, lo cual es equivalente a demostrar $(n+1)^3 - (n+1) = 6 \cdot q; \quad \text{con } q \in \mathbb{Z}$.

Para ello veamos lo siguiente:

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3 \cdot n^2 + 3 \cdot n + 1 - n - 1 \\ &= n^3 - n + 3 \cdot n^2 + 3 \cdot n \\ &= 6 \cdot k + 3 \cdot n \cdot (n+1)\end{aligned}$$

Pero de la suma de los primeros n naturales obtenemos que $(\forall n \in \mathbb{N})(2|n \cdot (n+1))$ que se puede reescribir del siguiente modo $(\forall n \in \mathbb{Z})(\exists r \in \mathbb{Z})(n \cdot (n+1) = 2 \cdot r)$, queda como ejercicio su demostración, reemplazando este resultado, tenemos

$$\begin{aligned}(n+1)^3 - (n+1) &= 6 \cdot k + 3 \cdot 2 \cdot r \\ &= 6 \cdot k + 6 \cdot r \\ &= 6 \cdot (k + r)\end{aligned}$$

Luego

$$6|((n+1)^3 - (n+1))$$

y por teorema de inducción, obtenemos

$$(\forall n \in \mathbb{N})(6|(n^3 - n)).$$

Ejercicio 16 *Demostrar*

$$(\forall n \in \mathbb{Z})(\ 2|n \cdot (n+1))$$

Teorema 51 (Algoritmo de la División) *Sean $a, b \in \mathbb{Z}, a > 0$. Entonces existen únicos enteros q y r tales que:*

$$b = qa + r,$$

donde $0 \leq r < a$.

Además si $a \nmid b$ entonces $0 < r < a$.

Demostración: Consideremos el conjunto

$$A = \{b - qa \mid q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Como $a, b \in \mathbb{Z}$ se tiene tres caso y verificando cada uno de ello se comprueba que el conjunto es no vacío.

Luego por el Teorema Buen Orden (33) existe un elemento mínimo de A, el cual llamaremos r. Por definición de A, se tiene que $r \geq 0$.

Supongamos que $r \geq a$, entonces

$$r = b - qa \geq \quad a,$$

de donde $b - (q+1)a \geq 0$, es decir, $b - (q+1)a \in A$.

Ahora bien como

$$b - (q+1)a \leq b - qa = r,$$

se tiene que r no es el menor elemento de A, lo cual es una contradicción, por lo tanto $r < a$ y en consecuencia que

$$0 \leq r < a.$$

Para mostrar la unicidad de q y r, supongamos que existe otro par de elementos q' y r' que satisfacen las hipótesis del teorema. Tenemos entonces que $aq + r - aq' - r' = 0$, luego $a(q - q') = r' - r$, es decir, $a|(r' - r)$. Ahora bien si $r' \neq r$, por el teorema (50) parte (5), se tiene que $(r' - r) \geq a > 0$, lo cual es una contradicción pues $-a < r' - r < a$, por lo tanto $r' = r$. Pero entonces $a(q - q') = 0$ y $a \neq 0$, así $q = q'$.

Corolario 52 *Sean a, x enteros positivos, con $a > 1$. Entonces x tiene una única representación de la forma*

$$x = b_0 + b_1 a + \cdots b_n a^n,$$

con $n \geq 0$, $0 < b_n < a$ y $0 \leq b_i < a$, para $0 \leq i \leq n-1$.

Demostración: Usaremos inducción sobre la existencia de la representación de x.

Si $x = 1$, tomamos $b_0 = 1$ y $n = 0$ y el resultado es válido.

Supongamos que cualquier entero $m < x$, puede ser representado de manera única en la forma

$$r_0 + r_1 a + \cdots + r_k a^k,$$

donde $0 < r_i < a, 0 \leq i \leq k$ y $r_k > 0$.

Por el algoritmo de la división $x = qa + r$ con $0 \leq r < a$.

Si $q \geq x$, amplificando por a obtenemos $aq \geq ax$ pero $ax > x$, luego tenemos que $aq > x$ sumando r obtenemos $aq + r > x + r \geq x$ lo cual es imposible. Por lo tanto, $q < x$

Veamos ahora, si $q = 0$, tenemos que

$$x = r + 0 \cdot a,$$

luego obtenemos la representación que buscada, es decir, $p(x)$ es verdadero .

Finalmente, falta el caso que $0 < q < x$.

Por hipótesis de inducción tenemos que, existen k, $0 \leq r_i < a$ y $0 < r_k$ tales que

$$q = r_0 + r_1 a + \cdots r_k a^k.$$

Entonces, reemplazando se tiene

$$x = aq + r = r_k a^{k+1} + \cdots r_0 a + r,$$

haciendo un cambio de indices apropiado, obtenemos que

$$x = b_0 + b_1 a + \cdots b_n a^n.$$

Luego existe la representación

Ahora para demostrar la unicidad de esta representación, supongamos que existe otra representación, es decir

$$x = b_0 + b_1 a + \cdots + b_n a^n = c_0 + c_1 a + \cdots + c_j a^j,$$

tenemos entonces que

$$0 = h_0 + h_1 a + \cdots + h_s a^s,$$

donde $|h_i| < a$, para $0 \leq i \leq s,\ h_s \neq 0, s \geq 0$.

Ahora bien como $|h_i| < a$, entonces $|h_i| \leq a - 1$ y así

$$\begin{aligned} a^s &\leq |h_s a^s| \\ &= |h_o + h_1 a + \cdots + h_{s-1} a^{s-1}| \\ &\leq |h_0| + |h_1| a + \cdots + |h_{s-1}| a^{s-1} \\ &\leq (a-1) + (a-1)a + \cdots + (a-1)a^{s-1} \\ &= (a-1)(1 + a + \cdots + a^{s-1}) \\ &= a^s - 1 \end{aligned}$$

lo cual es una contradicción y en consecuencia se tiene al unicidad. □

2.3.1. Representaciones de Números Enteros

$$\begin{aligned} 122 &= 3 \cdot 40 + 2 \\ 40 &= 3 \cdot 13 + 1 \\ 13 &= 3 \cdot 4 + 1 \\ 4 &= 3 \cdot 1 + 1 \\ 1 &= 3 \cdot 0 + 1 \end{aligned}$$

$$\begin{aligned} 122 &= 3 \cdot 40 + 2 \\ &= 3 \cdot (3 \cdot 13 + 1) + 2 \\ &= 3^2 \cdot 13 + 1 \cdot 3 + 2 \\ &= 3^2(3 \cdot 4 + 1) + 1 \cdot 3 + 2 \\ &= 3^3 \cdot 4 + 1 \cdot 3^2 + 1 \cdot 3 + 2 \\ &= 3^3(3 \cdot 1 + 1) + 1 \cdot 3^2 + 1 \cdot 3 + 2 \end{aligned}$$

Luego

$$\begin{aligned} 122 &= 1 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3 + 2 \\ 122 &= (1\ 1\ 1\ 1\ 2)_3 \quad \text{(base 3)} \\ 122 &= 1 \cdot 10^2 + 2 \cdot 10 + 2 = (122)_{10} \quad \text{(base 10)} \end{aligned}$$

Veamos ahora el 7 en base 3

$$7 = 2 \cdot 3^1 + 1 \cdot 3^0$$

Al sumar $\begin{array}{r} (1\ 1\ 1\ 1\ 2)_3 \\ +\quad\quad (2\ 1)_3 \\ \hline (1\ 1\ 2\ 1\ 0)_3 \end{array}$ Verificando con las potencias tenemos

$$\begin{aligned}
&(1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2)+(2\cdot 3+1)\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+(1+2)3\cdot 3\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+(3+1)3+0\\
&1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3^2+1\cdot 3+0\\
&1\cdot 3^4+1\cdot 3^3+(1+1)3^2+1\cdot 3+0\\
&1\cdot 3^4+1\cdot 3^3+2\cdot 3^2+1\cdot 3+0
\end{aligned}$$

Ahora revisemos la multiplicación

$$(1\ 1\ 1\ 1\ 2)_3\times(2\ 1)_3=(1\ 0\ 1\ 1\ 1\ 2\ 2)_3$$

$$\begin{array}{r} \underline{1\ 1\ 1\ 1\ 2}\times 2\ 1 \\ 1\ 1\ 1\ 1\ 2 \\ \underline{1\ 0\ 0\ 0\ 0\ 1\ \ } \\ (1\ 0\ 1\ 1\ 1\ 2\ 2)_3 \end{array}$$

Con la aritmética habitual.

$$\begin{array}{rcl} (1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2) & \times & (2\cdot 3+1) \\ 1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+1\cdot 3+2 & & \\ \underline{2\cdot 3^5+2\cdot 3^4+2\cdot 3^3+2\cdot 3^2+4\cdot 3} & & \\ 2\cdot 3^5+3\cdot 3^4+3\cdot 3^3+3\cdot 3^2+5\cdot 3+2 & & \\ 1\cdot 3^6+0\cdot 3^5+1\cdot 3^4+1\cdot 3^3+1\cdot 3^2+2\cdot 3+2 & & \end{array}$$

2.4. Regla de Divisibilidad

Debemos tener presente que todo natural se puede escribir en base 10 en forma única, corolario 52

$$n=a_ma_{m-1}a_{m-2}\dots a_1a_0=a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110+a_0$$

donde los a_i son dígitos.

Además recordemos el corolario $a|n\wedge a|y\Rightarrow a|(n-y)$, que en nuestro caso lo aplicaremos para $n=x+y$, es decir $n|x$

2.4.1. Divisibilidad por 2

Dado $n=a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110+a_0$, con los a_i dígitos.

Además se tiene que $2|10^i$, para todo $i>0$.

Luego se tiene que

$$2|(a_m10^m+a_{m-1}10^{m-1}+a_{m-2}10^{m-2}+\cdots+a_110).$$

de lo cual se tiene

Propiedad 53 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$2|n \Leftrightarrow 2|a_0 \Leftrightarrow a_0 \text{ es par}$$

Ejemplo 17 *El número* $n = 8334216$ *es divisible por* 2*, ya que* $a_0 = 6$ *número par.*

2.4.2. Divisibilidad por 3

Dado $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar por inducción que $3|(10^i - 1)$, para todo $i > 0$.
Luego se tiene que

$$3|(a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + a_{m-2}(10^{m-2} - 1) + \cdots + a_1(10 - 1))$$

además

$$n = (a_m + a_{m-1} + \cdots + a_1 + a_0) + (a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + \cdots + a_1(10 - 1))$$

de lo cual se tiene

Propiedad 54 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$3|n \Leftrightarrow 3|(a_m + a_{m-1} + a_{m-2} + \cdots + a_1 + a_0)$$

Ejemplo 18 *El número* $n = 134718$ *es divisible por* 3*, ya que* $1 + 3 + 4 + 7 + 1 + 8 = 24$ *es divisible por* 3*.*

2.4.3. Divisibilidad por 4

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $4|10^i$, con $i > 1$ y además se tiene que $10 = 4 \cdot 2 + 2$. De lo cual se obtiene

$$4|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 8)$$

además

$$n = (2a_1 + a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 8)$$

de lo cual se tiene

Propiedad 55 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$4|n \Leftrightarrow 4|(2a_1 + a_0)$$

Ejemplo 19 *El número* $n = 231528$ *es divisible por* 4*, ya que* $2 \cdot 2 + 8 = 12$ *es divisible por* 4*.*

2.4.4. Divisibilidad por 5

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $5|10^i$, con $i > 0$.
De lo cual se obtiene

$$5|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10)$$

además

$$n = (a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10)$$

de lo cual se tiene

Propiedad 56 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$5|n \Leftrightarrow 5|a_0$$

Ejemplo 20 *El número* $n = 5689425$ *es divisible por* 5*, ya que* 5 *es divisible por* 5*.*

2.4.5. Divisibilidad por 6

Propiedad 57 *Sea* $n \in \mathbb{N}^*$*, luego*

$$6|n \;\Leftrightarrow\; 2|n \wedge 3|n$$

2.4.6. Divisibilidad por 8

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que: $8|10^i$, con $i > 2$ y además $10^2 = 8 \cdot 12 + 4$, $10 = 8 \cdot 1 + 2$. De lo cual se obtiene

$$8|(a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} \cdots + a_2 96 + a_1 8)$$

además

$$n = (4a_2 + 2a_1 + a_0) + (a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_2 96 + a_1 8)$$

de lo cual se tiene

Propiedad 58 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$8|n \Leftrightarrow 8|(4a_2 + 2a_1 + a_0)$$

Ejemplo 21 *El número* $n = 231528$ *es divisible por* 8*, ya que* $4 \cdot 5 + 2 \cdot 2 + 8 = 32$ *es divisible por* 8*.*

2.4.7. Divisibilidad por 9

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Es fácil demostrar que $9|(10^i - 1)$, con $i > 0$.
De lo cual se obtiene

$$9|(a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + a_{m-2}(10^{m-2} - 1) + \cdots + a_1 9)$$

además

$$n = (a_m + a_{m-1} + \cdots + a_1 + a_0) + (a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + \cdots + a_1 9)$$

de lo cual se tiene

Propiedad 59 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$9|n \Leftrightarrow 9|(a_m + a_{m-1} + a_{m-2} + \cdots + a_1 + a_0)$$

Ejemplo 22 *El número* $n = 245718$ *es divisible por* 3, *ya que* $2 + 4 + 5 + 7 + 1 + 8 = 27$ *es divisible por* 9.

2.4.8. Divisibilidad por 11

Sea $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$, con los a_i dígitos.
Se sabe que $11|(10^i - (-1)^i)$, para todo $i \geq 0$. De lo cual se obtiene

$$9|(a_m(10^m - (-1)^m) + a_{m-1}(10^{m-1} - (-1)^{m-1}) + \cdots + a_1(10 + 1))$$

además

$$n = (a_m(-1)^m + \cdots + a_1(-1)^1 + a_0) + (a_m(10^m - (-1)^m) + \cdots + a_1(10 + 1))$$

de lo cual se tiene

Propiedad 60 *Sea* $n = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 \in \mathbb{N}$

$$11|n \Leftrightarrow 11|(a_m(-1)^m + a_{m-1}(-1)^{m-1} + a_{m-2}(-1)^{m-2} + \cdots + a_2(-1)^2 + a_1(-1)^1 + a_0)$$

Ejemplo 23 *El número* $n = 245718$ *es divisible por* 11, *ya que* $-2 + 4 - 5 + 7 - 1 + 8 = 11$ *es divisible por* 11.

2.5. Máximo Común Divisor

Definición 15 (Divisor Común) *Sean* $a, b, c \in \mathbb{Z}$.

Se dice que a *es un divisor común de* b *y* c *si y sólo si* $a|b$ *y* $a|c$.

En general dados $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, *se dice que* a *es divisor común de* $x_1, x_2, \ldots, x_n$ *si y sólo si* $a|x_1 \wedge a|x_2 \wedge \cdots \wedge a|x_n$.

Definición 16 (Máximo Común Divisor) *Sean a, b dos enteros no nulos. El máximo común divisor entre a y b es el mayor divisor común positivo de a y b, el cual denotaremos por (a, b).*

En general dados $x_1, x_2, \ldots, x_n \in \mathbb{Z}^*$, el máximo común divisor de $x_1, x_2, \ldots, x_n$ es el mayor divisor común de $x_1, x_2, \cdots, x_n$, el cual denotamos por $(x_1, x_2, \ldots, x_n)$

Teorema 61 (Bézout) *Sean a, b dos enteros no nulos.*

Si $g = (a, b)$, entonces existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$g = ax_0 + by_0.$$

Demostración: Consideremos el conjunto

$$A = \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}^*.$$

La considerar $x = a$, e $y = b$, el conjunto es no vacío, luego por el Teorema del Buen Orden (33). El conjunto A posee un primer elemento, el que denotaremos por d.

Ahora bien como $d \in A$, se tiene que existen enteros x_0, y_0 tales que $d = ax_0 + by_0$, luego por el algoritmo de la división $a = qd + r$, con $0 \leq r < d$. Entonces,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Si $r > 0$ entonces $r \in A$, pero $r < d$, lo cual contradice la minimalidad de d, por lo tanto $d|a$. Análogamente se demuestra que $d|b$ y así se obtiene que d es un divisor común de a y b.

Para verificar que d es el mayor divisor común positivo de a y b, sea $t \geq 1$ otro divisor común. Por el teorema (50) parte (3), $t|(ax + by)$, para cualquier $x, y \in \mathbb{Z}$, en particular $t|d$, luego $0 < t \leq d$. □

Corolario 62 *Sean $a, b \in \mathbb{Z}^*$ entonces*

1. $(a, b) = \text{mín}\{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}^*$.
2. $(a, b) = (|a|, |b|)$.

Teorema 63 *Sean $a, b, c \in \mathbb{Z}^*$, tales que $a|b$ y $a|c$, entonces $a|(b, c)$*

Demostración: Si $a|b$ y $a|c$, entonces por el teorema (50) parte (3) tenemos que $a|(mb+nc)$, para cualquier par de enteros n, m y luego por el teorema (61), se tiene que $a|(b, c)$ □

Corolario 64 *Sean $a_1, a_2, \cdots, a_n \in \mathbb{Z}^*$ entonces*

1. $(a_1, a_2, \cdots, a_n) = (a_1, (a_2, \cdots, a_n))$.
2. *Existen $x_1, x_2, \cdots, x_n \in \mathbb{Z}$ tales que*

$$(a_1, a_2, \cdots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Teorema 65 *Para todo $a, b \in \mathbb{Z}^*$, $m \in \mathbb{Z}^+$, se tiene que*

$$(ma, mb) = m(a, b)$$

Demostración: Del corolario (62) tenemos que:

$$\begin{aligned}(ma, mb) &= \text{mín}\{(ma)x + (mb)y > 0 \mid x, y \in \mathbb{Z}\} \\ &= \text{mín}\{m(ax + by) > 0 \mid x, y \in \mathbb{Z}\} \\ &= m \cdot \text{mín}\{ax + by > 0 \mid x, y \in \mathbb{Z}\} \\ &= m(a, b).\end{aligned}$$

□

Ejercicio 24 *Sean $a \in \mathbb{Z}^+$, $b \in \mathbb{Z}^*$ entonces*

$$(a, ab) = a(1, b) = a$$

Corolario 66 *Si $d|a$ y $d|b$, $d > 0$, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

En particular se tiene que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

Demostración: El resultado es consecuencia directa del teorema (65) tomando

$$m = d, a = \frac{a}{d} \text{ y } b = \frac{b}{d}.$$

□

Corolario 67 *Si $c|ab$ y $(b, c) = 1$, entonces $c|a$.*

Demostración: Por el teorema (65), tenemos que

$$(ab, ac) = a(b, c) = a. \tag{2.2}$$

Ahora bien como $c|ab$ y $c|ac$, por el teorema (63) tenemos que $c|(ab, ac)$, pero de (2.2) se tiene que $c|a$. □

Definición 17 *Sean a, b dos enteros no ambos nulos. Se dice que a y b son primos relativos si y sólo si $(a, b) = 1$.*

Teorema 68 *Sean a, b, c enteros no ambos nulos. Si $(a, c) = 1$ y $(b, c) = 1$, entonces $(ab, c) = 1$.*

Demostración: Si $(a, c) = 1$ y $(b, c) = 1$, por el teorema (61) obtenemos que existen enteros x_0, x_1, y_0, y_1 tales que

$$\begin{aligned}ax_0 + cy_0 &= 1 \\ bx_1 + cy_1 &= 1,\end{aligned}$$

de donde se obtiene que

$$(ab)(x_0x_1) + c(y_1 + y_0 - cy_0y_1) = 1. \tag{2.3}$$

Por otro lado, sabemos que $(ab, c)|ab$ y $(ab, c)|c$. Luego por el teorema (50) parte (3) se tiene que $(ab, c)|(abx + cy)$, para todo $x, y \in \mathbb{Z}$, en particular para $x = x_0x_1$ e $y = y_1 + y_0 - my_0y_1$. Así

$$(ab, c)|((ab)(x_0x_1) + c(y_1 + y_0 - my_0y_1)),$$

pero por (2.3) obtenemos que $(ab, c)|1$ y en consecuencia que $(ab, c) = 1$. □

Teorema 69 *Para todo $a, b \in \mathbb{Z}^*$, $k \in \mathbb{Z}$, se tiene que*

$$(a, b) = (a, b + ak).$$

Demostración: En primer lugar notemos que $(a, b)|a$ y $(a, b)|b$, ahora bien, por el teorema (50) parte (1), se tiene que $(a, b)|ak$, para todo $k \in \mathbb{Z}$, tenemos así que $(a, b)|ak$ y $(a, b)|b$, luego por el teorema (50) parte (3) obtenemos que $(a, b)|(b + ak)$. De lo anterior tenemos que $(a, b)|a$ y $(a, b)|b + ak$ y por lo tanto

$$(a, b)|(a, b + ak). \tag{2.4}$$

Por otro lado $(a, b + ak)|a$ y $(a, b + ak)|b + ak$, por el teorema (50) parte (1), se tiene que $(a, b + ak)|ak$, para todo $k \in \mathbb{Z}$. En virtud del teorema (50) parte (3), obtenemos que $(a, b + ak)|(b + ak - ak)$. Luego se tiene que $(a, b + ak)|b$ y $(a, b + ak)|a$, con lo cual

$$(a, b + ak)|(a, b). \tag{2.5}$$

Ahora de (2.4) y (2.5) se tiene que $(a, b) = (a, b + ak)$. □

Ejemplo 25 *Calcular $(45, 18)$ y $(72, 15)$*

Solución: En el primer caso

$$(45, 18) = (45 - 18 \cdot 2, 18) = (9, 18) = (9, 9 \cdot 2) = 9(1, 2) = 9.$$

Ene segundo

$$(72, 15) = (72 - 60, 15) = (12, 15) = (12, 3) = 3.$$

♡

Teorema 70 (Algoritmo de Euclides) *Sean a y b enteros, con $a > 0$. Aplicando repetidamente el teorema (51), obtenemos la siguiente secuencia de ecuaciones:*

$$\begin{aligned}
b &= aq_1 + r_1, \quad 0 < r_1 < a \\
a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\
&\vdots \\
r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1} \\
r_{j-1} &= r_jq_{j+1.}
\end{aligned}$$

Entonces $(a,b) = r_j$, resto inmediatamente anterior al resto que se anula. Además los valores de x_0 e y_0 tales que

$$(a,b) = ax_0 + by_0$$

pueden ser obtenidos de $r_{j-1}, \ldots, r_2, r_1$ en esta secuencia de ecuaciones.

Demostración: es inmediata de teorema 69, ya que

$$(b,a) = (b - aq_1, a) = (r_1, a) = (r_1, r_2) = \cdots = (r_j, r_{j_1}) = r_j(1, q_{j+1})$$

La segunda parte se obtiene, al despejar los restos y reemplazando recursivamente se obtiene el resultado deseado □

Observación: Veamos el despeje en un ejemplo pequeño. El cálculo anterior se realiza despejando y reemplazando, para ello lo haremos en el siguiente ejemplo

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < a \\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= r_3q_4 + 0 \end{aligned}$$

$$\begin{aligned} r_3 &= r_1 - r_2q_3 \text{ reemplazo } r_2 \\ &= r_1 - (a \cdot 1 - r_1q_2)q_3 \text{reordenado} \\ &= a \cdot (-q_3) + r_1(1 + q_2q_3) \text{ reemplazo } r_1 \\ &= a \cdot (-q_3) + (b - aq_1)(1 + q_2q_3) \text{reordenado} \\ &= a(-q_3 - q_1 - q_1q_2q_3) + b(1 + q_2q_3) \end{aligned}$$

de otro modo

$$\begin{pmatrix} b & 1 & 0 \\ a & 0 & 1 \end{pmatrix} \underset{F_{21}(-q_1)}{\sim} \begin{pmatrix} r_1 & 1 & -q_1 \\ a & 0 & 1 \end{pmatrix} \underset{F_{12}(-q_2)}{\sim} \begin{pmatrix} r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1 + q_1q_2 \end{pmatrix}$$

$$\underset{F_{21}(-q_3)}{\sim} \begin{pmatrix} r_3 & 1 + q_2q_3 & -q_1 - q_3 - q_1q_2q_3 \\ r_2 & -q_2 & 1 + q_1q_2 \end{pmatrix} \underset{F_{12}(-q_4)}{\sim} \begin{pmatrix} r_3 & 1 + q_2q_3 & -q_1 - q_3 - q_1q_2q_3 \\ 0 & * & * \end{pmatrix}$$

Ejemplo 26 *Encontrar el máximo común divisor (MCD) en cada caso*

a) $(5, 19)$ Apliquemos el algoritmo de la división

$$\begin{aligned} 19 = 5 \cdot 3 + 4 \quad &\text{o bien} \quad 4 = 19 - 5 \cdot 3 \\ 5 = 4 \cdot 1 + 1 \quad &\text{o bien} \quad 1 = 5 - 4 \cdot 1 \\ 4 = 1 \cdot 4 + 0 \end{aligned}$$

Por lo tanto $(5, 19) = 1$. Además

$$1 = 5(1) - 4(1) = 5(1) - (19 - 5 \cdot 3)(1) = 19(-1) + 5(1 + 3) = 19(-1) + 5(4)$$

b) $(2,5,19)$ Para ello $(2,5,19) = (2,(5,19)) = (2,1) = 1$ Por lo tanto $(2,5,19) = 1$

c) $(5748,-7207)$

Para determinar el MCD no se considera los signos corolario 62.

$$\begin{aligned}
7207 &= 5748\cdot 1 + 1459 \quad \text{o bien} \quad 1459 = 7207 - 5748\cdot 1\\
5748 &= 1459\cdot 3 + 1371 \quad \text{o bien} \quad 1371 = 5748 - 1459\cdot 3\\
1459 &= 1371\cdot 1 + 88 \quad \text{o bien} \quad 88 = 1459 - 1371\cdot 1\\
1371 &= 88\cdot 15 + 51 \quad \text{o bien} \quad 51 = 1371 - 88\cdot 15\\
88 &= 51\cdot 1 + 37 \quad \text{o bien} \quad 37 = 88 - 51\cdot 1\\
51 &= 37\cdot 1 + 14 \quad \text{o bien} \quad 14 = 51 - 37\cdot 1\\
37 &= 14\cdot 2 + 9 \quad \text{o bien} \quad 9 = 37 - 14\cdot 2\\
14 &= 9\cdot 1 + 5 \quad \text{o bien} \quad 5 = 14 - 9\cdot 1\\
9 &= 5\cdot 1 + 4 \quad \text{o bien} \quad 4 = 9 - 5\cdot 1\\
5 &= 4\cdot 1 + 1 \quad \text{o bien} \quad 1 = 5 - 4\cdot 1\\
4 &= 1\cdot 4
\end{aligned}$$

Por lo tanto $(5748,-7207) = 1$

Observación: La aritmética anterior se puede reescribir del siguiente modo

$$\begin{pmatrix} 7207 & 1 & 0\\ 5748 & 0 & 1\end{pmatrix} \underset{F_{21}(-1)}{\sim} \begin{pmatrix} 1459 & 1 & -1\\ 5748 & 0 & 1\end{pmatrix} \underset{F_{12}(-3)}{\sim} \begin{pmatrix} 1459 & 1 & -1\\ 1371 & -3 & 4\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 88 & 4 & -5\\ 1371 & -3 & 4\end{pmatrix} \underset{F_{12}(-15)}{\sim} \begin{pmatrix} 88 & 4 & -5\\ 51 & -63 & 79\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 37 & 67 & -84\\ 51 & -63 & 79\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 37 & 67 & -84\\ 14 & -130 & 163\end{pmatrix}$$
$$\underset{F_{21}(-2)}{\sim} \begin{pmatrix} 9 & 327 & -410\\ 14 & -130 & 163\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 9 & 327 & -410\\ 5 & -457 & 573\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 4 & 784 & -983\\ 5 & -457 & 573\end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 4 & 784 & -983\\ 1 & -1241 & 1556\end{pmatrix}$$
$$\underset{F_{21}(-1)}{\sim} \begin{pmatrix} 0 & * & *\\ 1 & -1241 & 1556\end{pmatrix}$$

Note que

$$(-1241)\cdot(7207) + (1556)\cdot(5748) = 1 \text{ o bien } (1241)\cdot(-7207) + (1556)\cdot(5748) = 1$$

2.6. Números Primos

Definición 18 *Sea $p \in \mathbb{Z}$, tal que $p \notin \{-1,0,1\}$*

Se dice que p es número primo, si y sólo si los únicos divisores dde él son ± 1 y $\pm p$. En caso contrario se dice que p es un número compuesto.

Ejemplo 27 *Algunos primos positivos son*

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31, \cdots$$

No se conoce la formula general de esta sucesión, pero son infinitos.

Propiedad 71 *Sean $a, b, p \in \mathbb{Z}^*$, tal que p es primo*

$$\textit{Si } p|ab \textit{ entonces } p|a \textit{ o } p|b$$

Demostración: Si p divide a a listo. Por ello suponemos que p no divide a a, entonces p y a son primos relativos y por la Teorema 61 existen x e y enteros tales que $px + ay = 1$. Multiplicando por b se obtiene $pbx + aby = b$, y puesto que los dos sumandos del lado izquierdo son divisibles por p, el término de la derecha también es divisible por p. □

Teorema 72 (Fundamental de la Aritmética) *Todo numero entero positivo mayor que uno, puede ser escrito como producto de números primos positivos. Más aún, dicha factorización es única salvo el orden de los factores.*

Demostración:

Existencia de la descomposición: Suponemos que existe algún entero positivo que no puede representarse como producto de primos. Entonces debe haber un mínimo número n con esa propiedad (principio del Buen Orden). Este número n no puede ser 1, por la convención anterior. Tampoco puede ser un primo, porque todo primo es el producto de un único número primo: él mismo. Así pues, $n = ab$, donde a y b son enteros positivos menores que n. Como n es el mínimo entero positivo para el que falla el teorema, tanto a como b pueden escribirse como producto de primos. Pero entonces $n = ab$ también puede escribirse como producto de primos, lo que es contradictorio.

Unicidad de la descomposición: Dados dos productos de primos que tengan igual resultado, tómese un primo p del primer producto. Divide al primer producto, y por lo tanto también al segundo. Por la propiedad anterior, p debe dividir al menos a un factor del segundo producto; pero los factores son todos primos, así que p debe ser igual a uno de los factores del segundo producto. Se puede entonces cancelar a p de ambos productos. Siguiendo de esta forma se cancelarán todos los factores de ambos productos, con lo cual éstos deben coincidir exactamente □

Teorema 73 *Existen infinitos números primos.*

Demostración: Supongamos que existe sólo una cantidad finita de números primos, digamos $p_1, p_2, \ldots, p_n$.

Consideremos el número

$$P = p_1 \cdot p_2 \cdots p_n + 1.$$

Es claro que $P > p_j$, para $1 \leq j \leq n$, luego P no es primo. Por otra parte P no es divisible por ninguno de los p_j, para $1 \leq j \leq n$, pero por el teorema (72), P debe ser divisible por algún primo, lo cual es claramente una contradicción.

Propiedad 74 *Sea a un entero positivo tal que para todo primo $p \leq \sqrt{a}$ no se cumple $p|a$, entonces a es primo*

Demostración: Supongamos que a es un número compuesto, es decir, tal que no es divisible por algún primo p, con $p \leq \sqrt{a}$ y $a = b \cdot c$ con $1 < b < a,\ 1 < c < a$.

Podemos suponer sin perdida de generalidad que $b \leq c$. multiplicando por b obtenemos

$$b^2 \leq b \cdot c = a.$$

Luego $b \leq \sqrt{a}$. Pero esto es una contradicción porque:

Si b es primo llegamos a una contradicción por suponer que a no es divisible por algún primo $p \leq \sqrt{a}$.

Si b es compuesto llegamos a una contradicción, pues b compuesto podría expresarse como producto de primos, y siendo p uno de ellos: $b|a$, $p|b$ por lo tanto $p|a$, siendo $p < b \leq \sqrt{a}$. Luego a es primo. □

Ejemplo 28 $\sqrt{19} = 4,35\cdots$, *inspeccione con* 2 *y* 3 *como ninguno lo divide, entonces* 19 *es primo*

Propiedad 75 *Sean $a, b \in \mathbb{Z}^+$ tales que*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},\ b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

con p_i primos distintos $\alpha_i,\ \beta_i \in \mathbb{N}_0$, entonces

$$(a, b) = p_1^{\text{mín}\{\alpha_1,\beta_1\}} p_2^{\text{mín}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{mín}\{\alpha_n,\beta_n\}}$$

Demostración: Sabemos que $a = (a, b)k_1,\ b = (a, b)k_2$, luego en (a, b), los únicos primos que pueden aparecer en la descomposición son los primos p_i. Por lo tanto

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$$

De la primera ecuación tenemos que

$$\alpha_i = \lambda_i + \gamma_i,\ \beta_i = \lambda_i + \gamma_i',$$

es decir,

$$\alpha_i \geq \lambda_i,\ \beta_i \geq \lambda_i,$$

de lo cual, se tiene

$$\text{mín}\{\alpha_i, \beta_i\} \geq \lambda_i,$$

Como (a, b) es el máximo con es condición, se obtiene que

$$(a, b) = p_1^{\text{mín}\{\alpha_1,\beta_1\}} p_2^{\text{mín}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{mín}\{\alpha_n,\beta_n\}}$$

□

Ejemplo 29 *Sea p un número primo. Demostrar que si $p|a \ \wedge\ p|(a^2 + b^2)$ entonces $p|b$*

Solución: Sabemos que $p|a$ luego tenemos que $p|a^2$, así $p|a^2 \wedge p|(a^2+b^2)$ de lo cual obtenemos que

$$p|(a^2+b^2)-a^2$$

Por ende tenemos que $p|b^2$, de este modo en la descomposición en primo de b tiene que estar el primo p, por lo tanto $p|b$

Observación: Note que si $a^2+b^2=c^2$, el ejemplo anterior, nos dice que:

Si $p|a \wedge p|c$ entonces $p|b$.

Además si se define $a=x^2-y^2, b=2x^2y^2, c=x^2+y^2$ entonces son ternas pitagóricas

2.7. Mínimo Común Múltiplo

Definición 19 (Múltiplo Común) *Sean $a,b,c \in \mathbb{Z}$.*

Se dice que c es un múltiplo común de a y b si $a|c$ y $b|c$.

En general dados $x_1,x_2,\ldots,x_n \in \mathbb{Z}$, se dice que a es un múltiplo común de $x_1,x_2,\ldots,x_n$ si y sólo si $x_1|a \wedge x_2|a \wedge \cdots \wedge x_n|a$.

Definición 20 (Mínimo Común Múltiplo) *Sean $a,b \in \mathbb{Z}^*$.*

El mínimo común múltiplo entre a y b, es el menor múltiplo común positivo de a y b, el cual denotaremos por $[a,b]$.

En general dados $x_1,x_2,\ldots,x_n \in \mathbb{Z}^*$, el mínimo común múltiplo de $x_1,x_2,\ldots,x_n$ es el menor múltiplo común de $x_1,x_2,\cdots,x_n$, el cual denotamos por $[x_1,x_2,\ldots,x_n]$

Propiedad 76 *Sean $a,b \in \mathbb{Z}^*$ entonces*

$$[a,b]=[|a|,|b|].$$

Propiedad 77 *Sean $a,b \in \mathbb{Z}^+$ tales que*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n},\ b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$$

con p_i primos distintos $\alpha_i,\ \beta_i \in \mathbb{N}_0$, entonces

$$[a,b]=p_1^{\text{máx}\{\alpha_1,\beta_1\}}p_2^{\text{máx}\{\alpha_2,\beta_2\}}\cdots p_n^{\text{máx}\{\alpha_n,\beta_n\}}$$

Demostración: Sabemos que $[a,b]=ak_1,\ [a,b]=bk_2$, luego en $[a,b]$, a lo menos aparecer en la descomposición los primos p_i. Por lo tanto

$$(a,b)=p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_n^{\lambda_n}c$$

con c, tal que $(c,p_i)=1$.

De la primera ecuación tenemos que

$$\lambda_i=\alpha_i+\gamma_i,\ \lambda_i=\beta_i+\gamma_i',$$

es decir,

$$\lambda_i \geq \alpha_i,\ \lambda_i \geq \beta_i,$$

de lo cual, se tiene

$$\lambda_i \geq \text{máx}\{\alpha_i, \beta_i\},$$

Como $[a, b]$ es el mínimo con es condición, se obtiene que $c = 1$ y

$$[a, b] = p_1^{\text{máx}\{\alpha_1,\beta_1\}} p_2^{\text{máx}\{\alpha_2,\beta_2\}} \cdots p_n^{\text{máx}\{\alpha_n,\beta_n\}}$$

□

Propiedad 78 *Si m es múltiplo común de a y b, entonces $[a, b]|m$.*

Propiedad 79 *Sean $a_1, a_2, \cdots, a_n \in \mathbb{Z}^*$ entonces*

$$[a_1, a_2, \cdots, a_n] = [a_1, [a_2, \cdots, a_n]]$$

Teorema 80 *Si a, b son enteros no nulos,*

$$[a, b] = \frac{|ab|}{(a, b)}.$$

Corolario 81 *Sea $m \in \mathbb{Z}^+$, entonces $[ma, mb] = m[a, b]$.*

Demostración: Del teorema (80), tenemos que

$$[ma, mb] = \frac{|mamb|}{(ma, mb)} = m^2 \frac{|ab|}{(ma, mb)},$$

luego por el teorema (65) se tiene que $(ma, mb) = m(a, b)$, así obtenemos que

$$[ma, mb] = m\frac{|ab|}{(a, b)} = m[a, b].$$

□

Ejemplo 30 *Encontrar el mínimo común múltiplo MCM de:*

a) $[10, 18]$

Calculemos el máximo común divisor

$$\begin{pmatrix} 18 & 1 & 0 \\ 10 & 0 & 1 \end{pmatrix} \underset{F_{21}(-1)}{\sim} \begin{pmatrix} 8 & 1 & -1 \\ 10 & 0 & 1 \end{pmatrix} \underset{F_{12}(-1)}{\sim} \begin{pmatrix} 8 & 1 & -1 \\ 2 & -1 & 2 \end{pmatrix} \underset{F_{21}(-4)}{\sim} \begin{pmatrix} 0 & * & * \\ 2 & -1 & 2 \end{pmatrix}$$

Luego

$$(10, 18) = 2 \text{ y } 18(-1) + 10(2) = 2$$

Como

$$[10, 18] = \frac{|10 \cdot 18|}{(10, 18)} = \frac{180}{2} = 90$$

Por lo tanto $[10, 18] = 90$

b) $[-2, 3, 18]$.

Veamos primero

$$[-2, 3, 18] = [-2, [3, 18]] = [-2, 18] = 18$$

Ya que

$$\begin{aligned} 18 &= 3 \cdot 6 + 0 \\ [3, 18] &= \frac{|3 \cdot 18|}{3} = 18 \end{aligned}$$

Además

$$\begin{aligned} 18 &= 2 \cdot 9 + 0 \\ [-2, 18] &= \frac{|-2 \cdot 18|}{(-2, 18)} = 18 \end{aligned}$$

2.8. Ecuaciones Diofánticas Lineales

El nombre de ecuaciones diofánticas proviene de Diofanto (Matemático de la antigua Grecia), y su origen está ligado a la siguiente pregunta: ¿Cuantos números naturales son necesarios para expresar un número natural cualquiera como suma de cuadrados $n = x^2 + y^2 + z^2 ...$?.

Note que

$$3 = x^2 + y^2 \qquad 7 = x^2 + y^2 + z^2$$

no tiene soluciones en los enteros

La respuesta que los antiguos griegos dieron a esta pregunta fue:

"siempre es posible, si el número de términos es cuatro´´

Definición 21 *Una ecuación diofántica lineal, es una ecuación de la forma*

$$ax + by = c,$$

donde x, y son incógnitas y $a, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. El conjunto solución es

$$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid ax + by = c \}$$

En general, sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, con $x_1, x_2, x_3, ...x_n$ incógnitas entonces la ecuación

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b$$

es llamada ecuación diofántica lineal. El conjunto solución es

$$S = \{x \in \mathbb{Z}^n \mid a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b \}$$

Teorema 82 *$a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$. La ecuación*

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n \quad = \quad b, \tag{2.6}$$

tiene solución en $\mathbb{Z}$ si y sólo si $(a_1, a_2, a_3, \cdots, a_n)|b$.

Demostración: Supongamos que $(a_1, a_2, a_3, \cdots, a_n) \mid b$, entonces existe k tal que $b = (a_1, a_2, a_3, \cdots, a_n)k$, además existe $y_1, y_2, \cdots, y_n$ enteros tales que

$$a_1y_1 + a_2y_2 + a_3y_3 + \cdots + a_ny_n = (a_1, a_2, a_3, \cdots, a_n)$$

Amplificando, obtenemos

$$a_1(y_1k) + a_2(y_2k) + a_3(y_3k) + \cdots + a_n(y_nk) = (a_1, a_2, a_3, \cdots, a_n)k = b$$

luego la ecuación tiene solución.

Supongamos que tiene solución enteras de (2.6), luego existe $z_1, z_2, \cdots, z_n$ enteros tales que

$$a_1z_1 + a_2z_2 + a_3z_3 + \cdots + a_nz_n = b$$

Pero por teorema (50), tenemos que $(a_1, a_2, a_3, \cdots, a_n)|(a_1z_1 + a_2z_2 + a_3z_3 + \cdots + a_nz_n)$, luego $(a_1, a_2, a_3, \cdots, a_n)|b$. □

Teorema 83 *Sean $a, b \in \mathbb{Z}^*, c \in \mathbb{Z}$. La ecuación*

$$ax + by \quad = \quad c, \tag{2.7}$$

Si (2.7) es soluble y $x_0, y_0 \in \mathbb{Z}$ es una solución, entonces todas las soluciones están dadas por

$$x = x_0 - \frac{tb}{(a,b)} \quad \wedge \quad y = y_0 + \frac{ta}{(a,b)},$$

donde t recorre todos los enteros.

De otro modo

$$S = \left\{ \left(x_0 - \frac{tb}{(a,b)}, y_0 + \frac{ta}{(a,b)} \right) \in \mathbb{Z}^2 \mid t \in \mathbb{Z} \right\}$$

Demostración:

Sea $m = (a, b)$ y que x, y es otra solución, además de x_0, y_0. Entonces

$$ax_0 + by_0 = c = ax + by,$$

así

$$a(x_0 - x) = b(y - y_0) \quad \Leftrightarrow \quad \frac{a}{m}(x_0 - x) = \frac{b}{m}(y - y_0). \tag{2.8}$$

Luego por el corolario (66) tenemos que $\left(\frac{a}{m}, \frac{b}{m}\right) = 1$, ahora bien por el corolario (67), obtenemos que

$$\frac{b}{m}|(x_0 - x) \quad \text{y} \quad \frac{a}{m}|(y - y_0). \tag{2.9}$$

Así, de (2.8) y (2.9) se tiene que existe un entero t tal que

$$x_0 - x = \frac{tb}{m} \quad \wedge \quad y - y_0 = \frac{ta}{m},$$

es decir

$$x = x_0 - \frac{tb}{m} \quad \wedge \quad y = y_0 + \frac{ta}{m}. \tag{2.10}$$

Claramente para cualquier $t \in \mathbb{Z}$, (2.10) define una solución de (2.7). Para ver esto basta reemplazar los valores de x e y en (2.7) con lo cual se obtiene una tautología. □

Ejemplo 31 *Determinar la solución general de la ecuación diofántica lineal*

$$10 \cdot x - 32 \cdot y = 2.$$

Solución: Determinemos el máximo común divisor

$$\begin{aligned} 32 &= 10 \cdot 3 + 2 \\ 10 &= 2 \cdot 5 \end{aligned}$$

Por lo tanto $(10, 32) = 2$, de lo cual tenemos

$$\begin{aligned} 2 &= 32 - 10 \cdot 3 \\ 2 &= 10 \cdot (-3) - 32 \cdot (-1) \end{aligned}$$

es decir, $x_0 = -3$, $y_0 = -1$ es una solución particular

La solución general es:

$$x = -3 - \frac{32}{2} \cdot t \ \wedge \ y = -1 - \frac{10}{2} \cdot t \quad \forall t \in \mathbb{Z}$$

El conjunto solución de la ecuación diofántica es

$$S = \{(-3 - 16 \cdot t \ , \ -1 - 5 \cdot t) \mid t \in \mathbb{Z}\}$$

Propiedad 84 *Sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, tal que $(a_1, a_2) = 1 = a_1 z_1 + a_2 z_2$.*

La ecuación diofántica

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = b,$$

es soluble y las soluciones son

$$\begin{aligned} x_1 &= z_1(b - a_3x_3 - a_4x_4 \cdots - a_nx_n) + a_2t \\ x_2 &= z_2(b - a_3x_3 - a_4x_4 \cdots - a_nx_n) - a_1t \end{aligned}$$

con $t, x_3, x_4, x_5, ...x_n \in \mathbb{Z}$.

Ejemplo 32 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 7y + 5z = 2.$$

Solución: Note que la ecuación es igual a

$$7y + 5z = 2 - 10x.$$

El máximo común divisor, entre 5 y 7 es 1, para ello

$$\begin{aligned} 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Por lo tanto

$$5(3) + 7(-2) = 1$$

Amplificando por $2 - 10x$, tenemos una solución particular

$$5(6 - 30x) + 7(-4 + 20x) = 2 - 10x$$

La solución general es:

$$y = 6 - 30x - 7t \ \wedge \ z = -4 + 20x - 5t \qquad \forall t \in \mathbb{Z}$$

El conjunto solución de la ecuación diofántica es

$$S = \{(x, 6 - 30x - 7t \ , \ -4 + 20x - 5t) \mid x, t \in \mathbb{Z}\}$$

Propiedad 85 *Sean $a_1, a_2, a_3, ...a_n \in \mathbb{Z}^*$ y $b \in \mathbb{Z}$, tal que $(a_1, a_2) = d = a_1 z_1 + a_2 z_2$ y $(a_1, a_2, \cdots, a_n) = 1$.*

La ecuación diofántica

$$a_1 x_1 + a_2 x_2 + a_3 x_3 + \cdots + a_n x_n \ = \ b,$$

se resuelve usando la variable auxiliar x_0 y

$$\begin{aligned} x_1 &= z_1 x_0 + \tfrac{a_2}{d} t \\ x_2 &= z_2 x_0 - \tfrac{a_1}{d} t \\ d x_0 + a_3 x_3 + \cdots + a_n x_n &= b \end{aligned}$$

con $t, x_3, x_4, x_5, ...x_n \in \mathbb{Z}$.

Ejemplo 33 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 6y + 15z = 13.$$

Solución: Note que la ecuación es igual a

$$10x + 6y = 13 - 15z$$

Como el máximo común divisor, entre 10 y 6 es 2, luego existe r entero (variable auxiliar) tal que

$$10x + 6y = 2r = 13 - 15z$$

es decir

$$\begin{array}{|rcl} 10x + 6y & = & 2r \\ 13 - 15z & = & 2r \\ \hline \end{array}$$

Para la primera ecuación, una solución particular al máximo común divisor es

$$10(-1) + 6(2) = 2$$

amplificando obtenemos

$$10(-r) + 6(2r) = 2r$$

Y la solución es

$$\begin{array}{rcl} x & = & -r + 3t \\ y & = & 2r - 5t \end{array}$$

con $t \in \mathbb{Z}$.

La otra ecuación es

$$2r + 15z = 13$$

Una solución particular es $r = -1,\ z = 1$. Luego la general esta dada por:

$$\begin{array}{rcl} r & = & -1 + 15u \\ z & = & 1 - 2u \end{array}$$

con $u \in \mathbb{Z}$.

Reemplazando la variable auxiliar obtenemos

$$\begin{array}{rcl} x & = & 1 - 15u + 3t \\ y & = & -2 + 30u - 5t \\ z & = & 1 - 2u \end{array}$$

con $t, u \in \mathbb{Z}$.

$$S = \{(1 - 15u + 3t,\ -2 + 30u - 5t,\ 1 - 2u) \mid u, t \in \mathbb{Z}\}$$

Ejemplo 34 *Determinar la solución general de la ecuación diofántica lineal*

$$10x + 6y + 15z + 70w = 13.$$

Solución: Notemos que $(10,6)=2,\ (15,70)=5$. Consideremos las variables auxiliares u,l

$$\begin{aligned} 10x+6y &= 2u \\ 15z+70w &= 5l \end{aligned}$$

Reemplazando obtenemos $2u+5l=13$.

Para resolver las ecuaciones notemos que

$$10(-1)+6(2)=2\ \ 15(5)+70(-1)=5$$

amplificando obtenemos

$$10(-u)+6(2u)=2u\ \ 15(5l)+70(-l)=5l$$

Y la solución es

$$\begin{aligned} x &= -u+3t \\ y &= 2u-5t \\ z &= 5l+14r \\ w &= -l-3r \end{aligned}$$

Además las soluciones de $2u+5l=13$, son

$$\begin{aligned} u &= -1+5q \\ l &= 3-2q \end{aligned}$$

Reemplazando las variables auxiliares obtenemos,

$$\begin{aligned} x &= 1-5q+3t \\ y &= -2+10q-5t \\ z &= 15-10q+14r \\ w &= -3+2q-3r \end{aligned}$$

con $t,q,r\in\mathbb{Z}$.

$$S=\{(1-5q+3t,\ -2+10q-5t,\ 15-10q+14r,\ -3+2q-3r)\mid t,q,r\in\mathbb{Z}\}$$

2.9. Ejercicios Desarrollados

Ejemplo 35 *Demostrar que el cuadrado de cualquier entero de la forma* $5\cdot k+1$ *es de la misma forma.*

Solución:

$$\begin{aligned} (5\cdot k+1)^2 &= 25\cdot k^2+10\cdot k+1 \\ &= 5\cdot(5\cdot k^2+2\cdot k)+1 \\ &= 5\cdot r+1;\quad r=5\cdot k^2+2\cdot k \end{aligned}$$

Ejemplo 36 *Demostrar que el cuadrado de un entero impar es de la forma* $8 \cdot k + 1$.

Solución: Sea n un número impar entonces $n = 2 \cdot k + 1; \quad k \in \mathbb{Z}$
Por demostrar que $n^2 = 8 \cdot k' + 1$

$$\begin{aligned} n^2 &= (2 \cdot k + 1)^2 \\ &= 4 \cdot k^2 + 4 \cdot k + 1 \\ &= 4 \cdot k \cdot (k + 1) + 1 \end{aligned}$$

Recuerde que ($2|n \cdot (n + 1)$) o bien $(\forall n \in \mathbb{Z})(\exists r \in \mathbb{Z}) n \cdot (n + 1) = 2 \cdot r$), reemplazando obtenemos

$$\begin{aligned} n^2 &= 4 \cdot 2 \cdot r + 1 \\ &= 8 \cdot r + 1 \end{aligned}$$

Ejemplo 37 *Si* $a|b$ *y* $b|c$ *entonces* $a|c$.

Solución: $a|b \Leftrightarrow (\exists q \in \mathbb{Z})(b = a \cdot q)$ y $b|c \Leftrightarrow (\exists k \in \mathbb{Z})(c = b \cdot k)$.
Por demostrar que $a|c \Leftrightarrow (\exists r \in \mathbb{Z})(c = a \cdot r)$.

$$\begin{aligned} c &= b \cdot k \\ &= a \cdot q \cdot k \end{aligned}$$

Por lo tanto $a|c$

Ejemplo 38 *Si* $(b \cdot c)|a$ *entonces* $b|a$ *y* $c|a$.

Solución: $(b \cdot c)|a \Leftrightarrow a = b \cdot c \cdot q; \quad q \in \mathbb{Z}$
Por demostrar que $(b|a \Leftrightarrow a = b \cdot r;\ r \in \mathbb{Z})$ y $(c|a \Leftrightarrow a = c \cdot s;\ s \in \mathbb{Z})$

$$\begin{aligned} a &= b \cdot c \cdot q \\ &= b \cdot r; \quad r = c \cdot q \end{aligned}$$

Por lo tanto $b|a$
De igual manera

$$\begin{aligned} a &= b \cdot c \cdot q \\ &= c \cdot b \cdot q \\ &= c \cdot s; \quad s = b \cdot q \end{aligned}$$

Por lo tanto $c|a$.

Ejemplo 39 *Si* $(a, b \cdot c) = 1$ *entonces* $(a, b) = 1$ *y* $(a, c) = 1$.

Solución: $(a, b \cdot c) = 1 \Leftrightarrow$ existen $x, y \in \mathbb{Z}$ tal que $1 = a \cdot x + b \cdot c \cdot y$

Por demostrar que $((a, b) = 1 \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z}$ tal que $1 = a \cdot x_0 + b \cdot y_0)$ y $((a, c) = 1 \Leftrightarrow \exists x_1, y_1 \in \mathbb{Z}$ tal que $1 = a \cdot x_1 + c \cdot y_1)$

$$\begin{aligned} 1 &= a \cdot x + b \cdot c \cdot y \\ &= a \cdot x + b \cdot y_0; \quad y_0 = c \cdot y \end{aligned}$$

Por lo tanto $(a, b) = 1$

$$\begin{aligned} 1 &= a \cdot x + b \cdot c \cdot y \\ &= a \cdot x + c \cdot b \cdot y \\ &= a \cdot x + c \cdot y_0; \quad y_0 = b \cdot y \end{aligned}$$

Por lo tanto $(a, c) = 1$

Ejemplo 40 *Si $a|c$, $b|c$ y $(a, b) = 1$ entonces $(a \cdot b)|c$.*

Solución: Por hipótesis tenemos que $(a, b) = 1 \Leftrightarrow$ existen $x_0, y_0 \in \mathbb{Z}$ tal que $1 = a \cdot x_0 + b \cdot y_0$, $a|c \Leftrightarrow c = a \cdot r; \quad r \in \mathbb{Z}$, $b|c \Leftrightarrow c = b \cdot s; \quad s \in \mathbb{Z}$

Por demostrar que $a \cdot b|c \Leftrightarrow c = a \cdot b \cdot k; \quad k \in \mathbb{Z}$

$$\begin{aligned} 1 &= a \cdot x + b \cdot y \quad / \cdot c \\ c &= c \cdot a \cdot x + c \cdot b \cdot y \\ &= a \cdot b \cdot s \cdot x + b \cdot a \cdot r \cdot y \\ &= a \cdot b \cdot (s \cdot x + r \cdot y) \\ &= a \cdot b \cdot k; \quad k = s \cdot x + r \cdot y \end{aligned}$$

Por lo tanto $a \cdot b|c$

Ejemplo 41 *Determinar todos los $x, y \in \mathbb{Z}$ que cumplan con: $x + y = 100$ y $(x, y) = 3$*

Solución: $(x, y) = 3 \Leftrightarrow 3|x$ y $3|y$

$3|x \Leftrightarrow x = 3 \cdot q; \quad q \in \mathbb{Z}$; $3|y \Leftrightarrow y = 3 \cdot k; \quad k \in \mathbb{Z}$

$$\begin{aligned} x + y &= 3 \cdot q + 3 \cdot k \\ 100 &= 3 \cdot (q + k) \end{aligned}$$

Luego $3|100$, lo que es contradictorio, por lo tanto no existen $x \in \mathbb{Z}$ tal que $x + y = 100$ y $(x, y) = 3$

Ejercicio 42 *Sean $a, b, c \in \mathbb{Z}^*$, tales que $(a, b) = (a, c) = (b, c) = 1$ y $a^2 + b^2 = c^2$.*

Demostrar que

1. *si a es par entonces $(c - b, c + b) = 2$*
2. *si a es impar entonces $(c - a, c + a) = 2$*

3. *Si* $a = 2x,\ c+b = 2y,\ c-b = 2z, (y,z) = 1$ *entonces existe* u, v *tales que* $y = u^2 \wedge z = v^2$
4. *Si* $a = 2x,\ c+b = 2u^2,\ c-b = 2v^2$ *entonces* $c = u^2+v^2,\ b = u^2-v^2,\ a = 2u^2v^2$

Ejercicio 43 *Resolver la siguientes ecuaciones diofánticas*

1. $3x + 5y = 7$
2. $135x + 142y = 7$
3. $442x + 663y = 13$
4. $1527x - 3452y = 21$
5. $3x + 5y + 7z = 123$
6. $13x + 15y + 7z = 12$
7. $135x + 142y + 726z = 41$
8. $442x + 663y - 221z = 629$
9. $10x + 6y + 15z = 213$
10. $273x + 195y + 105z = 57$

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

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

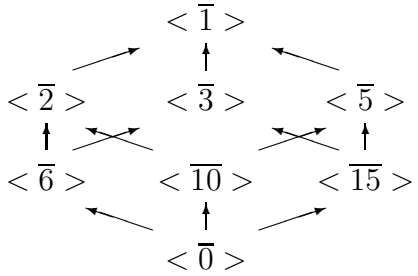
De acuerdo a la propiedad 97, el exponente aditivo t, que ser primo relativo con el orden, luego $(t, 15) = 1$ para obtener otro generador debo amplificar por $1, 2, 4, 7, 8, 11, 13, 14$.

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

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

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

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

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

es decir

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

Con lo cual obtenemos

$$x_1 - x_2 = m_1t_1 = m_2t_2 = \cdots = m_kt_k$$

Así se obtiene $m_2|m_1t_1$ y como $(m_1, m_2) = 1$ entonces $m_2|t_1$,

$$x_1 - x_2 = m_1m_2t_1' = m_3t_3 = \cdots = m_kt_k$$

Repitiendo el proceso tenemos que $m_3|m_1m_2t_1'$ 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

$$x_1 - x_2 = m_1m_2m_3\cdots m_kt_k' \equiv 0(\texttt{mod}\ m_1m_2m_3\cdots m_k)$$

□

Ejemplo 62 *Resolver:*

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

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

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

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

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

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*

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

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

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

□

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*

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

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

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

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

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

□

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

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

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

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

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

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

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:*

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

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* $(\mathbb{Z}_{12}, +)$

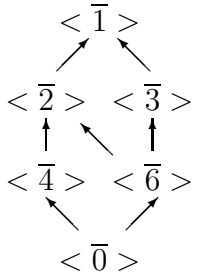
Solución: $\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{12}, +) \Leftrightarrow |\mathcal{H}|/|\mathcal{G}| = 12$ luego $|\mathcal{H}| \in \{1, 2, 3, 4, 6, 12\}$

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

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

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

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:*

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

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

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

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

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

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,

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

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

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*

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

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	$< \overline{8} >, < \overline{12} >$

Capítulo 4

Números Racionales.

Luego de construir los Números Naturales, se presentaron ciertos problemas como ¿Cuál es el resultado de 3 menos 5?, para poder encontrar una solución se creó a partir de $\mathbb{N}$ el conjunto de los Números Enteros que se representan con el símbolo de $\mathbb{Z}$. Pero la vida cotidiana siguió exigiendo la creación de nuevos conjuntos a partir de los ya conocidos.

Consideremos el conjunto $\mathbb{Z}$ como conjunto base y definamos

$$\mathbb{Z}^* := \mathbb{Z} - \{0\}$$

a partir de este nuevo conjunto construimos el producto cartesiano

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) \mid a \in \mathbb{Z} \ \wedge \ b \in \mathbb{Z}^*\}$$

de donde $\mathbb{Z} \times \mathbb{Z}^*$ se denominan fracciones
Notación: Sea $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ una mejor notación para los elementos de este nuevo conjunto es

$$(a, b) = \frac{a}{b}$$

Más aún el elemento a se denominará como numerador y b el denominador.

Definición 39 *Sean $\frac{a}{b}$ y $\frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^*$, definiremos la siguiente relación dada por*

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$$

Propiedad 129 *La relación definida anteriormente $\sim$, es una relación de equivalencia.*

Demostración:

(i) **La relación $\sim$ es refleja:**
Sean $\frac{a}{b} \in \mathbb{Z} \times \mathbb{Z}^*$
Como

$$ab = ab$$

entonces

$$\frac{a}{b} \sim \frac{a}{b}$$

luego la relación es refleja.

(ii) **La relación $\sim$ es simétrica:**

Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^*$ tales que

$$\begin{aligned} \frac{a}{b} \sim \frac{c}{d} &\Leftrightarrow \\ &\Leftrightarrow \quad cb = ad \\ &\Leftrightarrow \quad \frac{c}{d} \sim \frac{a}{b}. \end{aligned}$$

(iii) **La relación $\sim$ es transitiva:**

Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Z} \times \mathbb{Z}^*$ tales que

$$\frac{a}{b} \sim \frac{c}{d} \ \wedge \ \frac{c}{d} \sim \frac{e}{f}$$

Si

$$\begin{aligned} \frac{a}{b} \sim \frac{c}{d} \ \wedge \ \frac{c}{d} \sim \frac{e}{f} \ \Leftrightarrow \ & ad = cb \ \wedge \ cf = ed \\ & adf = cbf \ \wedge \ cfb = edb. \end{aligned}$$

Por lo tanto $adf = edb$, cancelando obtenemos $af = eb$, luego

$$\frac{a}{b} \sim \frac{e}{f}.$$

Observación: La relación de equivalencia definida anteriormente particiona el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ en las clases de equivalencia, que se denotan por

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim := \text{ conjunto cuociente}$$

Definición 40 *Dado $\mathbb{Z} \times \mathbb{Z}^*$, se define el conjunto cuociente*

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim := \left\{ \left[\frac{a}{b}\right] \mid \frac{a}{b} \in \mathbb{Z} \times \mathbb{Z}^* \right\}$$

donde

$$\left[\frac{a}{b}\right] := \left\{ \frac{c}{d} \in \mathbb{Z} \times \mathbb{Z}^* \mid \frac{c}{d} \sim \frac{a}{b} \right\}.$$

Notación: Para una mayor comodidad, denotamos

$$\mathbb{Z} \times \mathbb{Z}^*/_\sim = \mathbb{Q}$$

y $\mathbb{Q}$ se llama el conjunto de los números racionales.

4.1. Suma y Producto en $\mathbb{Q}$

Propiedad 130 *Sean* $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2} \in \mathbb{Z} \times \mathbb{Z}^*$, *tales que* $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$ *y* $\frac{c_1}{d_1} \sim \frac{c_2}{d_2}$ *entonces*

$$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} \sim \frac{a_2 d_2 + c_2 b_2}{b_2 d_2} \qquad y \qquad \frac{a_1 c_1}{b_1 d_1} \sim \frac{a_2 c_2}{b_2 d_2}$$

Demostración: Sean $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2} \in \mathbb{Z} \times \mathbb{Z}^*$, tales que

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \qquad \text{y} \qquad \frac{c_1}{d_1} \sim \frac{c_2}{d_2}$$

Luego se tiene que

$$a_1 b_2 = a_2 b_1 \qquad \text{y} \qquad c_1 d_2 = c_2 d_1$$

Ahora formaremos la Suma:

$$\begin{aligned}
(a_1 d_1 + c_1 b_1) b_2 d_2 &= a_1 d_1 b_2 d_2 + c_1 b_1 b_2 d_2 \\
&= (a_1 b_2) d_1 d_2 + (c_1 d_2) b_1 b_2 \\
&= (a_2 b_1) d_1 d_2 + (c_2 d_1) b_1 b_2 \\
&= (a_2 d_2 (b_1 d_1) + c_2 b_2 (d_1 b_1) \\
&= (a_2 d_2 + c_2 b_2) d_1 b_1
\end{aligned}$$

Por lo tanto

$$(a_1 d_1 + c_1 b_1) b_2 d_2 = (a_2 d_2 + c_2 b_2) d_1 b_1$$

de lo cual obtenemos que

$$\frac{a_1 d_1 + c_1 b_1}{b_1 d_1} \sim \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}$$

Ahora veremos la multiplicación

$$\begin{aligned}
(a_1 c_1)(b_2 d_2) &= (a_1 b_2)(c_1 d_2) \\
&= (a_2 b_1)(c_2 d_1) \\
&= a_2 c_2 b_1 d_1.
\end{aligned}$$

De esta manera tenemos que

$$(a_1 c_1)(b_2 d_2) = a_2 c_2 b_1 d_1.$$

es decir,

$$\frac{a_1 c_1}{b_1 d_1} \sim \frac{a_2 c_2}{b_2 d_2}$$

□

El teorema nos permite definir la suma y el producto

Definición 41 *Sean* $\left[\frac{a}{b}\right]$ *y* $\left[\frac{c}{d}\right] \in \mathbb{Q}$
Adición en $\mathbb{Q}$**:** *Se define la adición en* $\mathbb{Q}$ *por*

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right].$$

Producto $\mathbb{Q}$**:** *Se define la multiplicación en* $\mathbb{Q}$ *por:*

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right].$$

4.1.1. Suma de Números Racionales

Propiedad 131 *Los números racionales con la suma forman un grupo abeliano*

$$(\mathbb{Q}, +) \quad \textit{es un grupo abeliano.}$$

Demostración: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$.
Asociativa:

$$\left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] + \left[\frac{a_2}{b_2}\right]\right) + \left[\frac{a_3}{b_3}\right].$$

Para ellos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right] + \left(\left[\frac{a_2b_3 + a_3b_2}{b_2b_3}\right]\right) \\
&= \left[\frac{a_1}{b_1}\right] + \left[\frac{a_2b_3 + a_3b_2}{b_2b_3}\right] \\
&= \left[\frac{a_1b_2b_3 + a_2b_1b_3 + a_3b_1b_2}{b_1b_2b_3}\right] \\
&= \left[\frac{(a_1b_2 + a_2b_1)b_3 + a_3b_1b_2}{b_1b_2b_3}\right] \\
&= \left[\frac{a_1b_2 + a_2b_1}{b_1b_2}\right] + \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1b_2 + a_2b_1}{b_1b_2}\right]\right) + \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1}{b_1}\right] + \left[\frac{a_2}{b_2}\right]\right) + \left[\frac{a_3}{b_3}\right]
\end{aligned}$$

Por lo tanto la operación suma es asociativa.
Neutro Aditivo: Sean $\left[\frac{0}{1}\right] \in \mathbb{Q}$ y cumple con

$$\left[\frac{a_1}{b_1}\right] + \left[\frac{0}{1}\right] = \left[\frac{a_1}{b_1}\right]$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{0}{1}\right] &= \left[\frac{a_1 1+0b_1}{b_1 1}\right]\\ &= \left[\frac{a_1}{b_1}\right]\end{aligned}$$

luego tenemos que el neutro aditivo existe y es

$$\left[\frac{0}{b}\right]=\left[\frac{0}{1}\right] \quad \text{con } b\in\mathbb{Z}^*$$

Inverso Aditivo: Dado $\left[\frac{a_1}{b_1}\right]$ existe $\left[\frac{-a_1}{b_1}\right]\in\mathbb{Q}$ tal que

$$\left[\frac{a_1}{b_1}\right]+\left[\frac{-a_1}{b_1}\right]=\left[\frac{0}{1}\right]$$

Justifiquemos lo anterior

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{-a_1}{b_1}\right] &= \left[\frac{a_1b_1+(-a_1)b_1}{b_1b_1}\right]\\ &= \left[\frac{0}{b_1b_1}\right]=\left[\frac{0}{1}\right]\end{aligned}$$

Lo anterior demuestra que existe el inverso aditivo, de esta manera tenemos que el inverso aditivo de $\left[\frac{a_1}{b_1}\right]$ es $\left[\frac{-a_1}{b_1}\right]$
Conmutatividad: Debemos probar que

$$\left[\frac{a_1}{b_1}\right]+\left[\frac{a_2}{b_2}\right]=\left[\frac{a_2}{b_2}\right]+\left[\frac{a_1}{b_1}\right]$$

Para ello

$$\begin{aligned}\left[\frac{a_1}{b_1}\right]+\left[\frac{a_2}{b_2}\right] &= \left[\frac{a_2b_1+a_1b_2}{b_2b_1}\right]\\ &= \left[\frac{a_2}{b_2}\right]+\left[\frac{a_1}{b_1}\right].\end{aligned}$$

Luego la suma es conmutativa.
Notación: Sean $\left[\frac{a}{b}\right]$ y $\left[\frac{c}{d}\right]\in\mathbb{Q}$, entonces

$$\left[\frac{a}{b}\right]-\left[\frac{c}{d}\right]=\left[\frac{a}{b}\right]+\left[\frac{-c}{d}\right]$$

4.1.2. Multiplicación de Números Racionales

Propiedad 132 *Los números racionales con las propiedades de la multiplicación forman un grupo abeliano.*

$$(\mathbb{Q}^*, \cdot) \quad \textit{es un grupo abeliano,}$$

donde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.

Demostración: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$

Asociativa:

$$\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right].$$

Para ellos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2 a_3}{b_2 b_3}\right]\right) \\
&= \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2 a_3}{b_2 b_3}\right] \\
&= \left[\frac{a_1 a_2 a_3}{b_1 b_2 b_3}\right] \\
&= \left[\frac{a_1 a_2}{b_1 b_2}\right] \cdot \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1 a_2}{b_1 b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right] \\
&= \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) \cdot \left[\frac{a_3}{b_3}\right]
\end{aligned}$$

Luego la multiplicación es asociativa.

Neutro multiplicativo: Existe $\left[\frac{1}{1}\right] \in \mathbb{Q}$ que cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{1}{1}\right] = \left[\frac{a_1}{b_1}\right]$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{1}{1}\right] &= \left[\frac{a_1 1}{b_1 1}\right] \\
&= \left[\frac{a_1}{b_1}\right]
\end{aligned}$$

luego tenemos que el neutro aditivo existe y es

$$\left[\frac{a}{a}\right] = \left[\frac{1}{1}\right] \quad \text{con } a \in \mathbb{Z}^*$$

Inverso multiplicativo: Sean $\left[\frac{a_1}{b_1}\right] \in \mathbb{Q}^*$ luego existe $\left[\frac{b_1}{a_1}\right] \in \mathbb{Q}^*$ que cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{b_1}{a_1}\right] = \left[\frac{1}{1}\right]$$

Justifiquemos lo anterior

$$\begin{aligned} \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{b_1}{a_1}\right] &= \left[\frac{a_1 b_1}{a_1 b_1}\right] \\ &= \left[\frac{1}{1}\right] \end{aligned}$$

Lo anterior demuestra que existe el inverso multiplicativo, de esta manera tenemos que el inverso de $\left[\frac{a_1}{b_1}\right]$ es $\left[\frac{b_1}{a_1}\right]$
Conmutatividad: Debemos probar que

$$\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right] = \left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_1}{b_1}\right]$$

Para ello

$$\begin{aligned} \left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right] &= \left[\frac{a_1 a_2}{b_1 b_2}\right] \\ &= \left[\frac{a_2 a_1}{b_2 b_1}\right] \\ &= \left[\frac{a_2}{b_2}\right] \cdot \left[\frac{a_1}{b_1}\right]. \end{aligned}$$

Luego el producto es conmutativo □
Notación: Sean $\left[\frac{a}{b}\right]$ y $\left[\frac{c}{d}\right] \in \mathbb{Q}^*$, entonces

$$\left[\frac{a}{b}\right] : \left[\frac{c}{d}\right] = \left[\frac{a}{b}\right] \cdot \left[\frac{d}{c}\right].$$

Teorema 133 *El conjunto de los números racionales, con la suma y producto definidos anteriores* $(\mathbb{Q}, +, \cdot)$*, es un cuerpo.*

Demostración: Se ha demostrado anteriormente que $(\mathbb{Q}, +)$ y $(\mathbb{Q}^*, \cdot)$ son grupos abelianos, luego falta ver la distributividad
Distributividad: Sean $\left[\frac{a_1}{b_1}\right], \left[\frac{a_2}{b_2}\right], \left[\frac{a_3}{b_3}\right] \in \mathbb{Q}$, entonces se cumple

$$\left[\frac{a_1}{b_1}\right] \cdot \left(\left[\frac{a_2}{b_2}\right] + \left[\frac{a_3}{b_3}\right]\right) = \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_2}{b_2}\right]\right) + \left(\left[\frac{a_1}{b_1}\right] \cdot \left[\frac{a_3}{b_3}\right]\right)$$

Veamos

$$\begin{aligned}
\left[\frac{a_1}{b_1}\right]\cdot\left(\left[\frac{a_2}{b_2}\right]+\left[\frac{a_3}{b_3}\right]\right) &= \left[\frac{a_1}{b_1}\right]\cdot\left(\left[\frac{a_2b_3+a_3b_2}{b_2b_3}\right]\right)\\
&= \left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_2b_3+a_3b_2}{b_2b_3}\right]\\
&= \left[\frac{a_1a_2b_3+a_1a_3b_2}{b_1b_2b_3}\right]\\
&= \left[\frac{a_1a_2}{b_1b_2}\right]+\left(\left[\frac{a_1a_3}{b_1b_3}\right]\right)\\
&= \left(\left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_2}{b_2}\right]\right)+\left(\left[\frac{a_1}{b_1}\right]\cdot\left[\frac{a_3}{b_3}\right]\right)
\end{aligned}$$

Observación: Luego de haber definido el conjunto de los números racionales o $\mathbb{Q}$, el no contiene todos los números que necesitamos por ejemplo la ecuación $x^2 = 5$ no tiene solución en $\mathbb{Q}$, es decir, el número que en forma habitual se denotado por $\sqrt{5} \notin \mathbb{Q}$.

Propiedad 134 *Sea $p \in \mathbb{Z}$ un número primo entonces el número $\sqrt{p} \notin \mathbb{Q}$.*

Demostración: Para este caso la demostración la realizaremos por el método del absurdo que consiste en suponer como cierto la negación de la proposición como sigue:

Supongamos que la ecuación $x^2 = \left[\frac{p}{1}\right]$ tiene solución en $\mathbb{Q}$, entonces la solución se puede representar como una fracción

$$\begin{aligned}
\left[\frac{p}{1}\right] &= \left(\left[\frac{a}{b}\right]\right)^2 \quad \text{donde} \quad (a,b)=1\\
\text{Luego, } \frac{p}{1} &\sim \frac{a^2}{b^2}\\
pb^2 &= a^2
\end{aligned}$$

Luego $p|a^2$, es decir $p|a$. Por lo tanto $a = pk$ con $k \in \mathbb{Z}$ reemplazando

$$\begin{aligned}
pb^2 &= p^2k^2\\
b^2 &= pk^2
\end{aligned}$$

Por la justificación similar a la anterior $p|b^2$ es decir $p|b$, lo cual es una contradicción ya que $(a,b) = 1$. Por lo tanto

$$\sqrt{p} \notin \mathbb{Q}$$

□

Notación: A cada número racional

$$\left[\frac{a}{b}\right] = \left\{\frac{x}{y} \;\middle|\; \frac{x}{y} \sim \frac{a}{b}\right\}$$

lo denotaremos simplemente $\frac{a}{b}$.

Debemos tener claridad en la diferencia entre fracción y número racional ya que en este caso nos refiriendo a la clase.

Por ejemplo las fracciones $\frac{5}{15}$, $\frac{1}{3}$ no son iguales, pero como números racional si son iguales las clases, ya que $\frac{5}{15} \sim \frac{1}{3}$.

4.1.3. Expresión decimal en $\mathbb{Q}$.

Dado un número racional $\frac{a}{b}$, luego aplicamos el algoritmo de la división y obtenemos

$$a = bq + r, \quad \text{con } 0 \leq r < b$$

si volvemos aplicar el algoritmo de la división obtenemos

$$\begin{aligned} 10 \cdot r &= bq_1 + r_1, \quad \text{con } 0 \leq r_1 < b \\ 10 \cdot r_1 &= bq_2 + r_2, \quad \text{con } 0 \leq r_2 < b \\ &\vdots \\ 10 \cdot r_t &= bq_{t+1} + r_{t+1}, \quad \text{con } 0 \leq r_{t+1} < b \end{aligned}$$

como los posibles resto r_i son finito, luego en algún momento es 0 o se repite, de lo cual obtenemos que los números racionales se representan por números decimales finito o los números decimales infinitos periódicos, es decir,

$$\frac{a}{b} = q_1, q_2 q_3 \ldots q_t \text{ o bien } \frac{a}{b} = \frac{a}{b} = q_1, q_2 q_3 \ldots \overline{q_s \ldots q_t}$$

Ejemplo de ello tenemos

$$\frac{1}{4} = 0,25 \quad \frac{1}{3} = 0,\overline{3}$$

Existe otros números que no pertenecen a $\mathbb{Q}$, estos son los llamados números decimales infinitos no periódico o irracionales $\mathbb{I}$, ya que no se puede encontrar una representación en números racionales.

Los Números Reales

Con los conjuntos de los números racionales e irracionales que denotamos como $\mathbb{Q}$ e $\mathbb{I}$ respectivamente, podemos construir un nuevo conjunto que se puede crear a partir de estos dos. Estos nuevos elementos los llamaremos números reales y algunos elementos que pertenecen a este conjunto son

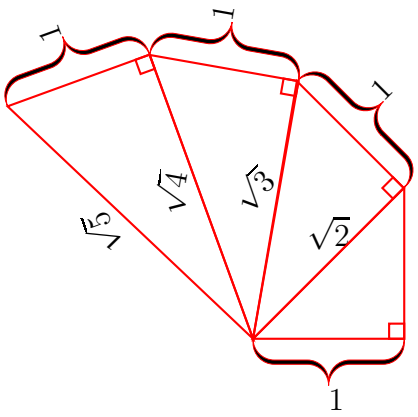
$$\pi;\ \sqrt{3};\ 0,1;\ 5,\overline{6};\cdots$$

En este conjunto existe un producto y una suma compatible con de $\mathbb{Q}$, que entrega la siguiente propiedad

Teorema 135 $(\mathbb{R}, +, \cdot)$ *es un cuerpo.*

4.2. Extensiones Cuadráticas de los Racionales $\mathbb{Q}[\sqrt{p}]$.

Como justificamos anteriormente los números $\sqrt{2}, \sqrt{3}, \cdots \notin \mathbb{Q}$, pero si a $\mathbb{Q}$ le agregamos estos números lo que tenemos como resultado son cuerpos intermedios llamados extensiones cuadráticas debido a que vienen dados por raíces cuadráticas.
Observación: De los números anterior existe algunos de ellos que pueden ser representados por el llamado espiral pitagórica, que se inicia con un triángulo isosceles, con lados de longitud 1, y el siguiente triángulo rectángulo de altura 1 y base la hipotenusa del anterior, como en la figura.



Definición 42 *Sea $p \in \mathbb{Z}$, tal que $\sqrt{p} \notin \mathbb{Q}$*
Se define $\mathbb{Q}[\sqrt{p}]$ por

$$\mathbb{Q}[\sqrt{p}] := \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$$

Observación: Notemos que dado un número $x \in \mathbb{Q}[\sqrt{p}]$, existe únicos elementos $a, b \in \mathbb{Q}$, tal que $x = a + b\sqrt{p}$.

Si suponemos que existe dos expresiones distintas $a + b\sqrt{p} = c + d\sqrt{p}$, obtenemos una contradicción con que $\sqrt{p} \notin \mathbb{Q}$. Esta observación nos permite definir las siguientes operaciones binarias.

4.2.1. Suma y Producto en $\mathbb{Q}[\sqrt{p}]$.

Sean $a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Se define las siguientes operaciones:
Suma:

$$(a_1 + b_1\sqrt{p}) + (a_2 + b_2\sqrt{p}) := (a_1 + a_2) + (b_1 + b_2)\sqrt{p}$$

Producto:

$$(a_1 + b_1\sqrt{p}) \cdot (a_2 + b_2\sqrt{p}) := (a_1a_2 + pb_1b_2) + (a_1b_2 + a_2b_1)\sqrt{p}$$

Propiedades de la Suma en $\mathbb{Q}[\sqrt{p}]$.

Propiedad 136 *La extensión cuadrática con la operación suma es un grupo abeliano, es decir,*

$$(\mathbb{Q}[\sqrt{p}],+) \quad \textit{es un grupo abeliano}$$

Demostración: Recuerde que $(\mathbb{Q},+)$ es un grupo abeliano.

Sean $a_1+b_1\sqrt{p},\ a_2+b_2\sqrt{p},\ a_3+b_3\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$

Asociativa:

$$(a_1+b_1\sqrt{p})+[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] = [(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p})]+(a_3+b_3\sqrt{p})$$

Para ello,

$$\begin{aligned}(a_1+b_1\sqrt{p})+[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] &= (a_1+b_1\sqrt{p})+[(a_2+a_3)+(b_2+b_3)\sqrt{p}] \\ &= (a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{p} \\ &= [(a_1+a_2)+(b_1+b_2)\sqrt{p}]+(a_3+b_3\sqrt{p}). \\ &= [(a_1+b_2)\sqrt{p})+(a_2+b_2\sqrt{p})]+(a_3+b_3\sqrt{p}).\end{aligned}$$

Por lo tanto, la operación suma es asociativa

Neutro Aditivo: Existe $0+0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$

Que cumple con:

$$\begin{aligned}(a_1+b_1\sqrt{p})+(0+0\sqrt{p}) &= (a_1+0)+(b_1+0)\sqrt{p} \\ &= a_1+b_1\sqrt{p}\end{aligned}$$

luego el neutro aditivo existe y es $0=0+0\sqrt{p}$.

Inverso Aditivo: Sea $a_1+b_1\sqrt{p}$, existe $(-a_1)+(-b_1)\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ que cumple con

$$(a_1+b_1\sqrt{p})+((-a_1)+(-b_1)\sqrt{p}) = 0+0\sqrt{p}$$

Comprobemos lo anterior

$$\begin{aligned}(a_1+b_1\sqrt{p})+((-a_1)+(-b_1)\sqrt{p}) &= (a_1+(-a_1))+(b_1+(-b_1))\sqrt{p} \\ &= 0+0\sqrt{p}\end{aligned}$$

Lo anterior demuestra que existe el inverso aditivo de $a_1+b_1\sqrt{p}$ es $(-a_1)+(-b_1)\sqrt{p}$.

Conmutatividad: Debemos probar

$$(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p}) = (a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p})$$

Para ello

$$\begin{aligned}(a_1+b_1\sqrt{p})+(a_2+b_2\sqrt{p}) &= (a_1+a_2)+(b_1+b_2)\sqrt{p} \\ &= (a_2+a_1)+(b_2+b_1)\sqrt{p} \\ &= (a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p}).\end{aligned}$$

□

Propiedad del Producto en $\mathbb{Q}[\sqrt{p}]$.

Propiedad 137 *El conjunto $\mathbb{Q}[\sqrt{p}]$ con la multiplicación forman un grupo abeliano*

$$(\mathbb{Q}^*[\sqrt{p}],\cdot) \quad \textit{es un grupo abeliano}$$

donde $\mathbb{Q}^*[\sqrt{p}]$ es $\mathbb{Q}[\sqrt{p}]-\{0\}$.

Demostración: Sean $a_1+b_1\sqrt{p},\ a_2+b_2\sqrt{p},\ a_3+b_3\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$
Asociativa:

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})\cdot(a_3+b_3\sqrt{p})]=[(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]\cdot(a_3+b_3\sqrt{p})$$

Para ello

$$\begin{aligned}
& (a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})\cdot(a_3+b_3\sqrt{p})]\\
= \ & (a_1+b_1\sqrt{p})\cdot[(a_2a_3+pb_2b_3)+(a_3b_2+a_2b_3)\sqrt{p}]\\
= \ & [a_1(a_2a_3+pb_2b_3)+pb_1(a_3b_2+a_2b_3)]+[a_1(a_3b_2+a_2b_3)+(a_2a_3+pb_2b_3)b_1]\sqrt{p}\\
= \ & (a_1a_2a_3+a_1pb_2b_3+a_3b_2b_1p+a_2b_3b_1p)+(a_1a_3b_2+a_1a_2b_3+a_2a_3b_1+pb_1b_2b_3)\sqrt{p}\\
= \ & [(a_1a_2+b_2b_1p)a_3+(a_1b_2+a_2b_1)b_3p]+[(a_1a_2+pb_1b_2)b_3+a_3(a_1b_2+a_2b_1)]\sqrt{p}\\
= \ & [(a_1a_2+b_2b_1p)+(a_1b_2+a_2b_1)\sqrt{p}](a_3+b_3\sqrt{p})\\
= \ & [(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]\cdot(a_3+b_3\sqrt{p})
\end{aligned}$$

Por lo tanto el producto es asociativo.
Neutro Multiplicativo: Existe $1+0\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$, tal que

$$(a_1+b_1\sqrt{p})\cdot(1+0\sqrt{p})=a_1+b_1\sqrt{p}$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}
(a_1+b_1\sqrt{p})\cdot(1+0\sqrt{p}) &= (a_11+p0b_1)+(a_10+1b_1)\sqrt{p}\\
&= a_1+b_1\sqrt{p}
\end{aligned}$$

luego tenemos que el neutro multiplicativo existe y es

$$1=1+0\sqrt{p}.$$

Inverso Multiplicativo: Sean $a+b\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$, en primer lugar notemos que $a^2-b^2p\neq 0$, propiedad 134, luego existe $\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$ que cumple con

$$(a+b\sqrt{p})\cdot(\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p})=1+0\sqrt{p}$$

La prueba de lo anterior esta dada por

$$\begin{aligned}
& (a+b\sqrt{p})\cdot(\frac{a}{a^2-b^2p}+\frac{-b}{a^2-b^2p}\sqrt{p}) \\
= & \left(a\frac{a}{a^2-b^2p}+pb\frac{-b}{a^2-b^2p}\right)+\left(a\frac{-b}{a^2-b^2p}+\frac{a}{a^2-b^2p}b\right)\sqrt{p} \\
= & \frac{a^2-b^2p}{a^2-b^2p}+\frac{-ba+ba}{a^2-b^2p}\sqrt{p} \\
= & 1+0\sqrt{p}
\end{aligned}$$

Por lo tanto el inverso multiplicativo de $a+b\sqrt{p}$ es

$$\frac{a}{a^2-pb^2}+\frac{-b}{a^2-pb^2}\sqrt{p}.$$

Conmutatividad: Debemos probar

$$(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})=(a_2+b_2\sqrt{p})\cdot(a_1+b_1\sqrt{p})$$

Para ello

$$\begin{aligned}
(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p}) &= (a_1a_2+pb_1b_2)+(a_1b_2+a_2b_1)\sqrt{p} \\
&= (a_2a_1+pb_2b_1)+(a_2b_1+a_1b_2)\sqrt{p} \\
&= (a_2+b_2\sqrt{p})\cdot(a_1+b_1\sqrt{p}).
\end{aligned}$$

Por lo tanto la multiplicación en $\mathbb{Q}[\sqrt{p}]$ es conmutativa. □

Notación: $a+b\sqrt{p}\in\mathbb{Q}[\sqrt{p}],\ c+d\sqrt{p}\in\mathbb{Q}^*[\sqrt{p}]$ entonces

$$(a+b\sqrt{p}):(c+d\sqrt{p})=(a+b\sqrt{p})\cdot(c+d\sqrt{p})^{-1}$$

Teorema 138 $(\mathbb{Q}[\sqrt{p}],+,\cdot)$ *es un cuerpo.*

Demostración: Se ha demostrado anteriormente que $(\mathbb{Q}[\sqrt{p}],+)$ y $(\mathbb{Q}^*[\sqrt{p}],\cdot)$ son grupos abelianos, luego falta ver la distributividad es decir, debemos demostrar

$a_1+b_1\sqrt{p},a_2+b_2\sqrt{p},a_3+b_3\sqrt{p}\in\mathbb{Q}[\sqrt{p}]$ tenemos

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})]=[(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})+(a_1+b_1\sqrt{p})\cdot(a_3+b_3\sqrt{p})].$$

Veamos

$$(a_1+b_1\sqrt{p})\cdot[(a_2+b_2\sqrt{p})+(a_3+b_3\sqrt{p})] = (a_1+b_1\sqrt{p})\cdot[(a_2+a_3)+(b_2+b_3)\sqrt{p}]$$

lo que es igual a

$$\begin{aligned}
& (a_1(a_2+a_3)+pb_1(b_2+b_3))+(a_1(b_2+b_3)+b_1(a_2+a_3)\sqrt{p} \\
= & (a_1a_2+a_1a_3+pb_1b_2+pb_1b_3)+(a_1b_2+a_1b_3+a_2b_1+a_3b_1)\sqrt{p} \\
= & (a_1a_2+pb_1b_2+a_1a_3+pb_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)\sqrt{p} \\
= & ((a_1a_2+pb_1b_2)+(a_1b_2+a_2b_1)\sqrt{p})+((a_1a_3+pb_1b_3)+(a_1b_3+a_3b_1)\sqrt{p}) \\
= & [(a_1+b_1\sqrt{p})\cdot(a_2+b_2\sqrt{p})]+[(a_1+b_1\sqrt{p})\cdot(a_3+b_3\sqrt{p})].
\end{aligned}$$

Ejemplo 106 *Resolver en* $\mathbb{Q}[\sqrt{5}]$*, la ecuación*

$$(2+3\sqrt{5})x = 3-\sqrt{5}$$

Solución: Como sabemos, el inverso se obtiene del siguiente modo

$$(2+3\sqrt{5})^{-1} = \frac{2}{4-5\cdot 9} - \frac{3}{4-5\cdot 9}\sqrt{5} = -\frac{2}{41} + \frac{3}{41}\sqrt{5}$$

luego se tiene que

$$x = (3-\sqrt{5})(-\frac{2}{41} + \frac{3}{41}\sqrt{5}) = (-3\frac{2}{41} + 5\cdot(-1)\frac{3}{41}) + (3\frac{3}{41} - \frac{2}{41}(-1))\sqrt{5}$$

Por lo tanto,

$$x = -\frac{21}{41} + \frac{11}{41}\sqrt{5}$$

El conjunto solución es

$$S = \left\{-\frac{21}{41} + \frac{11}{41}\sqrt{5}\right\}$$

Ejemplo 107 *Resolver en* $\mathbb{Q}[\sqrt{7}]$*, el sistema ecuaciones*

$$\boxed{\begin{array}{rcl}(2+\sqrt{7})x + y &=& 3+\sqrt{7}\\ (3-\sqrt{7})x + \sqrt{7}y &=& 1\end{array}}$$

Solución: Amplifiquemos la primera ecuación

$$\boxed{\begin{array}{rcll}(2+\sqrt{7})x + y &=& 3+\sqrt{7} & /\cdot -\sqrt{7}\\ (3+\sqrt{7})x + \sqrt{7}y &=& 1 & \end{array}}$$

Obtenemos

$$\boxed{\begin{array}{rcl}(-7-2\sqrt{7})x - \sqrt{7}y &=& -7-3\sqrt{7}\\ (3+\sqrt{7})x + \sqrt{7}y &=& 1\end{array}}$$

Sumando obtenemos

$$\begin{array}{rcl}(-4-\sqrt{7})x &=& -6-3\sqrt{7}\\ x &=& (-6-3\sqrt{7})(-4-\sqrt{7})^{-1}\\ x &=& (-6-3\sqrt{7})(\frac{-4}{9} + \frac{1}{9}\sqrt{7})\\ x &=& \frac{1}{3} + \frac{2}{3}\sqrt{7}\end{array}$$

Reemplazando en la primera ecuación obtenemos

$$\begin{array}{rcl}y &=& 3+\sqrt{7} - (2+\sqrt{7})(\frac{1}{3} + \frac{2}{3}\sqrt{7})\\ y &=& 3+\sqrt{7} - (\frac{16}{3} + \frac{5}{3}\sqrt{7})\\ y &=& -\frac{7}{3} - \frac{2}{3}\sqrt{7}\end{array}$$

Luego, el conjunto solución del sistema es

$$S = \left\{\left(\frac{1}{3} + \frac{2}{3}\sqrt{7}, -\frac{7}{3} - \frac{2}{3}\sqrt{7}\right)\right\}$$

4.2.2. Conjugación de $\mathbb{Q}[p]$.

Definición 43 *Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$.*
Se define el conjugación de $a+b\sqrt{p}$ por $a-b\sqrt{p}$ y se denota de la siguiente forma:

$$\overline{a+b\sqrt{p}} := a-b\sqrt{p}.$$

Observación: La conjugación es una función dada por

$$\begin{array}{rccc} \overline{} & : & \mathbb{Q}[\sqrt{p}\,] & \to & \mathbb{Q}[\sqrt{p}\,] \\ & & a+b\sqrt{p} & \mapsto & \overline{a+b\sqrt{p}} = a-b\sqrt{p}. \end{array}$$

Cumple las siguientes propiedades

Teorema 139 *Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$*

(i)
$$\overline{(a+b\sqrt{p})+(c+d\sqrt{p})} = \overline{(a+b\sqrt{p})} + \overline{(c+d\sqrt{p})}.$$

(ii)
$$\overline{(a+b\sqrt{p})\cdot(c+d\sqrt{p})} = \overline{(a+b\sqrt{p})} \cdot \overline{(c+d\sqrt{p})}.$$

(iii)
$$\overline{a+b\sqrt{p}} = a+b\sqrt{p} \quad \textit{si y sólo si} \quad b=0.$$

Demostración:

(i) Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\begin{aligned} \overline{(a+b\sqrt{p})+(c+d\sqrt{p})} &= \overline{(a+c)+(b+d)\sqrt{p}} \\ &= (a+c)-(b+d)\sqrt{p} \\ &= (a+c)+((-b)+(-d))\sqrt{p} \\ &= (a-b\sqrt{p})+(c-d\sqrt{p}) \\ &= \overline{a+b\sqrt{p}} + \overline{c+d\sqrt{p}}. \end{aligned}$$

(ii) Sean $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, tenemos

$$\begin{aligned} \overline{(a+b\sqrt{p})\cdot(c+d\sqrt{p})} &= \overline{(ac+pbd)+(ad+bc)\sqrt{p}} \\ &= ((ac+bd)-(ad+bc)\sqrt{p} \\ &= (ac+(-b)(-d))+(a(-d)+(-b)c)\sqrt{p} \\ &= (a-b\sqrt{p})\cdot(c-d\sqrt{p}) \\ &= \overline{a+b\sqrt{p}} \cdot \overline{c+d\sqrt{p}}. \end{aligned}$$

(iii) Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\overline{a+b\sqrt{p}} = a-b\sqrt{p}$$

pero a, b son únicos luego

$$a = a \vee b = -b$$

Por lo tanto, $b=0$

4.2.3. La Norma de $\mathbb{Q}[\sqrt{p}]$.

Definición 44 *Sea $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, se define la norma de $a+b\sqrt{p}$ por a^2-b^2p y se denota por*

$$\| a + b\sqrt{p} \| := a^2 - b^2p.$$

Observación: La norma es una función dada por

$$\begin{array}{rccc} \| \ \| & : & \mathbb{Q}[\sqrt{p}] & \to & \mathbb{Q} \\ & & a + b\sqrt{p} & \mapsto & \| a + b\sqrt{p} \| = a^2 - b^2p. \end{array}$$

Teorema 140 *Sean $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$*

i)

$$\| \overline{(a + b\sqrt{p})} \| = \| a + b\sqrt{p} \|$$

ii)

$$\| (a + b\sqrt{p}) \| = (a + b\sqrt{p})\overline{(a + b\sqrt{p})}$$

iii)

$$\| (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) \| = \| a + b\sqrt{p} \| \cdot \| c + d\sqrt{p} \|$$

Demostración: Sean $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$, luego

$$\begin{array}{rcl} \| (a_+b\sqrt{p}) \cdot (c + d\sqrt{p}) \| & = & \| (ac + pbd) + (ad + bd)\sqrt{p} \| \\ & = & (ac + pbd)^2 - (ad + bd)^2p \\ & = & a^2c^2 + 2acpbd + p^2b^2d^2 - (a^2d^2 + 2adcb + c^2b^2)p \\ & = & a^2c^2 + 2acpbd + p^2b^2d^2 - a^2d^2p - 2adcbp - c^2b^2p \\ & = & a^2c^2 + p^2b^2d^2 - a^2d^2p - c^2b^2p \\ & = & (a^2 - pb^2) \cdot (c^2 - pd^2) \\ & = & \| a + b\sqrt{p} \| \cdot \| c + d\sqrt{p} \| \end{array}$$

4.2.4. Anillo de Enteros de $\mathbb{Z}[\sqrt{p}]$.

Definición 45 *Se define $\mathbb{Z}[\sqrt{p}]$ igual a*

$$\mathbb{Z}[\sqrt{p}] := \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$$

Observación: Dadas las contenciones anteriores se tiene que

$$\mathbb{Z}[\sqrt{p}] \subseteq \mathbb{Q}[\sqrt{p}]$$

Luego el conjugado y norma están definidas, más aún

$$\begin{array}{rccc} \| \ \| & : & \mathbb{Z}[\sqrt{p}\,] & \to & \mathbb{Z} \\ & & a + b\sqrt{p} & \mapsto & \| a + b\sqrt{p} \| := a^2 - b^2p. \end{array}$$

Teorema 141 $(\mathbb{Z}[\sqrt{p}], +, \cdot)$ *es un anillo conmutativo.*

Definición 46 *Sea $u \in \mathbb{Z}[\sqrt{p}]$, se dice que u es una unidad de $\mathbb{Z}[\sqrt{p}]$, si y sólo si existe un elemento $v \in \mathbb{Z}[\sqrt{p}]$, tal que $uv = 1$.*

Notación: Denotaremos el conjunto unidad de $\mathbb{Z}[\sqrt{p}]$ por $\mathcal{U}(\mathbb{Z}[\sqrt{p}])$

Ejemplo 108 *Determine en cada caso si el elemento es*

1. $3 + 2\sqrt{2}$ *es un unidad* $\mathbb{Z}[\sqrt{2}]$
2. $3 + 2\sqrt{3}$ *es un unidad* $\mathbb{Z}[\sqrt{3}]$

Solución: 1. Supongamos $3 + 2\sqrt{2}$ es un unidad, luego existe $x + y\sqrt{2}$ tal que

$$\begin{aligned}(3 + 2\sqrt{2})(x + y\sqrt{2}) &= 1 + 0\sqrt{2}\\ (3x + 4y) + (3y + 2x)\sqrt{2} &= 1 + 0\sqrt{2}\end{aligned}$$

De lo cual obtenemos, el siguiente sistema

$$\left.\begin{array}{rcl} 3x + 4y &=& 1 \ / \cdot 2 \\ 2x + 3y &=& 0 \ / \cdot -3 \end{array}\right|$$

Sumando las ecuaciones obtenemos $-y = 2$, es decir $y = -2$. reemplazando obtenemos $x = 3$,

$$(3 + 2\sqrt{2})^{-1} = 3 - 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

luego tenemos $3 + 2\sqrt{2} \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$.

2. Supongamos ahora que $3 + 2\sqrt{3}$ es un unidad, luego existe $x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ tal que

$$\begin{aligned}(3 + 2\sqrt{3})(x + y\sqrt{3}) &= 1 + 0\sqrt{3}\\ (3x + 6y) + (3y + 2x)\sqrt{3} &= 1 + 0\sqrt{3}\end{aligned}$$

De lo cual obtenemos

$$\left.\begin{array}{rcl} 3x + 6y &=& 1 \\ 2x + 3y &=& 0 \end{array}\right|$$

Pero la primera ecuación nos entrega que $3|1$, lo que es una contradicción. Por tanto tenemos $3 + 2\sqrt{3} \notin \mathcal{U}(\mathbb{Z}[\sqrt{3}])$.

Propiedad 142 *$a + b\sqrt{p} \in \mathcal{U}(\mathbb{Z}[\sqrt{p}])$ si y sólo si $\|a + b\sqrt{p}\| \in \{1. - 1\}$*

Demostración: Supongamos que $a + b\sqrt{p}$ es una unidad, luego existe $x + y\sqrt{p}$ tal que

$$\begin{aligned}(a + b\sqrt{p})(x + y\sqrt{p}) &= 1 + 0\sqrt{p} \ /\| \ \|\\ \|(a + b\sqrt{p})(x + y\sqrt{p})\| &= \|1 + 0\sqrt{p}\|\\ \|a + b\sqrt{p}\|\|x + y\sqrt{p}\| &= 1\end{aligned}$$

Por lo tanto, $\|a + b\sqrt{p})\|$ es unidad en $\mathbb{Z}$, por ende $\|a + b\sqrt{p}\| \in \{1. - 1\}$.

En el otro sentido, supongamos que $\|a + b\sqrt{p}\| = 1$, podemos comprobar que

$$(a + b\sqrt{p})(a - b\sqrt{p}) = (a^2 - bp^2) + (-ab + ab)\sqrt{p} = 1 + 0\sqrt{p}$$

Propiedad 143 $(\mathcal{U}(\mathbb{Z}[\sqrt{p}]), \cdot)$ *es un grupo abeliano.*

Observación: Note que los conjuntos anteriores incluido las operaciones, también es posible construirlos del siguiente modo, en $\mathbb{Z} \times \mathbb{Z}$ o en $\mathbb{Q} \times \mathbb{Q}$, se define las siguientes operaciones

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) \\ (a,b) \cdot (c,d) &= (ac + bdp, ad + bc) \end{aligned}$$

y con ellos tenemos la misma estructura, sin incorporar el símbolo $\sqrt{p}$ explícitamente.

Capítulo 5

Números Complejos.

En este capítulo, definiremos un nuevo conjunto que entrega solución a la ecuación $x^2 = -1$ y que contiene a los reales, de igual manera suponemos que i es una solución de esta ecuación, lo cual permite definir las operaciones esenciales para este nuevo conjunto.

Definición 47 *Definimos el conjunto de los números complejos como*

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$$

de donde $a+bi$ representa la forma binomial de un complejo el cual esta constituido por una parte Real que llamaremos

$$Re(a + bi) = a$$

y una parte imaginaria

$$Im(a + bi) = b$$

Observación: Tenemos que $Re(a + bi), Im(a + bi) \in \mathbb{R}$ y además

$$a + bi = Re(a + bi) + Im(a + bi)i$$

Observación: Sean $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{C}$ tenemos que dos números complejos son iguales, es decir

$$a_1 + b_1 i = a_2 + b_2 i \quad \text{si y sólo si} \quad a_1 = a_2 \quad \text{y} \quad b_1 = b_2$$

5.1. Estructura de Cuerpo.

Adición: Sean $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}$ definiremos la adición en $\mathbb{C}$ como

$$z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i$$

Multiplicación: Sean $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}$ definiremos la multiplicación en $\mathbb{C}$ como

$$z_1 \cdot z_2 = (a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$$

Propiedad 144 *La adición y multiplicación en $\mathbb{C}$ están bien definidos.*

5.1.1. Suma en $\mathbb{C}$.

Teorema 145 $(\mathbb{C}, +)$ *es un grupo abeliano.*

Demostración: Sean $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i$ y $z_3 = a_3 + b_3 i \in \mathbb{C}$
Asociativa:

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$$

Para ello $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i$ y $z_3 = a_3 + b_3 i$ entonces

$$\begin{aligned} z_1 + (z_2 + z_3) &= (a_1 + b_1 i) + [(a_2 + b_2 i) + (a_3 + b_3 i)] \\ &= (a_1 + b_1 i) + [(a_2 + a_3) + (b_2 + b_3) i] \\ &= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3) i \\ &= (a_1 + a_2) + (b_1 + b_2) i + (a_3 + b_3 i) \\ &= [(a_1 + b_1 i) + (a_2 + b_2 i)] + (a_3 + b_3 i) \\ &= [z_1 + z_2] + z_3. \end{aligned}$$

Por lo tanto la adición es asociativa en $\mathbb{C}$.
Neutro Aditivo: Existe $0 = 0 + 0i \in \mathbb{C}$ tal que cumple

$$z_1 + (0 + 0i) = z_1$$

Lo cual se comprueba del siguiente modo

$$z_1 + 0 + 0i = (a_1 + b_1 i) + (0 + 0i) = a_1 + b_1 i$$

luego tenemos que el neutro aditivo existe y es $0 = 0 + 0i$.
Inverso Aditivo: Sea $a_1 + b_1 i \in \mathbb{C}$, luego existe $(-a_1) + (-b_1)i \in \mathbb{C}$ tal que cumple

$$(a_1 + b_1 i) + (-a_1) + (-b_1)i = 0$$

Justifiquemos lo anterior

$$(a_1 + b_1 i) + (-a_1) + (-b_1)i = (a_1 - a_1) + (b_2 - b_2)i = 0 + 0i$$

Lo anterior demuestra que existe el inverso aditivo de $a_1 + b_1 i$ es $-a_1 - b_1 i$.
Conmutatividad: Debemos probar

$$z_1 + z_2 = z_2 + z_1$$

Para ello

$$\begin{aligned} z_1 + z_2 &= (a_1 + b_1 i) + (a_2 + b_2 i) \\ &= (a_1 + a_2) + (b_1 + b_2) i \\ &= (a_2 + a_1) + (b_2 + b_1) i \\ &= (a_2 + b_2 i) + (a_1 + b_1 i) \\ &= z_2 + z_1. \end{aligned}$$

Por lo tanto la adición en $\mathbb{C}$ es conmutativa.

5.1.2. Multiplicación en $\mathbb{C}$.

Teorema 146 *$(\mathbb{C}, \cdot)$ es un monoide abeliano, $(\mathbb{C}^*, \cdot)$ es un grupo abeliano, con $\mathbb{C}^* = \mathbb{C} - \{0\}$.*

Demostración: Sean $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i$ y $z_3 = a_3 + b_3 i \in \mathbb{C}$
Asociativa:

$$z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$$

Para ello

$$\begin{aligned}
z_1 \cdot (z_2 \cdot z_3) &= (a_1 + b_1 i) \cdot [(a_2 + b_2 i) \cdot (a_3 + b_3 i)] \\
&= (a_1 + b_1 i) \cdot [(a_2 a_3 - b_2 b_3) + (a_3 b_2 + a_2 b_3) i] \\
&= (a_1(a_2 a_3 - b_2 b_3) - b_1(a_3 b_2 + a_2 b_3)) + (a_1(a_2 b_3 + a_3 b_2) - b_1(a_2 a_3 - b_2 b_3)) i \\
&= (a_1 a_2 a_3 - a_1 b_2 b_3 - b_1 a_3 b_2 - b_1 a_2 b_3) + (a_1 a_2 b_3 + a_1 a_3 b_2 - b_1 a_2 a_3 + b_1 b_2 b_3) i \\
&= ((a_1 a_2 - b_1 b_2) a_3 - (a_1 b_2 + b_1 a_2) b_3) + ((a_1 a_2 + b_1 b_2) b_3 + (a_1 b_2 - b_1 a_2) a_3) i \\
&= [(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i] \cdot (a_3 + b_3 i) \\
&= [(a_1 + b_1 i) \cdot (a_2 + b_2 i)] \cdot (a_3 + b_3 i) \\
&= [z_1 + z_2] + z_3.
\end{aligned}$$

Por lo tanto la multiplicación es asociativa.
Neutro Multiplicativo: Existe $1 + 0i \in \mathbb{C}$, tal que

$$(a_1 + b_1 i) \cdot (1 + 0i) = a_1 + b_1 i$$

Lo cual se comprueba del siguiente modo

$$\begin{aligned}
(a_1 + b_1 i) \cdot (1 + 0i) &= (a_1 1 - b_1 0) + (1 b_1 + a_1 0) i \\
&= a_1 + b_1 i
\end{aligned}$$

luego tenemos que el neutro multiplicativo existe y es

$$1 = 1 + 0i.$$

Inverso Multiplicativo: Sea $a + bi \in \mathbb{C}^*$, existe $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i$, que cumple tenemos

$$(a + bi) \cdot \left(\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \right) = 1 + 0i$$

Justifiquemos lo anterior

$$\begin{aligned}
& (a + bi) \cdot \left(\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \right) \\
= & \left(a \frac{a}{a^2 + b^2} - b \frac{-b}{a^2 + b^2} \right) + \left(a \frac{-b}{a^2 + b^2} + b \frac{a}{a^2 + b^2} \right) i \\
= & \frac{a^2 + b^2}{a^2 + b^2} + \frac{-ba + ba}{a^2 + b^2} i \\
= & 1 + 0i
\end{aligned}$$

Por lo tanto el inverso multiplicativo de $a+bi$ es

$$\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i.$$

Conmutatividad: Debemos probar

$$z_1 \cdot z_2 = z_2 \cdot z_1$$

Para ello

$$\begin{aligned} z_1 \cdot z_2 &= (a_1+b_1i)\cdot(a_2+b_2i) \\ &= (a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i \\ &= (a_2a_1-b_2b_1)+(a_2b_1+b_2a_1)i \\ &= (a_2+b_2i)\cdot(a_1+b_1i) \\ &= z_2 \cdot z_1. \end{aligned}$$

Por lo tanto la multiplicación en $\mathbb{C}$ es conmutativa.
Notación: $a+bi \in \mathbb{C}$ y $c+di \in \mathbb{C}^*$ entonces

$$(a+bi):(c+di) = (a+bi)\cdot(c+di)^{-1}$$

Teorema 147 $(\mathbb{C},+,\cdot)$ *es un cuerpo.*

Demostración: Se ha demostrado anteriormente que $(\mathbb{C},+)$ y $(\mathbb{C}^*,\cdot)$ son grupos abelianos, luego falta ver la distributividad, es decir debemos demostrar

$$(a_1+b_1i)\cdot[(a_2+b_2i)+(a_3+b_3i)] = [(a_1+b_1i)\cdot(a_2+b_2i)+(a_1+b_1i)\cdot(a_3+b_3i)].$$

Veamos

$$(a_1+b_1i)\cdot[(a_2+b_2i)+(a_3+b_3i)] \;=\; (a_1+b_1i)\cdot[(a_2+a_3)+(b_2+b_3)i]$$

lo que es igual a

$$\begin{aligned} &= (a_1(a_2+a_3)-b_1(b_2+b_3))+(a_1(b_2+b_3)+b_1i(a_2+a_3))i \\ &= (a_1a_2+a_1a_3-b_1b_2-b_1b_3)+(a_1b_2+a_1b_3+a_2b_1+a_3b_1)i \\ &= (a_1a_2-b_1b_2+a_1a_3-b_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)i \\ &= [(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i]+[(a_1a_3-b_1b_3)+(a_1b_3+a_3b_1)i] \\ &= [(a_1+b_1i)\cdot(a_2+b_2i)]+[(a_1+b_1i)\cdot(a_3+b_3i)]. \end{aligned}$$

5.2. Conjugado en $\mathbb{C}$.

Definición 48 *Sea $z = a + bi \in \mathbb{C}$,*
Se define el conjugación de $a + bi$ por $a - bi$ y se denota de la siguiente forma:

$$\overline{a + bi} := a - bi.$$

Observación: La conjugación es una función dada por

$$\begin{array}{rccc} \overline{} & : & \mathbb{C} & \to & \mathbb{C} \\ & & a + bi & \mapsto & \overline{a + bi} = a - bi. \end{array}$$

Cumple las siguientes propiedades

Propiedad 148 *Sean $z_1, z_2 \in \mathbb{C}$ se cumple*

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$
3. $\overline{\overline{z}} = z$
4. $\overline{z} = z$ *si y sólo si* $b = 0$
5. $Re(z) = 0$ *si y sólo si* $\overline{z} = -z$

Demostración:

1. Tomemos $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}$

$$\begin{array}{rcl} \overline{z_1 + z_2} & = & \overline{(a_1 + b_1 i) + (a_2 + b_2 i)} \\ & = & \overline{(a_1 + a_2) + (b_1 + b_2)i} \\ & = & (a_1 + a_2) - (b_1 + b_2)i \\ & = & (a_1 - b_1 i) + (a_2 - b_2 i) \\ & = & \overline{(a_1 - b_1 i)} + \overline{(a_2 - b_2 i)} \\ & = & \overline{z_1} + \overline{z_2}. \end{array}$$

2. Consideremos $z_1 = a_1 + b_1 i, z_2 = a_2 + b_2 i \in \mathbb{C}$

$$\begin{array}{rcl} \overline{z_1 \cdot z_2} & = & \overline{(a_1 + b_1 i) \cdot (a_2 + b_2 i)} \\ & = & \overline{(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i} \\ & = & (a_1 a_2 - b_1 b_2) - (a_1 b_2 + a_2 b_1)i \\ & = & (a_1 a_2 - (-b_1)(-b_2)) + (a_1(-b_2) + a_2(-b_1))i \\ & = & (a_1 - b_1 i) \cdot (a_2 - b_2 i) \\ & = & \overline{(a_1 - b_1 i)} \cdot \overline{(a_2 - b_2 i)} \\ & = & \overline{z_1} \cdot \overline{z_2}. \end{array}$$

3. Tenemos $z = a + bi$ luego

$$\begin{aligned} \overline{\overline{z}} &= \overline{\overline{(a+bi)}} \\ &= \overline{(a-bi)} \\ &= a+bi \\ &= z. \end{aligned}$$

4. Si $\overline{z} = z$ por demostrar que $b = 0$, luego

$$\overline{z} = a - bi$$

pero $\overline{z} = z$ entonces

$$\begin{aligned} a - bi &= a + bi \\ -bi &= bi \\ 2bi &= 0. \end{aligned}$$

Como $2 \neq 0$ e $i = \sqrt{-1} \neq 0$ no queda mas que $b = 0$. Por otro lado debemos demostrar que

Si $b = 0$ por demostrar que $\overline{z} = z$, como $b = 0$ entonces $z = a + 0i = a$, calculemos su conjugado

$$\overline{z} = a - 0i = a = z.$$

5. Primero demostremos que

Si $Re(z) = 0$ por demostrar que $\overline{z} = -z$. Como

$$Re(z) = Re(a + bi) = 0$$

entonces $z = bi$, calculemos

$$\overline{z} = \overline{bi} = -bi = -z.$$

5.3. Módulo de un Número Complejo.

Definición 49 *Sea $a + bi \in \mathbb{C}$, se define el módulo de $a + bi$ por $\sqrt{a^2 + b^2}$ y se denota por*

$$|a + bi| := \sqrt{a^2 + b^2}.$$

y la norma de del complejo

$$\|a + bi\| := a^2 + b^2.$$

Observación: La módulo es una función dada por

$$\begin{array}{rccl} |\ |\ : & \mathbb{C} & \to & \mathbb{R} \\ & a + bi & \mapsto & |a + bi| = \sqrt{a^2 + b^2}. \end{array}$$

Teorema 149 *Sean* $a+bi, c+di \in \mathbb{C}$

i) $|(\overline{a+bi})| = |a+bi|$

ii) $|a+bi| = \sqrt{(a+bi)\overline{(a+bi)}}$

iii) $|(a+bi)\cdot(c+di)| = |a+bi|\cdot|c+di|$

iv) $\mid a+bi \mid = 0$ *si y sólo si* $a=0 \wedge b=0$.

v) $\mid (a+bi)+(c+di) \mid \leq \mid a+bi \mid + \mid c+di \mid$

Demostración:

iii) Tomemos $z_1 = a_1+b_1i, z_2 = a_2+b_2i \in \mathbb{C}$ tenemos

$$\begin{aligned}
\mid z_1\cdot z_2 \mid &= \mid (a_1+b_1i)\cdot(a_2+b_2i) \mid \\
&= \mid (a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i \mid \\
&= \sqrt{(a_1a_2-b_1b_2)^2+(a_1b_2+a_2b_1)^2} \\
&= \sqrt{a_1^2a_2^2-2a_1a_2b_1b_2+b_1^2b_2^2+a_1^2b_2^2+2a_1a_2b_1b_2+a_2^2b_1^2} \\
&= \sqrt{a_1^2a_2^2+b_1^2b_2^2+a_1^2b_2^2+a_2^2b_1^2} \\
&= \sqrt{(a_1^2+b_1^2)\cdot(a_2^2+b_2^2)} \\
&= \sqrt{(a_1^2+b_1^2)}\cdot\sqrt{(a_2^2+b_2^2)} \\
&= \sqrt{(a_1+b_1i)(a_1-b_1i)}\cdot\sqrt{(a_2+b_2i)(a_2-b_2i)} \\
&= \mid a_1+b_1i \mid \cdot \mid a_2+b_2i \mid \\
&= \mid z_1 \mid \cdot \mid z_2 \mid .
\end{aligned}$$

Teorema 150 *Sea* $\mathbb{U} := \{z \in \mathbb{C} \mid \mid z \mid = 1\}$*, entonces* $(\mathbb{U},\cdot)$ *es un grupo abeliano*

Demostración: La demostración quedará como ejercicio para el estudiante.

5.3.1. Ecuación de Segundo Grado

Sean $a,b,c \in \mathbb{C}$ con $a \neq 0$. La ecuación de segundo grado

$$az^2+bz+c=0 \Longleftrightarrow (2az+b)^2 = b^2-4ac$$

con un cambio de variable se obtiene

$$w^2 = \Delta$$

Observación: Las ecuación del tipo $w^2 = r \in \mathbb{R}$, se separan en dos caso, si $r \geq 0$, entonces $w = \pm\sqrt{r}$, y si $r < 0$, entonces $w = \pm\sqrt{|r|}i$.

Veremos ahora el caso en que no Δ no es real. Consideremos $w = x + yi$, $\Delta = r + ti$. Luego se tiene que $x^2 - y^2 + 2xyi = r + ti$, es decir,

$$\begin{array}{|rcl} x^2 - y^2 & = & r \\ 2xy & = & t \end{array}$$

Amplificando por $4x^2$ la primer ecuación, y la segunda elevando al cuadrado, al sumar obtenemos

$$4x^4 = 4x^2 r + t^2$$

es decir,

$$4x^4 - 4x^2 r - t^2 = 0$$

luego $\Delta_1 = 16r^2 + 16t^2$,

$$x^2 = \frac{4r \pm \sqrt{16r^2 + 16t^2}}{8} = \frac{r \pm \sqrt{r^2 + t^2}}{2}$$

Uno de los valores no es admisible, luego

$$x = \pm\sqrt{\frac{r + \sqrt{r^2 + t^2}}{2}}$$

despejando de la primer a ecuación obtenemos que

$$y = \pm\sqrt{\frac{-r + \sqrt{r^2 + t^2}}{2}}$$

Verificando la segunda ecuación, obtenemos $\pm|s| = s$, luego sólo obtenemos signo posible a la vez, es decir,

$$w = \pm\left[\sqrt{\frac{\sqrt{r^2 + t^2} + r}{2}} + sg(t)\sqrt{\frac{\sqrt{r^2 + t^2} - r}{2}}i\right]$$

Propiedad 151 *La ecuación de segundo grado*

$$\delta^2 = \Delta, \ \textit{con } Im(\Delta) \neq 0$$

tiene dos soluciones

$$\delta = \pm\left[\sqrt{\frac{|\Delta| + Re(\Delta)}{2}} + sg(Im(\Delta))\sqrt{\frac{|\Delta| - Re(\Delta)}{2}}i\right]$$

Propiedad 152 *Dada la ecuación de segundo grado*

$$az^2 + bz + c = 0 \ \textit{con } a \neq 0$$

el discriminante de la ecuación de segundo grado es $\Delta = b^2 - 4ac = \delta^2$ *y tiene dos soluciones*

$$z = \frac{-b \pm \delta}{2a}$$

Ejemplo 109 *Resolver las ecuaciones e segundo grado*

1. $z^2 + (1+2i)z + (3-i) = 0$
2. $(4+2i)z^2 - 2iz + (8-i) = 0$

Solución:

1. Dado la ecuación $z^2 + (1+2i)z + (3-i) = 0$, tenemos

$$\Delta = (1+2i)^2 - 4(3-i) = 1 + 4i - 4 - 12 + 4i = -15 + 8i = \delta^2$$

Calculemos $|\Delta| = 17$, $Re(\Delta) = -15$, $sg(Im(\Delta)) = 1$ luego

$$\delta = \pm\left[\sqrt{\frac{17-15}{2}} + (1)\sqrt{\frac{17+15}{2}}i\right] = \pm\left[1+4i\right]$$

De lo cual obtenemos

$$z = \frac{-(1+2i) \pm (1+4i)}{2}$$

o bien

$$z_0 = i; \quad z_1 = -1 - 3i$$

2. Dada la ecuación $(4+2i)z^2 - 2iz + (8-i) = 0$, tenemos

$$\Delta = (-2i)^2 - 4(4+2i)(8-i) = -4(35+12i) = \delta^2$$

Calculemos $|\Delta| = 148$, $Re(\Delta) = -140$, $sg(Im(\Delta)) = -1$, luego

$$\delta = \pm\left[\sqrt{\frac{148-140}{2}} + (-1)\sqrt{\frac{148+140}{2}}i\right] = \pm\left[2-12i\right]$$

De lo cual obtenemos

$$z = \frac{2i \pm (2-12i)}{2(4+2i)} = \frac{i \pm (1-6i)}{4+2i}$$

o bien

$$z_0 = \frac{1-5i}{4+2i} = -\frac{3}{10} - \frac{11}{10}i; \qquad z_1 = \frac{-1+7i}{4+2i} = \frac{1}{2} + \frac{3}{2}i$$

5.4. Representación Cartesiana de $\mathbb{C}$.

El plano euclidiano

$$\mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\},$$

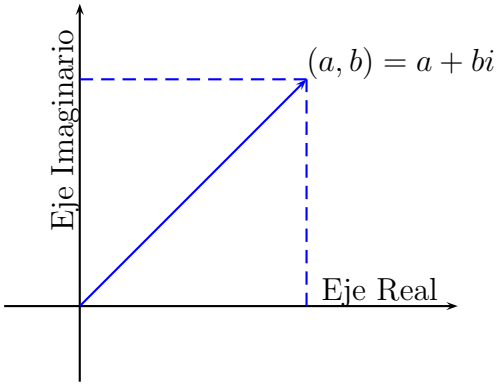
el conjunto número complejo

$$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$$

y la siguiente correspondencia

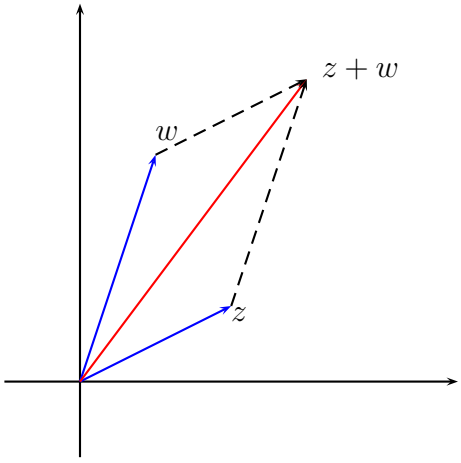
$$\begin{array}{rccl} f & : & \mathbb{R}^2 & \to & \mathbb{C} \\ & & (a,b) & \mapsto & f(a,b) = a+bi. \end{array}$$

de esta manera todo número complejo puede ser representado de la siguiente manera

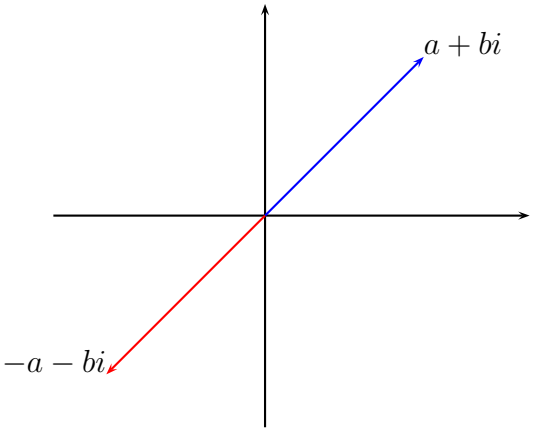


Suma.

Adición: Sean $z, w \in \mathbb{C}$, donde $z = a + bi$ y $w = c + di$. construimos el paralelogramo con los vectores z y w

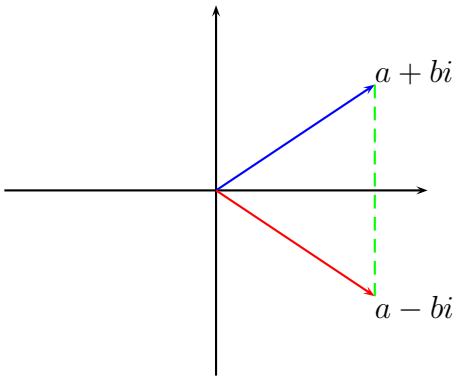


Inverso aditivo: La representación del inverso aditivo de un complejo en el plano es del siguiente figura



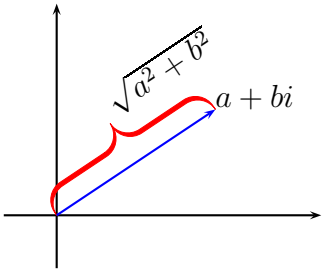
Conjugación en el plano.

Dada $a + bi \in \mathbb{C}$, el conjugado es $a - bi$



Módulo en el plano.

Dada $a+bi \in \mathbb{C}$, el módulo es $\sqrt{a^2+b^2}$



Traslación en el plano.

Otra función que actúa de forma geométrica sobre los vectores, es la traslación, dada por

$$\begin{array}{rccl} T_w & : & \mathbb{C} & \to & \mathbb{C} \\ & & z & \mapsto & T_w(z) = z + w. \end{array}$$

Distancia en el plano.

En el plano esta definida la distancia entre dos pares ordenados, que se puede interpretar en los números complejos del siguiente modo.

Sean $z, w \in \mathbb{C}$, donde $z = a+bi$ y $w = c+di$, entonces la distancia entre z y w esta dada por

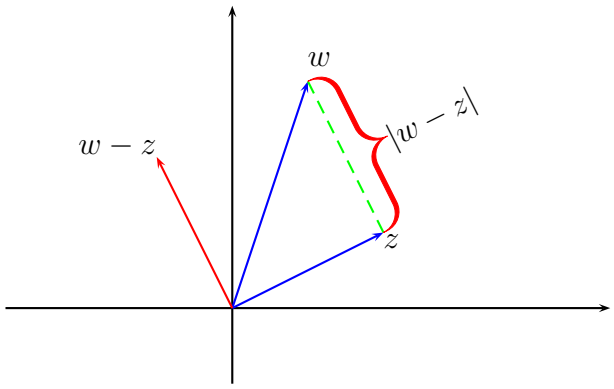
$$dist(z,w) = \mid w - z \mid$$

es decir,

$$\mid z - w \mid \;\; = \;\; \sqrt{(a-c)^2 + (b-d)^2}.$$

Definición 50 *Sean $z = a+bi, w = c+di \in \mathbb{C}$ tenemos*

$$dist(z,w) = \sqrt{(a-c)^2 + (b-d)^2}$$



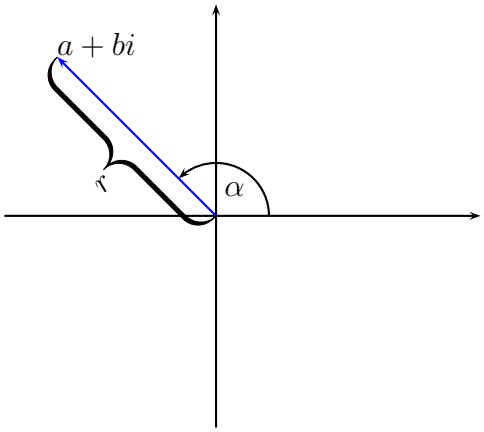
5.5. Forma Polar de un Número Complejo.

Dado un número complejo $z = a + bi \in \mathbb{C}$, tiene su representación geométrica (a, b) en el plano euclidiano, dada las coordenadas en el plano existe un único α y r, tal que

$$(a, b) = (r\cos(\alpha), r\,\text{sen}(\alpha))$$

donde r es el módulo del complejo y α es ángulo con el semi eje positivo real.

$$r = \sqrt{a^2 + b^2},\ \arg(z) = \alpha$$



Notación: Al considerar la forma polar de $z \in \mathbb{C}$, la podemos representar como

$$z = r(\cos(\alpha) + i\,\text{sen}(\alpha)) = rcis(\alpha)$$

Igualdad en forma Polar Dada dos complejos en forma polar $r_1cis(\alpha),\ r_2cis(\beta)$ entonces se cumple que

$$r_1cis(\alpha) = r_2cis(\beta) \text{ si y sólo si } r_1 = r_2 \text{ y } \alpha = \beta + 2k\pi, \text{ con } k \in \mathbb{Z}$$

5.5.1. Multiplicación de Complejos.

Teorema 153 *Sean $z_1, z_2 \in \mathbb{C}$ con forma polar*

$$z_1 =\mid z_1 \mid cis(\alpha) \qquad z_2 =\mid z_2 \mid cis(\beta)$$

entonces

1. $z_1 \cdot z_2 =\mid z_1 \mid \cdot \mid z_2 \mid cis(\alpha+\beta)$.
2. $(z_1)^{-1} = \frac{1}{\mid z_1 \mid} cis(-\alpha)$.
3. $z_1 : z_2 = \frac{\mid z_1 \mid}{\mid z_2 \mid} \mid cis(\alpha-\beta)$.
4. $\overline{z_1} =\mid z_1 \mid cis(-\alpha)$.

Demostración: Veamos el producto

$$\begin{aligned} z_1 \cdot z_2 &= (\mid z_1 \mid cis(\alpha)) \cdot (\mid z_2 \mid cis(\beta)) \\ &= \mid z_1 \mid \cdot \mid z_2 \mid (\cos(\alpha) + i\,\mathrm{sen}(\alpha)) \cdot (\cos(\beta) + i\,\mathrm{sen}(\beta)) \\ &= \mid z_1 \mid \cdot \mid z_2 \mid (\cos(\alpha)\cos(\beta) + \cos(\alpha)\,\mathrm{sen}(\beta)i + \cos(\beta)\,\mathrm{sen}(\alpha)i - \mathrm{sen}(\alpha)\,\mathrm{sen}(\beta)) \\ &= \mid z_1 \mid \cdot \mid z_2 \mid (\cos(\alpha)\cos(\beta) - \mathrm{sen}(\alpha)\,\mathrm{sen}(\beta)) + (\cos(\alpha)\,\mathrm{sen}(\beta) + \cos(\beta)\,\mathrm{sen}(\alpha))i \end{aligned}$$

por identidades trigonométrica

$$\begin{aligned} \mathrm{sen}(\alpha+\beta) &= \mathrm{sen}(\alpha)\cos(\beta) + \mathrm{sen}(\beta)\cos(\alpha) \\ \cos(\alpha+\beta) &= \cos(\alpha)\cos(\beta) - \mathrm{sen}(\alpha)\,\mathrm{sen}(\beta) \end{aligned}$$

obtenemos

$$\begin{aligned} z_1 \cdot z_2 &= \mid z_1 \mid \cdot \mid z_2 \mid (\cos(\alpha)\cos(\beta) - \mathrm{sen}(\alpha)\,\mathrm{sen}(\beta)) + (\cos(\alpha)\,\mathrm{sen}(\beta) + \cos(\beta)\,\mathrm{sen}(\alpha))i \\ &= \mid z_1 \mid \cdot \mid z_2 \mid (\cos(\alpha+\beta) + \mathrm{sen}(\alpha+\beta)i) \\ &= \mid z_1 \mid \cdot \mid z_2 \mid cis(\alpha+\beta). \end{aligned}$$

Veremos el Inverso Multiplicativo en forma Polar.

$$\begin{aligned} z^{-1} &= (\mid z \mid cis(\alpha))^{-1} = \frac{1}{\mid z \mid cis(\alpha)} \\ z^{-1} &= \frac{1}{\mid z \mid (\cos(\alpha) + \mathrm{sen}(\alpha)i)} \quad / \cdot \frac{\cos(\alpha) - \mathrm{sen}(\alpha)i}{\cos(\alpha) - \mathrm{sen}(\alpha)i} \\ &= \frac{1}{\mid z \mid} \frac{\cos(\alpha) - \mathrm{sen}(\alpha)i}{\cos^2(\alpha) - \mathrm{sen}^2(\alpha)i^2} \\ &= \frac{1}{\mid z \mid} \frac{\cos(\alpha) - \mathrm{sen}(\alpha)i}{\cos^2(\alpha) + \mathrm{sen}^2(\alpha)} \\ &= \frac{1}{\mid z \mid} \cos(\alpha) - \mathrm{sen}(\alpha)i \\ &= \frac{1}{\mid z \mid} cis(-\alpha). \end{aligned}$$

Ahora la División de Complejos en forma Polar:
sea $z_2 =\mid z_2 \mid cis(\beta) \neq 0$

$$\frac{z_1}{z_2} = z_1 \cdot z_2^{-1} = (\mid z_1 \mid cis(\alpha))(\mid z_2 \mid cis(\beta))^{-1}$$

por lo anterior tenemos

$$(\mid z_2 \mid cis(\beta))^{-1} \quad = \quad \frac{1}{\mid z_2 \mid} \, cis(-\beta)$$

reemplazando obtenemos

$$\begin{aligned} z_1 \cdot z_2^{-1} &= (\mid z_1 \mid \ cis(\alpha))\frac{1}{\mid z_2 \mid} \, cis(-\beta) \\ &= \frac{\mid z_1 \mid}{\mid z_2 \mid} \, cis(\alpha)cis(-\beta) \end{aligned}$$

por multiplicación de complejos obtenemos

$$z_1 \cdot z_2^{-1} = \frac{\mid z_1 \mid}{\mid z_2 \mid} \, cis(\alpha - \beta)$$

Finalmente la conjugación, para ello calculemos el conjugado

$$\begin{aligned} \overline{z} &= \overline{\mid z \mid \cos(\alpha) + \mid z \mid \operatorname{sen}(\alpha)i} \\ &= \mid z \mid \cos(\alpha) - \mid z \mid \operatorname{sen}(\alpha)i \\ &= \mid z \mid (\cos(\alpha) - \operatorname{sen}(\alpha)i). \end{aligned}$$

Recordemos que la función coseno es par y la función seno es impar luego

$$\begin{aligned} \overline{z} &= \mid z \mid (\cos(\alpha) + \operatorname{sen}(-\alpha)i) \\ &= \mid z \mid (\cos(-\alpha) + \operatorname{sen}(-\alpha)i) \\ &= \mid z \mid cis(-\alpha). \end{aligned}$$

□

5.5.2. Teorema de Moivre.

El siguiente teorema es la generalización natural del teorema anterior y nos ayuda en poder calcular las potencias de un número complejo.

Teorema 154 *Sea $z \in \mathbb{C}, n \in \mathbb{N}$ donde $z = \mid z \mid \ cis(\alpha)$ entonces*

$$z^n = \mid z \mid^n \ cis(n\alpha)$$

Demostración: Tomemos $z = \mid z \mid \ cis(\alpha)$ y calculemos su potencia n-ésima

$$\begin{aligned} z^n &= (\mid z \mid \ cis(\alpha))^n \\ &= \mid z \mid^n \ cis^n(\alpha). \end{aligned}$$

Veamos el valor de $cis^n(\alpha)$

$$\begin{aligned} cis^n(\alpha) &= cis^{n-1}(\alpha)cis(\alpha) \\ &= cis((n-1)\alpha)cis(\alpha) \\ &= cis((n-1)\alpha + \alpha) \\ &= cis(n\alpha) \end{aligned}$$

La demostración es por inducción y sólo hemos realizado la parte medular □

5.5.3. Raíz n-ésima de un Complejo.

Encontrar o determinar los números complejos que a la n-esima potencia nos dan un complejo conocido, es decir, dado $w \in \mathbb{C}$, cuales son los $z \in \mathbb{C}$ tales que $z^n = w$. Tales números complejos son llamados raíz n-ésima de w.

Propiedad 155 *Sea $w \in \mathbb{C}, n \in \mathbb{N}$ donde $w =\mid w \mid cis(\alpha)$ entonces la soluciones de la ecuación $z^n = w$ son*

$$z_k = \sqrt[n]{\mid w \mid}\ cis\left(\frac{\alpha + 2k\pi}{n}\right)$$

con $k = 0, 1, \cdots, n-1$, llamadas las raíz n-ésima de w

Demostración: Supongamos que $z = |z|cis(\beta)$ entonces

$$\begin{aligned} z^n &= w \\ (\mid z \mid \ cis(\beta))^n &= \mid w \mid \ cis(\alpha) \\ \mid z \mid^n \ cis^n(\beta) &= \mid w \mid \ cis(\alpha) \end{aligned}$$

Por teorema 154 tenemos

$$\begin{aligned} \mid z \mid^n \ cis^n(\beta) &= \mid w \mid \ cis(\alpha) \\ \mid z \mid^n \ cis(n\beta) &= \mid w \mid \ cis(\alpha) \end{aligned}$$

Luego

$$\mid z \mid^n = \mid w \mid \quad \text{y} \quad cis(n\beta) = cis(\alpha)$$

Por lo tanto

$$\mid z \mid = \sqrt[n]{\mid w \mid}$$

y además

$$cis(n\beta) = cis(\alpha).$$

Por ser un punto de la circunferencia unitaria luego tenemos

$$\begin{aligned} n\beta &= \alpha + 2k\pi \quad k \in \mathbb{Z} \\ \beta &= \frac{\alpha + 2k\pi}{n} \quad k = 0, 1, \cdots, n-1 \end{aligned}$$

Claramente todas $z_k = \sqrt[n]{\mid w \mid} cis(\frac{\alpha+2k\pi}{n})$ es una solución de la ecuación, ya que

$$\begin{aligned} z_k^n &= \left(\sqrt[n]{\mid w \mid} cis\left(\frac{\alpha + 2k\pi}{n}\right)\right)^n \\ &= \left(\sqrt[n]{\mid w \mid}\right)^n \left(cis\left(\frac{\alpha + 2k\pi}{n}\right)\right)^n \\ &= \mid w \mid cis(\alpha + 2k\pi) = \mid w \mid cis(\alpha) = w \end{aligned}$$

□

Observación: Un caso particular de la raíz n-esima de un complejo es la raíz n- esima de la unidad o 1.

Ejemplo 110 *Resolver*

$$z^n = 1$$

Solución: Antes de resolver la ecuación notemos que $1 = cis(0)$, la ecuación esta dada por $z^n = cis(0)$. Por lo tanto

$$\begin{aligned} z_k &= cis\left(\frac{0 + 2k\pi}{n}\right) = cis\left(\frac{2k\pi}{n}\right) = cis^k\left(\frac{2\pi}{n}\right)) \\ & k \in 0, 1, 2, \ldots, (n-1) \end{aligned}$$

Observación: Las raíces n-ésimas de la unidad, geométricamente representan los vertices de un polígono regular de n lados inscrito en la circunferencia unitaria.

Si consideramos el conjunto de las n raíces de la unidad

$$\mathcal{R}_n := \left\{ cis^k\left(\frac{2\pi}{n}\right) \mid k = 0, 1, \cdots, n-1 \right\}$$

Propiedad 156 *El conjunto $\mathcal{R}_n$ es un grupo abeliano.*

5.6. Los Enteros Gaussianos.

Definición 51 *Sean $\mathbb{Z}$ el conjunto de los números enteros. Se define los enteros Gaussianos por:*

$$\mathbb{Z}[i] := \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Observación: Note que tenemos las operaciones definida en $\mathbb{C}$, solamente no se cumple la propiedad del inverso multiplicativo, además tiene sentido el conjugado, el módulo y la norma.

Teorema 157 *$(\mathbb{Z}[i], +, \cdot)$ es un anillo conmutativo.*

5.6.1. La Norma de $\mathbb{Z}[i]$.

Definición 52 *Sea $a + bi \in \mathbb{Z}[i]$, definiremos la norma de $a + bi$ como*

$$\|a + bi\| := a^2 + b^2.$$

Observación: La norma la podemos considerar como una función de la siguiente forma

$$\begin{array}{rccl} \| \quad \| & : & \mathbb{Z}[i] & \to & \mathbb{Z} \\ & & a + bi & \mapsto & \|a + bi\| = a^2 + b^2. \end{array}$$

Propiedad 158 *Tenemos que la norma cumple con la siguiente propiedad*

$$\|(a_1 + b_1 i) \cdot (a_2 + b_2 i)\| = \|a_1 + b_1 i\| \cdot \|a_2 + b_2 i\|.$$

Demostración: Sean $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{Z}[i]$, luego

$$\begin{array}{rcl} \|(a_1 + b_1 i) \cdot (a_2 + b_2 i)\| & = & \|(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i\| \\ & = & (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \\ & = & a_1^2 a_2^2 - 2 a_1 a_2 b_1 b_2 + b_1^2 b_2^2 + a_1^2 b_2^2 + 2 a_1 b_2 a_2 b_1 + a_2^2 b_1^2 \\ & = & a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 \\ & = & a_1^2 a_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + b_1^2 b_2^2 \\ & = & (a_1^2 + b_1^2) \cdot (a_2^2 + b_2^2) \\ & = & \|a_1 + b_1 i\| \cdot \|a_2 + b_2 i\|. \end{array}$$

Como la función norma tiene como resultante un número en $\mathbb{Z}$, tenemos que las propiedades de $\mathbb{Z}$ se pueden heredar a la función norma.
Observación: Repasaremos los conceptos anteriormente definidos para extensiones cuadráticas de los números racionales

5.6.2. Unidades de $\mathbb{Z}[i]$.

Definición 53 *Sea $u \in \mathbb{Z}[i]$, se dice que u es una unidad de $\mathbb{Z}[i]$ si y sólo existe $v \in \mathbb{Z}[i]$ tal que multiplicados por u, se obtiene el resultado 1, es decir,*

$$u \in \mathcal{U}(\mathbb{Z}[i]) \quad \textit{si y sólo si, existe } v \in \mathbb{Z}[i] \quad \textit{tal que} \quad u \cdot v = 1$$

Teorema 159 *Sea $z \in \mathbb{Z}[i]$ diremos*

$$z \in \mathcal{U}(\mathbb{Z}[i]) \quad \textit{si y sólo si} \quad \|z\| = 1$$

Demostración: Si $z \in \mathcal{U}(\mathbb{Z}[i])$ por demostrar que $\|z\| = 1$
Como $z \in \mathcal{U}(\mathbb{Z}[i])$ entonces $\exists\ v \in \mathbb{Z}[i]$ tal que

$$\begin{aligned} z \cdot v &= 1 \quad /\| \quad \| \\ \|z \cdot v\| &= \|1\| \\ \|z\| \cdot \|v\| &= 1 \end{aligned}$$

Como $\|z\|, \|v\| \in \mathbb{Z}$ y tienen inversos multiplicativos entonces

$$(\|z\| = 1 \ \wedge \ \|v\| = 1) \quad \vee \quad (\|z\| = -1 \ \wedge \ \|v\| = -1)$$

pero $\|z\|$ y $\|v\|$ son suma de números positivos entonces

$$\|v\| = 1 \quad \wedge \quad \|v\| = 1$$

En el otro sentido, si $\|v\| = 1$ por demostrar $z \in \mathcal{U}(\mathbb{Z}[i])$ quedará como ejercicio para el lector. □

Definición 54 *Sean $z \in \mathbb{Z}[i] - \{0\}$, $w \in \mathbb{Z}[i]$, se dice que z divide a w si y sólo si existe $u \in \mathbb{Z}[i]$, tal que $w = zu$, es decir*

$$z|w \iff (\exists\ u \in \mathbb{Z}[i])(w = z \cdot u).$$

Ejemplo 111

1. *Determine* $3|6i \in \mathbb{Z}[i]$.
2. *Determine* $3i|6 \in \mathbb{Z}[i]$.
3. *Determine* $(2-i)|(1+2i) \in \mathbb{Z}[i]$.
4. *Determine* $(3-i)|(2+5i) \in \mathbb{Z}[i]$.

Solución:

1. Determine $3|6i \in \mathbb{Z}[i]$. Como $6i = 3(2i)$, con $u = 2i \in \mathbb{Z}[i]$ Por lo tanto $3|6i$.
2. Determine $3i|6 \in \mathbb{Z}[i]$. Ya que $6 = 3i(-2i)$, con $u = -2i \in \mathbb{Z}[i]$ Por lo tanto $3i|6$.
3. Determine $(2-i)|(1+2i) \in \mathbb{Z}[i]$. Supongamos que $(2-i)|(1+2i)$, luego existen $a, b \in \mathbb{Z}$ tal que:

$$\begin{aligned} 1+2i &= (2-i) \cdot (a+bi) \\ 1+2i &= 2a+2bi-ai+b \\ 1+2i &= 2a+b+(-a+2b)i \end{aligned}$$

Luego tenemos el sistema

$$\begin{array}{rcl|} 1 & = & 2a+b \\ 2 & = & -a+2b \\ \hline \end{array}$$

Amplificando por 2 la segunda ecuación y sumando obtenemos

$$5 = 5b$$

de lo cual $b = 1$, reemplazando obtenemos $a = 0$, luego tenemos

$$1 + 2i = (2 - i)(i)$$

Por lo tanto $2 - i$ divide a $1 + 2i$ en $\mathbb{Z}[i]$.

4. Determine $(3-i)|(2+5i) \in \mathbb{Z}[i]$. Supongamos que $(3-i)|(2+5i)$, luego existen $a, b \in \mathbb{Z}$ tal que:

$$\begin{array}{rcl} 2+5i & = & (3-i)\cdot(a+bi) \\ 2+5i & = & 3a+3bi-ai+b \\ 2+5i & = & 3a+b+(-a+3b)i \end{array}$$

Luego tenemos el sistema

$$\begin{array}{rcl|} 2 & = & 3a+b \\ 5 & = & -a+3b \\ \hline \end{array}$$

Amplificando por 3 la segunda ecuación y sumando obtenemos

$$17 = 10b$$

de lo cual $10|17$, lo que es imposible

Por lo tanto $3 - i$ no divide a $2 + 5i$ en $\mathbb{Z}[i]$

Propiedad 160 *Sean $z, w \in \mathbb{Z}[i]$ entonces se cumple*

$$z|w \quad \textit{en } \mathbb{Z}[i] \quad \textit{implica} \quad \|z\| \mid \|w\| \quad \textit{en } \mathbb{Z}.$$

Demostración: Sean $z, w \in \mathbb{Z}[i]$, tal que $z|w$, luego existe $u \in \mathbb{Z}[i]$ tal que

$$\begin{array}{rcl} w & = & z\cdot u \quad /\| \quad \| \\ \|w\| & = & \|z\cdot u\| \\ \|w\| & = & \|z\|\cdot\|u\| \end{array}$$

De lo cual obtenemos

$$\|z\| \mid \|w\|.$$

□

Definición 55 *Sea $z \in \mathbb{Z}[i] - \mathcal{U}(\mathbb{Z}[i])$ no nulo, se dice que z es* **primo** *en $\mathbb{Z}[i]$ si y sólo si*

$$(\forall w \in \mathbb{Z}[i] - \mathcal{U}(\mathbb{Z}[i]))(\exists u \in \mathcal{U}(\mathbb{Z}[i]))(w|z \Rightarrow w = zu)$$

Observación: Sea p es un entero distinto de cero y tal que $p = a^2 + b^2$ entonces p no es primo de $\mathbb{Z}[i]$, ya que

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

Ejemplo 112 *No son primos en $\mathbb{Z}[i]$*
$2 = 1^2 + 1^2 = (1 + i)(1 - i)$; $5 = 2^2 + 1^2 = (2 - i)(2 + i)$; $13 = 3^2 + 2^2 = (3 - 2i)(3 + 2i)$

Ejemplo 113 *$1 + 2i$ es primo en $\mathbb{Z}[i]$*

Solución: $1 + 2i$ es no nulo y no es unidad. Sea $w \in \mathbb{Z}[i] - \mathcal{U}(\mathbb{Z}[i]$ tal que $w|z$, luego existe $u \in \mathbb{Z}[i]$ tal que $z = wu$, calculando la norma obtenemos que $\|z\| = \|wu\| = \|w\|\|u\|$, por lo tanto $5 = \|w\|\|u\|$, pero w no es unidad, luego $\|w\| \neq 1$, de este modo se tiene que $\|u\| = 1$, por lo tanto invertible $w = zu^{-1} = z\overline{u}$, luego $1 + 2i$ es primo en $\mathbb{Z}[i]$.

Teorema 161 *Sea p un número primo en $\mathbb{Z}$ tal que $p \equiv 1(\mathtt{mod}\ 4)$ entonces p no es un número primo en $\mathbb{Z}[i]$*

Demostración: Sea p primo tal que $p \equiv 1(\mathtt{mod}\ 4)$, luego existe $x \in \mathbb{Z}$ tal que $x^2 \equiv -1(\mathtt{mod}\ p)$, luego

$$p|(x - i)(x + i)$$

Supongamos que p es primo en $\mathbb{Z}[i]$ entonces

$$p|(x - i) \quad \vee \quad p|(x + i)$$

existe $a, b \in \mathbb{Z}$ tal que

$$\begin{array}{rcl} x - i = p(a + bi) & \vee & x + i = p(a + bi) \\ x - i = pa + pbi & \vee & x + i = pa + pbi \end{array}$$

de lo cual $pb = \pm 1$, luego es una unidad en $\mathbb{Z}$, lo que es una contradicción. Por lo tanto p no es un número primo en $\mathbb{Z}[i]$ □

5.7. Algoritmo de la División

El algoritmo de la división en $\mathbb{Z}$, corresponde a dado dos elementos $a, b \in \mathbb{Z}$, con a no nulo existen $q, r \in \mathbb{Z}$, tales que $b = aq + r$, con $0 \leq r < |a|$.

La anterior se puede reescribir del siguiente modo, existen $q, r \in \mathbb{Z}$, tales que $b = aq + r$, con $0 \leq |r| \leq \frac{|a|}{2}$.

Por ejemplo;

$$15 = 4(3) + 3 = 4(4) + (-1) \qquad -13 = 4(-4) + 3 = 4(-3) + (-1)$$

los valores anteriores eran únicos, pero con la condición actual no son únicos, $14 = 4(3) + 2 = 4(4) + (-2)$.

Propiedad 162 *Sean $z, w \in \mathbb{Z}[i]$, con z no nulo, entonces existen $q, r \in \mathbb{Z}[i]$, tales que $w = zq + r$, con $0 \leq \|r\| < \|z\|$.*

Demostración: Primer caso: Sea $w = a + bi$ y $z = c$, con $a, b, c \in \mathbb{Z}$. Luego existen $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, tales que

$$a = cq_1 + r_1 \qquad b = cq_2 + r_2, \text{ con } |r_i| \leq \frac{|c|}{2}.$$

Reescribiendo tenemos $a + bi = c(q_1 + q_2 i) + (r_1 + r_2 i)$

$$\|r_1 + r_2 i\| = r_1^2 + r_2^2 \leq \frac{c^2}{2} < c^2$$

De este modo tenemos existen $q = q_1 + q_2 i, r = r_1 + r_2 i$, tal que $w = zq + r$ con $0 \leq \|r\| < \|z\|$.

Segundo caso: Sea $w = a + bi$ y $z = c + di$, con $a, b, c, d \in \mathbb{Z}$. Luego por el caso anterior existen $q, r_1 \in \mathbb{Z}$, tales que

$$w\overline{z} = (a + bi)(c - di) = (c^2 + d^2)q + r_1 \text{ con } \|r_1\| < \|c^2 + d^2\|.$$

de lo cual se tiene que $r_1 = (a + bi)(c - di) - (c^2 + d^2)q = [(a + bi) - (c + di)q](c - di)$.

Definamos $r = (a + bi) - (c + di)q$, luego tenemos $r_1 = r(c - di)$

$$\|r\|(c^2 + d^2) = \|r(c - di)\| = \|r_1\| \leq \|c^2 + d^2\|$$

Simplificando obtenemos $0 \leq \|r\| < \|z\|$ y se cumple que $w = zq + r$. □

Ejemplo 114 *En cada caso, determine $q, r \in \mathbb{Z}[i]$ tal que*

1. $13 + 21i = 4q + r$ *con* $\|r\| < \|4\|$
2. $7 + 2i = (3 + i)q + r$ *con* $\|r\| < \|3 + i\|$
3. $3 - 5i = (3 - 2i)q + r$ *con* $\|r\| < \|3 - 2i\|$

Solución:

1. $13 + 21i = 4q + r$ con $\|r\| < \|4\|$ Como $15 = 4(4) - 1,\ 21 = 4(5) + 1$, por lo tanto

   $$13 + 21i = (4(4) - 1) + (4(5) + 1)i = 4(4 + 5i) + (-1 + i)$$

   Además $\| - 1 + i\| = 2 < 16 = \|4\|$.

2. $7+2i = (3+i)q+r$ con $\|r\| < \|3+i\|$ Veamos primeros $\|3+i\| = 10$ y $(7+2i)(3-i) = 23 - i$ Como $23 = 10(2) + 3,\ -1 = 10(0) - 1$, luego tenemos $q = 2 + 0i,\ r_1 = 3 - i$

   Sea $r = 7 + 2i - 2(3 + i) = 1$, luego $\|1\| = 1 < 10 = \|3 + i\|$ y se cumple que $7 + 2i = (3 + i)2 + 1$

3. $3-5i = (3-2i)q+r$ con $\|r\| < \|3-2i\|$ Veamos primeros $\|3-2i\| = 13$ y $(3-5i)(3+2i) = 19 - 9i$ Como $19 = 13(1) + 6,\ -9 = 13(-1) + 4$, luego tenemos $q = 1 - i,\ r_1 = 6 + 4i$

   Sea $r = 3 - 5i - (1 - i)(3 - 2i) = 3 - 5i - (1 - 5i) = 2$, luego $\|2\| = 4 < 13 = \|3 - 2i\|$ y se cumple que $3 - 5i = (3 - 2i)(1 - i) + 4$.

5.8. Ejercicios Desarrollados

Ejemplo 115 *Determinar $z \in \mathbb{C}$ tal que:*

a) $|z| - z = 1 + i$ **Solución:** Sea $z = a + bi, \quad |z| = \sqrt{a^2 + b^2}$

$$\begin{aligned} 1 + i &= |z| - z \\ 1 + i &= \sqrt{a^2 + b^2} - a - bi, \end{aligned}$$

luego tenemos el sistema

$$\left.\begin{aligned} \sqrt{a^2 + b^2} - a &= 1 \\ -b &= 1 \end{aligned}\right|$$

Reemplazando obtenemos

$$\begin{aligned} \sqrt{a^2 + 1} &= 1 + a \quad /()^2 \\ a^2 + 1 &= 1 + 2a + a^2 \\ 0 &= 2a \\ 0 &= a \end{aligned}$$

Por lo tanto $z = 0 - i$ es la solución.

b) $|z| + z = 3 + 2i$.

Solución: Sea $z = a + bi, \quad |z| = \sqrt{a^2 + b^2}$

$$\begin{aligned} 3 + 2i &= |z| + z \\ 3 + 2i &= \sqrt{a^2 + b^2} + a + bi \end{aligned}$$

luego tenemos el sistema

$$\left.\begin{aligned} \sqrt{a^2 + b^2} + a &= 3 \\ b &= 2 \end{aligned}\right|$$

Reemplazando obtenemos

$$\begin{aligned} \sqrt{a^2 + 4} &= 3 - a \quad /()^2 \\ a^2 + 4 &= 9 - 6a + a^2 \\ -5 &= -6a \\ \frac{5}{6} &= a \end{aligned}$$

Note que, para elevar al cuadrado era necesario que $3 - a$ es no negativo, con el valor encontrado lo cumple. Por lo tanto $z = \frac{5}{6} + 2i$ es la solución.

c) $z^2 + |z|^2 = 0$

Solución: Sea $z = a + bi, \quad z^2 = a^2 + 2abi - b^2, \quad |z|^2 = a^2 + b^2$

$$\begin{aligned} z^2 + |z|^2 &= 0 \\ a^2 + 2abi - b^2 + a^2 + b^2 &= 0 \\ a^2 + 2abi &= 0 \end{aligned}$$

De lo cual obtenemos

$$\begin{array}{rcl} a^2 &=& 0 \\ 2ab &=& 0 \end{array}$$

Luego $a = 0$.

De este modo, el conjunto solución es $S = \{0 + bi \mid b \in \mathbb{R}\}$

d) $\left|\frac{z-4}{z-8}\right| = 1$

Solución: Sea $z = a + bi$

$$\begin{array}{rcl} \dfrac{|z-4|}{|z-8|} &=& 1 \\ |z-4| &=& |z-8| \\ |a+bi-4| &=& |a+bi-8| \\ |a-4+bi| &=& |a-8+bi| \\ \sqrt{(a-4)^2+b^2} &=& \sqrt{(a-8)^2+b^2} \quad /()^2 \\ a^2-8a+16+b^2 &=& a^2-16a+64+b^2 \\ 16a-8a &=& 64-16 \\ 8a &=& 48 \\ a &=& 6 \end{array}$$

Por lo tanto, el conjunto solución es $S = \{6 + bi; b \in \mathbb{R}\}$

Ejemplo 116 *Determinar el lugar geométrico en cada caso*

a) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z-4-i| = |z-5|\}$

Solución: Sea $z = a + bi$

$$\begin{array}{rcl} |a+bi-4-i| &=& |a+bi-5| \\ |a-4+(b-1)i| &=& |a-5+bi| \\ \sqrt{(a-4)^2+(b-1)^2} &=& \sqrt{(a-5)^2+b^2} \quad /()^2 \\ (a-4)^2+(b-1)^2 &=& (a-5)^2+b^2 \\ a^2-8a+16+b^2-2b+1 &=& a^2-10a+25+b^2 \\ 2a-2b &=& 8 \quad /\div 2 \\ a-b &=& 4 \end{array}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad a - b = 4\}$, representa una recta en $\mathbb{R}^2$.

b) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad \left|\frac{z+2}{z-2}\right| = 2\}$

Solución: Sea $z = a + bi$

$$\begin{array}{rcl} \dfrac{|z+2|}{|z-2|} &=& 2 \\ |z+2| &=& 2|z-2| \\ |a+bi+2| &=& 2|a+bi-2| \\ |a+2+bi| &=& 2|a-2+bi| \end{array}$$

$$\begin{aligned}
\sqrt{(a+2)^2+b^2} &= 2\sqrt{(a-2)^2+b^2} \quad /()^2 \\
a^2+4a+4+b^2 &= 4a^2-16a+16+4b^2 \\
0 &= 3a^2-20a+12+3b^2 \quad / \div 3 \\
0 &= a^2-\frac{20}{3}a+4+b^2 \\
0 &= \left(a-\frac{20}{6}\right)^2+b^2-\frac{400}{36}+4 \\
\frac{256}{36} &= \left(a-\frac{20}{6}\right)^2+b^2 \\
\left(\frac{16}{6}\right)^2 &= \left(a-\frac{20}{6}\right)^2+b^2
\end{aligned}$$

Por lo tanto $\mathcal{A}=\left\{a+bi\in\mathbb{C} \quad | \quad \left(a-\frac{10}{3}\right)^2+b^2=\left(\frac{8}{3}\right)^2\right\}$, representa una circunferencia en $\mathbb{R}^2$.

c) $\mathcal{A}=\{z\in\mathbb{C} \quad | \quad z-\overline{z}=i\}$

Solución: Sea $z=a+bi, \quad \overline{z}=a-bi$

$$\begin{aligned}
z-\overline{z} &= a+bi-a+bi \\
i &= 2bi \\
1 &= 2b \\
\frac{1}{2} &= b
\end{aligned}$$

Por lo tanto $\mathcal{A}=\{a+bi\in\mathbb{C} \quad | \quad b=\frac{1}{2}\}$, representa una recta en $\mathbb{R}^2$.

d) $\mathcal{A}=\{z\in\mathbb{C} \quad | \quad z+\overline{z}=|z|^2\}$

Solución: Sea $z=a+bi, \quad \overline{z}=a-bi, \quad |z|=\sqrt{a^2+b^2}$

$$\begin{aligned}
\overline{z}+z &= a-bi+a+bi \\
a^2+b^2 &= 2a \\
a^2-2a+1+b^2 &= 1 \\
(a-1)^2+b^2 &= 1
\end{aligned}$$

Por lo tanto $\mathcal{A}=\{a+bi\in\mathbb{C} \quad | \quad (a-1)^2+b^2=1\}$, representa una circunferencia en $\mathbb{R}^2$.

e) $\mathcal{A}=\{z\in\mathbb{C} \quad | \quad |(1+i)z-(1+3i)|\leq 1\}$

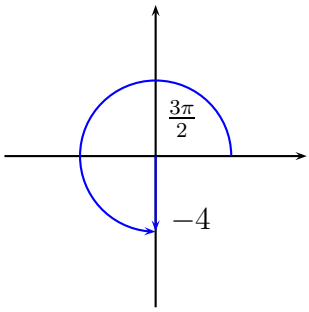
Solución: Sea $z = a + bi$

$$\begin{aligned}
|(1+i)z - (1+3i)| &\leq 1 \\
|(1+i)\cdot(a+bi) - (1+3i)| &\leq 1 \\
|a+bi+ai-b-1-3i)| &\leq 1 \\
|(a-b-1)+(a+b-3)i| &\leq 1 \\
\sqrt{(a-b-1)^2+(a+b-3)^2} &\leq 1 \quad /()^2 \\
(a-b-1)^2+(a+b-3)^2 &\leq 1 \quad /()^2 \\
a^2+b^2+1-2ab-2a+2b+b^2+a^2+9+2ab-6a-6b &\leq 1 \\
2a^2-8a+2b^2-4b &\leq -9 \quad /\div 2 \\
a^2-4a+b^2-2b &\leq -\frac{9}{2} \\
(a-2)^2-4+(b-1)^2-1 &\leq -\frac{9}{2} \\
(a-2)^2+(b-1)^2 &\leq \frac{1}{2}
\end{aligned}$$

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad (a-2)^2+(b-1)^2 \leq = \frac{1}{2}\}$, representa un disco de centro $(2,1)$ y radio $\frac{1}{\sqrt{2}}$ en $\mathbb{R}^2$.

Ejemplo 117 *Encontrar el Arg(z) en cada caso*

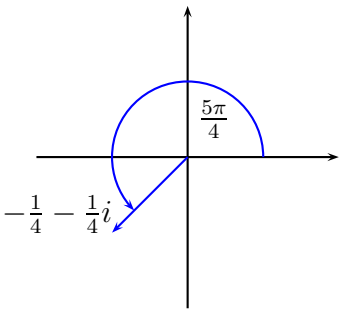
a) $z = -4i$



Por lo tanto $Arg(z) = \frac{3\pi}{2}$

b) $z = \frac{i}{-2-2i}$

$z = \frac{i}{-2-2i}\cdot\frac{-2+2i}{-2+2i} = \frac{-2-2i}{4+4} = -\frac{1}{4} - \frac{1i}{4}$



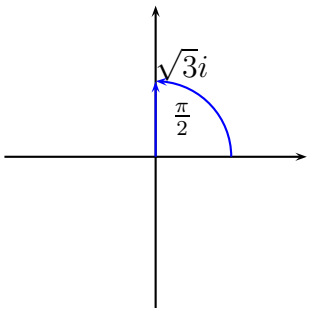
$$\text{tg}^{-1}\left(\frac{-\frac{1}{4}}{-\frac{1}{4}}\right) = \text{tg}^{-1}(1) = \frac{\pi}{4}$$

Pero el número complejo, esta en el tercer cuadrante luego

$$Arg(z) = \frac{5\pi}{4}$$

Ejemplo 118 *Escriba en forma polar en cada caso*

a) $z = \sqrt{3}i$

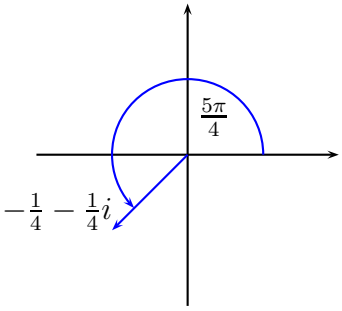


Por lo tanto $Arg(z) = \frac{\pi}{2}$, $|z| = \sqrt{3}$

$$z = \sqrt{3} \cdot cis\left(\frac{\pi}{2}\right)$$

b) $z = \frac{i}{-2-2i}$

$z = \frac{i}{-2-2i} \cdot \frac{-2+2i}{-2+2i} = \frac{-2-2i}{4+4} = -\frac{1}{4} - \frac{1}{4}i$



Veamos ahora su módulo

$|z| = \sqrt{\frac{1}{16} + \frac{1}{16}} = \sqrt{\frac{1}{8}} = \frac{1}{2\sqrt{2}}$

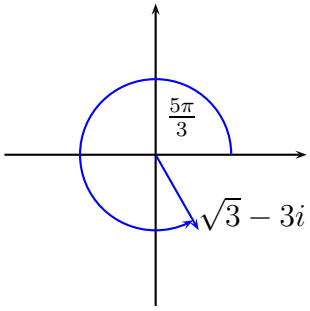
De lo cual obtenemos

$$z = \frac{1}{2\sqrt{2}} \cdot cis\left(\frac{5\pi}{4}\right)$$

Ejemplo 119 *Encuentre el valor de:*

a) $(\sqrt{3} - 3i)^6$

Solución: Sea $z = \sqrt{3} - 3i$, primero graficaremos para observar el cuadrante en que se encuentra



Además tenemos que

$$\text{tg}^{-1}\left(\frac{-3}{\sqrt{3}}\right) = -60$$

y el número complejo esta en el cuarto cuadrante, luego $Arg(z) = \frac{5\pi}{3}$. El módulo es $|z| = \sqrt{3+9} = \sqrt{12} = 2 \cdot \sqrt{3}$. Veamos ahora su potencia

$$\begin{aligned}(\sqrt{3} - 3i)^6 &= \left(2 \cdot \sqrt{3} \cdot cis\left(\frac{5\pi}{3}\right)\right)^6 = 2^6 \cdot 3^{\frac{6}{2}} \cdot cis\left(\frac{5 \cdot 6\pi}{3}\right) \\ &= 2^6 \cdot 3^3 \cdot cis(10\pi) = 2^6 \cdot 3^3 \cdot (\cos(0) + i\,\text{sen}(0)) = 2^6 \cdot 3^3.\end{aligned}$$

Por lo tanto $(\sqrt{3} - 3i)^6 = 1728$.

b) $(1+i)^{30}$

Solución: Sea $z = 1 + i$, note que esta en el primer cuadrante y que $\text{tg}^{-1}\left(\frac{1}{1}\right) = 45$, luego tenemos $Arg(z) = \frac{\pi}{4}$. además su módulo es $|1+i| = \sqrt{1^2 + 1^2} = \sqrt{2}$. Con lo cual obtenemos $1 + i = 2^{\frac{1}{2}} \cdot cis\left(\frac{\pi}{4}\right)$.

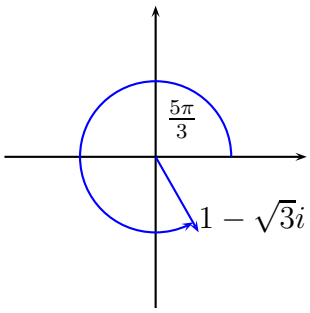
Reemplazando

$$\begin{aligned}(1+i)^{30} &= 2^{\frac{30}{2}} \cdot cis\left(\frac{30\pi}{4}\right) = 2^{15} \cdot cis\left(\frac{15\pi}{2}\right)\\ &= 2^{15} \cdot cis\left(\frac{3\pi}{2}\right) = 2^{15} \cdot \left(\cos\left(\frac{3\pi}{2}\right) + i\,\text{sen}\left(\frac{3\pi}{2}\right)\right)\end{aligned}$$

Por lo tanto obtenemos que $(1+i)^{30} = 2^{15} \cdot (0-i) = -2^{15}i$

c) $(1-\sqrt{3}i)^5$

Solución: Sea $z = 1-\sqrt{3}i$, $\text{tg}^{-1}\left(\frac{-\sqrt{3}}{1}\right) = -60$.



Por lo tanto $Arg(z) = \frac{5\pi}{3}$ y $|z| = \sqrt{1+3} = 2$.

Reemplazando

$$\begin{aligned}(1-\sqrt{3}i)^5 &= \left(2 \cdot cis\left(\frac{5\pi}{3}\right)\right)^5 = 2^5 \cdot cis\left(\frac{25\pi}{3}\right)\\ &= 2^5 \cdot \left(\cos\left(\frac{\pi}{3}\right) + i\,\text{sen}\left(\frac{\pi}{3}\right)\right)\\ z^5 &= 2^5 \cdot \left(\frac{1}{2} + \frac{\sqrt{3}i}{2}\right)\end{aligned}$$

Luego obtenemos $(1-\sqrt{3}i)^5 = 2^4 \cdot (1+\sqrt{3}i)$

Ejemplo 120 *Determinar todos los* $z \in \mathbb{C}$ *tal que:* $\left(\frac{1-z}{2z+i}\right)^4 = 1$

Solución:

$$\begin{aligned}\left(\frac{1-z}{2z+i}\right)^4 &= 1 = 1cis(0)\\ \frac{1-z}{2z+i} &= cis\left(\frac{2k\pi}{4}\right) \quad k = 0,1,2,3\end{aligned}$$

Luego despejando z tenemos

$$\begin{aligned}1-z &= cis\left(\frac{2k\pi}{4}\right)(2z+i)\\ (1+2cis\left(\frac{2k\pi}{4}\right))z &= 1-icis\left(\frac{2k\pi}{4}\right)\end{aligned}$$

Ahora veremos las cuatro posibilidades

- $k = 0, \quad cis(0) = 1.$

  Reemplazamos obtenemos $3z = 1-i$, luego $z = \frac{1}{3} - \frac{1}{3}i$.

- $k = 1, \quad cis(\frac{\pi}{2}) = i$

  Reemplazamos obtenemos $(1+2i)z = 2$, luego

$$z = 2 \cdot (1+2i)^{-1} = \frac{2}{5} - \frac{4}{5}i$$

- $k = 2, \quad cis(\pi) = -1$

  Reemplazamos obtenemos $-z = 1+i$, luego $z = -1-i$.

- $k = 3, \quad cis(\frac{3\pi}{2}) = -i$

  Reemplazamos obtenemos $(1-2i)z = 0$, luego $z = 0$

Por lo tanto $z \in \left\{\frac{1}{3} - \frac{1}{3}i, \quad \frac{2}{5} - \frac{4}{5}i, \quad -1-i, \quad 0+0i\right\}$

Ejemplo 121 *Resuelva en los siguientes casos*

a) $z^2 = 2i$

Solución: Como $2i = 2cis(\frac{\pi}{2})$

$$z_k \quad = \quad \sqrt{2} \cdot cis\left(\frac{\frac{\pi}{2} + 2k\pi}{2}\right); \quad k = 0, 1$$

Si $k = 0, \quad z_0 = \sqrt{2} \cdot cis\left(\frac{\pi}{4}\right) = \sqrt{2} \cdot \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) = 1+i$

Si $k = 1, \quad z_1 = \sqrt{2} \cdot cis\left(\frac{5\pi}{4}\right) = \sqrt{2} \cdot \left(-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i\right) = -1-i.$

Por lo tato el conjunto solución es

$$S = \{1+i, \ -1-i\}$$

b) $z^6 = 8$

Solución: Se tiene $8 = 8cis(0)$

$$z_k \quad = \quad \sqrt[6]{8} \cdot cis\left(\frac{2k\pi}{6}\right); \quad k = 0, 1, 2, 3, 4, 5$$

Si $k = 0, \quad z_0 = \sqrt[6]{8} \cdot cis(0) = \sqrt[6]{8} \cdot 1 = \sqrt[6]{8}$

Si $k = 1, \quad z_1 = \sqrt[6]{8} \cdot cis\left(\frac{\pi}{3}\right) = \sqrt[6]{8} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$

Si $k = 2, \quad z_2 \sqrt[6]{8} \cdot cis\left(\frac{2\pi}{3}\right) = \sqrt[6]{8} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$

Si $k = 3, \quad z_3 = \sqrt[6]{8} \cdot cis(\pi) = \sqrt[6]{8} \cdot -1 = -\sqrt[6]{8}$

Si $k = 4, \quad z_4 = \sqrt[6]{8} \cdot cis\left(\frac{4\pi}{3}\right) = \sqrt[6]{8} \cdot \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$

Si $k=5, \quad z_5=\sqrt[6]{8}\cdot cis\left(\frac{5\pi}{3}\right)=\sqrt[6]{8}\cdot\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)$.

Por lo tato el conjunto solución es

$$S=\left\{\pm\sqrt[6]{8},\ \pm\sqrt[6]{8}\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right),\ \pm\sqrt[6]{8}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\right\}$$

c) $z^3=-1+i$

Solución: Como $-1+i=\sqrt{2}cis(\frac{3\pi}{4}$

$$z_k \ = \ \sqrt[6]{2}\cdot cis\left(\frac{\frac{3\pi}{4}+2k\pi}{3}\right); \quad k=0,1,2$$

Si $k=0 \quad z_0=\sqrt[6]{2}\cdot cis\left(\frac{\pi}{4}\right)=\sqrt[6]{2}\cdot\left(\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right)$

Si $k=1 \quad z_1=\sqrt[6]{2}\cdot cis\left(\frac{11\pi}{12}\right)$

Si $k=2 \quad z_2=\sqrt[6]{2}\cdot cis\left(\frac{19\pi}{12}\right)$

Por lo tato el conjunto solución es

$$S=\left\{\sqrt[6]{2}\left(\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right),\ \sqrt[6]{2}cis\left(\frac{11\pi}{12}\right),\ \sqrt[6]{2}cis\left(\frac{19\pi}{12}\right)\right\}$$

Ejemplo 122 *¿El número 47 es primo en $\mathbb{Z}[i]$? Justifique*

Solución: Sean $z_1=a+bi, \quad w=c+di$, no unidades, tales que

$$\begin{aligned} z\cdot w &= 47 \quad /\|\ \| \\ \|z\|\cdot\|w\| &= \|47\| \\ \|z\|\cdot\|w\| &= 47^2 \end{aligned}$$

Considerando que son positivo y 47 es primo en $\mathbb{Z}$ tenemos

$$\|z\|=47 \quad \wedge \quad \|w\|=47$$

Supongamos

$$\begin{aligned} \|z\| &= 47 \\ a^2+b^2 &= 47 \\ a^2+b^2 &\equiv 0(\texttt{mod}\ 47) \\ a_1^2 &\equiv -b_1^2(\texttt{mod}\ 47) \quad / \cdot b_1^{-2}, b_1\neq 0 \\ a_1^2\cdot b_1^{-2} &\equiv -1(\texttt{mod}\ 47) \\ (a_1\cdot b_1^{-1})^2 &\equiv -1(\texttt{mod}\ 47) \end{aligned}$$

Luego -1 es un cuadrado módulo 47. Por otro lado, determine si es un cuadrado con el símbolo de Legendre

$$\left(\frac{-1}{47}\right) = (-1)^{\frac{47-1}{2}} = -1$$

Lo que es una contradicción.

Por lo tanto 47 es primo en $\mathbb{Z}[i]$

Ejemplo 123 *Determine si* $7+4i$ *es primo en* $\mathbb{Z}[i]$

Solución: Sean $z_1 = a+bi,\ w = c+di$ no unidades, tales que

$$\begin{aligned} z \cdot w &= 7+4i \quad /\| \ \| \\ \|z\| \cdot \|w\| &= \|7+4i\| \\ \|z\| \cdot \|w\| &= 65 = 13 \cdot 5 \end{aligned}$$

Salvo orden obtenemos

$$\begin{aligned} \|z\| = 5 \ &\wedge \ \|w\| = 13 \\ a^2+b^2 = 5 \ &\wedge \ c^2+d^2 = 13 \end{aligned}$$

Una solución es

$$7+4i = (1+2i)\cdot(3-2i)$$

Por lo tanto $7+4i$ no es primo en $\mathbb{Z}[i]$.

Capítulo 6

Anillo de Polinomios.

Una forma de definir los polinomios en forma intuitiva es la siguiente:

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo, entonces un polinomio con coeficiente en $\mathbb{K}$ es de la siguiente forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$$

donde $n \in \mathbb{N}$, $a_n, a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ son los coeficientes del polinomio, elementos de $\mathbb{K}$

Se dice que el grado de $p(x)$ es n si y sólo si $a_n \neq 0$, y se denota por $\text{gr}(p(x)) = n$

Se denota el conjunto de los polinomios con coeficiente en $\mathbb{K}$ del siguiente modo

$$\mathbb{K}[x] := \{p(x) \mid a_i \in \mathbb{K} \text{ y } n \in \mathbb{N}\}$$

Sean $p(x), q(x) \in \mathbb{K}[x]$, se dice que los polinomios son iguales o $p(x) = q(x)$ si y sólo si son iguales coeficiente a coeficiente.

Definición 56 *Sea $F(\mathbb{N}, \mathbb{K})$ el conjunto de la funciones de $\mathbb{N}$ en $\mathbb{K}$, entonces el conjunto de los polinomios con coeficiente en $\mathbb{K}$ en la variable x es*

$$\mathbb{K}[x] := \{\ p \in F(\mathbb{N}, \mathbb{K}) \mid p^{-1}(\mathbb{K}^*) \quad \textit{es finito}\ \}$$

Además si $p \in \mathbb{K}[x]$ no nulo, entonces se define el grado

$$\text{gr}(p) = \text{máx}(p^{-1}(\mathbb{K}^*)).$$

Notación: Sea $p \in \mathbb{K}[x]$, y $\text{gr}(p) = n$ entonces

$$p(x) = p_0 + p_1 x^1 + \cdots + p_{n-1}x^{n-1} + p_n x^n = \sum_{i=0}^{n} p_i x^i$$

La igual de polinomio corresponde a una igual de funciones

6.1. Estructura Anillo.

Adición: Sean $p(x), q(x) \in \mathbb{K}[x]$, entonces la suma es la suma funcional, es decir,

$$\begin{array}{rccc} p+q & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & p_i + q_i \end{array}$$

luego se tiene para que el valor $p_i + q_i$ es distinta de cero, al menos un de ello debe ser distinto de cero. Por lo tanto

$$\mathrm{gr}(p+q) \leq \mathrm{máx}\{\mathrm{gr}(p), \mathrm{gr}(q)\}$$

Con la notación intuitiva, tenemos que esta definición se transforma del siguientes modo: Sean $p(x) = a_n x^n + \cdots + a_0$ y $q(x) = b_m x^m + \cdots + b_0$ para ello consideraremos 3 casos

(i) Si $\mathrm{gr}(p(x)) > \mathrm{gr}(q(x))$ entonces $n > m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_m x^m + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= a_n x^n + \cdots + (a_m + b_m) x^m + (a_0 + b_0). \end{aligned}$$

(ii) Si $\mathrm{gr}(p(x)) = \mathrm{gr}(q(x))$ entonces $n = m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) \\ &= (a_n + b_n) x^n + \cdots + (a_0 + b_0). \end{aligned}$$

(iii) Si $\mathrm{gr}(p(x)) < (q(x))$ entonces $n < m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_n x^n + \cdots + b_0) \\ &= b_m x^m + \cdots + (a_n + b_n) x^n + (a_0 + b_0). \end{aligned}$$

6.1.1. Suma en $\mathbb{K}[x]$

Propiedad 163 *Sea $\mathbb{K}[x]$ el anillo de polinomios se cumple*

$$(\mathbb{K}[x], +) \quad \textit{forman un grupo abeliano.}$$

Demostración: Sean $p(x), q(x), r(x) \in \mathbb{K}[x]$,
Asociativa:

$$p(x) + [q(x) + r(x)] = [p(x) + q(x)] + r(x)$$

Luego

$$\begin{aligned} (p + (q + r))_i &= p_i + (q + r)_i \\ &= p_i + (q_i + r_i) \\ &= (p_i + q_i) + r_i \\ &= (p + q)_i + r_i \\ &= ((p + q) + r)_i \end{aligned}$$

Neutro Aditivo: existe $0(x) \in \mathbb{K}[x]$ función nula

$$p(x) + 0(x) = p(x)$$

Para ello

$$\begin{aligned}(p+0)_i &= p_i + 0_i \\ &= p_i + 0 \\ &= p_i\end{aligned}$$

Observación: Notemos que $0(x) = 0x^m + \cdots + 0 = 0x^n + \cdots + 0$.
Inverso Aditivo: Sea $p(x) \in \mathbb{K}[x]$, existe

$$\begin{array}{rccc} -p & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & -p_i \end{array}$$

tal que

$$p(x) + (-p(x)) = 0(x)$$

Para ello

$$\begin{aligned}(p+(-p))_i &= p_i + (-p_i) \\ &= 0 \\ &= 0_i\end{aligned}$$

Observación: Notemos que $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{K}[x]$, entonces $-p(x) = -a_n x^n - a_{n-1}x^{n-1} \cdots - a_0$.
Conmutatividad: Debemos probar

$$p(x) + q(x) = q(x) + p(x)$$

Para ello

$$\begin{aligned}(p+q)_i &= p_i + q_i \\ &= q_i + p_i \\ &= (q+p)_i\end{aligned}$$

6.1.2. Multiplicación en $\mathbb{K}[x]$

Multiplicación: Consideremos $p(x), q(x) \in \mathbb{K}[x]$, entonces la multiplicación es dada por

$$\begin{array}{rccc} p \cdot q & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & \sum_{k=0}^{i} p_{k-i} q_k \end{array}$$

note que el valor $\sum_{k=0}^{i} p_{k-i} q_k$ es cero, si el $i > n + m$ y $\sum_{k=0}^{n+m} p_{k-i} q_k = p_n q_m$, cuando $n = \text{gr(p(x))}$ y $m = \text{gr(q(x))}$. Por lo tanto

$$\text{gr}(p \cdot q) \leq \text{gr}(p) + \text{gr}(q)$$

Con la notación intuitiva, tenemos que esta definición se transforma del siguientes modo: Sean

$$p(x) = a_n x^n + \cdots + a_0 \quad \text{y} \quad q(x) = b_m x^m + \cdots + b_0$$

tenemos

$$\begin{aligned} p(x) \cdot q(x) &= (a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0) \\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_o + a_0 b_1) x + a_0 b_0. \end{aligned}$$

Propiedad 164 $(\mathbb{K}[x], +, \cdot)$ *es un anillo conmutativo.*

Demostración: Sean $p(x), q(x), r(x) \in \mathbb{K}[x]$,
Asociativa:

$$p(x) \cdot [q(x) \cdot r(x)] = [p(x) \cdot q(x)] \cdot r(x)$$

Neutro:

$$p(x) \cdot 1 = p(x)$$

Conmutatividad:

$$p(x) \cdot q(x) = q(x) \cdot p(x)$$

Distributividad:

$$p(x) \cdot [q(x) + r(x)] = [p(x) \cdot q(x)] + [p(x) \cdot r(x)]$$

Definición 57 *Sean $p(x), q(x) \in \mathbb{K}[x]$, se dice que $p(x)$ divide a $q(x)$ si y sólo si existe $r(x) \in \mathbb{K}[x]$ tal que*

$$q(x) = p(x) \cdot r(x).$$

La notación es similar:

$$p(x) \text{ divide a } q(x), \text{ lo denotamos por } p(x) | q(x).$$

Definición 58 *Las unidades de $\mathbb{K}[x]$, corresponde a lo elementos que tiene inverso multiplicativos, es decir,*

$$p(x) \in \mathcal{U}(\mathbb{K}[x]) \quad \Leftrightarrow \quad (\exists\ q(x) \in \mathbb{K}[x])(\ p(x)q(x) = 1\ )$$

Propiedad 165 *Sea $\mathbb{K}$ un cuerpo entonces*

$$\mathcal{U}(\mathbb{K}[x]) = \mathbb{K}^*.$$

6.2. Algoritmo de la División en $\mathbb{K}[x]$.

Sean $\mathbb{K}$ un cuerpo y $p(x), q(x) \in \mathbb{K}[x]$ tal que $q(x)$ no nulo, entonces existe $r(x), s(x) \in \mathbb{K}[x]$ tal que

$$p(x) = q(x) \cdot s(x) + r(x) \qquad \text{gr}(r(x)) < \text{gr}(q(x)) \text{ o } r(x) = 0.$$

Demostración: Tomemos el conjunto de los polinomios de la siguiente forma

$$\mathcal{H} := \{p(x) - q(x) \cdot a(x) \mid a(x) \in \mathbb{K}[x]\}$$

Si consideramos $r(x)$ como el polinomio de menor grado o $r(x) = 0$, que pertenece a $\mathcal{H}$ tenemos

$$\begin{aligned} r(x) &= p(x) - q(x) \cdot s(x) \\ p(x) &= q(x) \cdot s(x) + r(x) \end{aligned}$$

Supongamos que $r(x) \neq 0$ y $\text{gr}(r(x)) \geq \text{gr}(q(x))$, con

$$r(x) = a_n x^n + \cdots + a_0, \quad q(x) = b_m x^m + \cdots + b_0$$

luego

$$r_1(x) = r(x) - \frac{a_n}{b_m} x^{n-m} q(x) \in \mathbb{K}[x]$$

Tiene grado menor y pertenece a $\mathcal{H}$. □

Notación: En el algoritmo de la división el polinomio $s(x)$ se llama cuociente y $r(x)$ el resto.

6.3. División Sintética.

Ejemplo 124 *Determinar el resto y el cuociente al dividir* $p(x) = x^4 + 6x^3 + 7x^2 - 6x - 8 \in \mathbb{R}[x]$ *por* $x + 1$

$$\begin{array}{rrrrrl} x^4 & +6x^3 & +7x^2 & -6x & -8 & : x+1 \quad = x^3 + 5x^2 + 2x - 8 \\ \cline{1-1} -x^4 & -x^3 & & & & \\ \cline{2-5} & 5x^3 & +7x^2 & -6x & -8 & \\ & -5x^3 & -5x^2 & & & \\ \cline{3-5} & & 2x^2 & -6x & -8 & \\ & & -2x^2 & -2x & & \\ \cline{4-5} & & & -8x & -8 & \\ & & & 8x & +8 & \\ \cline{5-5} & & & & 0 & \end{array}$$

Luego tenemos

$$x^4 + 6x^3 + 7x^2 - 6x - 8 = (x+1)(x^3 + 5x^2 + 2x - 8) + (0)$$

El proceso anterior, lo podemos resumir de la siguiente manera

-1	1	6	7	-6	-8
		-1	-5	-2	8
	1	5	2	-8	0

El proceso de la división sintética es un regla, que permite resumir la división de polinomios para un caso particular.

Para ello supongamos que deseamos dividir $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ deseamos dividir por $x - \alpha$.

Lo cual lo denotamos por:

α	a_n	a_{n-1}		a_1	a_0
		αb_{n-1}		αb_1	αb_0
	a_n	$a_{n-1} + \alpha a_n$		$a_1 + \alpha b_1$	$a_0 + \alpha b_0$
	b_{n-1}	b_{n-2}	$\cdots$	b_0	c_0

y obtenemos el siguiente resultado

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha)(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) + c_0.$$

6.4. Máximo Común Divisor

Definición 59 *Sean $a(x), b(x) \in \mathbb{K}[x]$. Se dice que $d(x) = MCD(a(x), b(x)) \in \mathbb{K}[x]$ si y sólo si*

1. *$d(x)|a(x) \ \wedge \ d(x)|b(x)$*
2. *Si $h(x)|a(x) \ \wedge \ h(x)|b(x)$ entonces $h(x)|d(x)$*

Observación: si $d(x)$ es un máximo común divisor de $a(x), b(x)$ y $\alpha \in \mathbb{K}^*$ entonces $\alpha d(x)$ también es máximo común divisor de $a(x), b(x)$

Teorema 166 *Sean $a(x), b(x) \in \mathbb{K}[x]$. Si $d(x) = MCD(a(x), b(x)) \in \mathbb{K}[x]$ entonces existe $p(x), q(x) \in \mathbb{K}[x]$ tal que*

$$d(x) = a(x)p(x) + b(x)q(x)$$

Demostración: Sea $\mathcal{A} = \{a(x)p(x) + b(x)q(x) \mid p(x), q(x) \in \mathbb{K}[x]\}$.

Primero notemos que si $r(x), s(x) \in \mathcal{A}, c(x) \in \mathbb{K}[x]$, entonces $r(x) + c(x)s(x) \in \mathcal{A}$, para ello sea

$$r(x) = a(x)p_1(x) + b(x)q_1(x), \quad s(x) = a(x)p_2(x) + b(x)q_2(x)$$

luego tenemos

$$\begin{aligned} r(x) + c(x)s(x) &= a(x)p_1(x) + b(x)q_2(x)(+c(x)(a(x)p_2(x) + b(x)q_2(x)) \\ &= a(x)(p_1(x) + c(x)p_2(x)) + b(x)(q_1(x) + c(x)q_2(x)) \end{aligned}$$

Sea $d(x)$ el polinomio no nulo de grado menor en $\mathcal{A}$, demostraremos que todo polinomio en $\mathcal{A}$ es un múltiplo de $d(x)$.

Sea $h(x) \in \mathcal{A}$, luego aplicando el algoritmo de la división obtenemos

$$h(x) = d(x)s(x) + r(x) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(d(x)) \text{ o } r(x) = 0.$$

Luego tenemos que $r(x) = h(x) - d(x)s(x) \in \mathcal{A}$, por lo tanto $r(x) = 0$, es decir,

$$h(x) = d(x)s(x).$$

Notemos que $a(x), b(x) \in \mathcal{A}$, luego $d(x)|a(x)$ y $d(x)|b(x)$.
Ahora supongamos que $h(x)|a(x)$ y $h(x)|b(x)$, como $d(x) \in \mathcal{A}$, luego tenemos

$$\begin{aligned} d(x) &= a(x)p(x) + b(x)q(x) \\ d(x) &= h(x)s_1(x)p(x) + h(x)s_2(x)q(x) \\ d(x) &= h(x)(s_1(x)p(x) + s_2(x)q(x)) \end{aligned}$$

de lo cual tenemos $h(x)|d(x)$. □

6.5. Raíces de un Polinomio.

En esta sección se relaciona las raíces de un polinomio con una factorización, pero antes veremos la diferencia entre polinomio y función polinomial Sea $p(x) \in \mathbb{K}[x]$, luego

$$\begin{array}{rccc} p & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & p_i \end{array}$$

y la función polinomial

$$\begin{array}{rccc} : & \mathbb{K} & \to & \mathbb{K} \\ & \alpha & \rightsquigarrow & p_0 + \sum_{k=1}^{\mathrm{gr(p)}} p_i \cdot \alpha^i \end{array}$$

Definición 60 *Sea $p(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$.*
Se dice que α una raíz o un cero de $p(x)$ si y sólo si $p(\alpha) = 0$

Teorema 167 (del factor) *Sean $p(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$ con $\mathrm{gr}(p(x)) \geq 1$ tenemos*

$$\alpha \text{ es raíz de } p(x) \text{ si y sólo si } (x - \alpha)|p(x).$$

Demostración: En primer lugar suponemos que α una raíz de $p(x)$
Aplicando el algoritmo de la división a $p(x)$ con $(x - \alpha)$ tenemos

$$p(x) = (x - \alpha) \cdot s(x) + r(x) \tag{6.1}$$

donde $r(x)$ es una constante.
Si evaluamos la función polinomial en α obtenemos

$$\begin{aligned} p(\alpha) &= (\alpha - \alpha) \cdot s(\alpha) + r(\alpha) \\ 0 &= r(\alpha) \end{aligned}$$

Luego $r(x) = 0$, reemplazando en 6.1 tenemos

$$p(x) = (x - \alpha) \cdot s(x)$$

Por lo tanto $(x - \alpha)|p(x)$.

En el otro sentido, si $(x - \alpha)|p(x)$ entonces

$$p(x) = (x - \alpha) \cdot q(x)$$

Evaluando en α obtenemos

$$\begin{aligned} p(\alpha) &= (\alpha - \alpha) \cdot q(\alpha) \\ &= 0. \end{aligned}$$

Por lo tanto α es raíz de $p(x)$. □

Notación: Sea $p(x) \in \mathbb{K}[x]$, si consideramos $p(x) = 0$, la llamaremos ecuación polinomial. Y las solución entregan las raíces de $p(x)$.

Teorema 168 *Sea $p(x) \in \mathbb{K}[x]$, $\text{gr}(p(x)) \geq 1$ entonces existe un cuerpo $\overline{\mathbb{K}}$ tal que $p(x)$ tiene todas las raíces en $\mathbb{K}$.*

Teorema 169 *Sea $p(x) \in \mathbb{K}[x]$, si $\text{gr}(p(x)) = n \geq 1$ entonces $p(x)$ tiene exactamente n raíces en $\overline{\mathbb{K}}$.*

Demostración: Sea $\alpha_1 \in \mathbb{K}$ una raíz del polinomio $p(x)$ entonces $(x - \alpha_1)$ divide a $p(x)$ y por algoritmo de la división

$$p(x) = (x - \alpha_1) \cdot r(x) \quad \text{y} \quad \text{gr}(r(x)) = n - 1$$

Ahora consideremos $\alpha_2 \in \mathbb{K}$ otra raíz pero del polinomio $r(x)$ entonces $(x - \alpha_2)$ divide a $r(x)$ y además

$$r(x) = (x - \alpha_1) \cdot s(x) \quad \text{y} \quad \text{gr}(s(x)) = n - 2$$

reemplazando obtenemos

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot s(x)$$

Si repetimos el proceso sucesivamente y suponiendo que todas las raíces están en $\mathbb{K}$ tenemos

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n)$$

donde α_i es una raíz de $p(x)$. Sea β una raíz entonces

$$0 = p(\beta) = (\beta - \alpha_1) \cdot (\beta - \alpha_2) \cdots (\beta - \alpha_n)$$

Como $\mathbb{K}$ es cuerpo, luego $\beta - \alpha_i = 0$ entonces $\beta = \alpha_i$. □

Observación: Si el polinomio $p(x)$ no tiene todas sus raíces en $\mathbb{K}[x]$ entonces

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_i) \cdot q(x) \quad \text{y} \quad \text{gr}(q(x)) = n - i$$

Teorema 170 *Sea $p(x) \in \mathbb{K}[x]$, si $\text{gr}(p(x)) \leq 4$ entonces existe una formular para determinar todas las raíces de $p(x)$.*

Teorema 171 *Sea $p(x) \in \mathbb{C}[x]$ tal que $\text{gr}(p(x)) = n > 1$ entonces $p(x)$ tiene todas sus n raíces en $\mathbb{C}$.*

Teorema 172 *Sea $p(x) \in \mathbb{Z}[x]$ donde $\text{gr}(p(x)) = n$ y*

$$p(x) = a_n x^n + \cdots + a_0$$

Si $\frac{a}{b} \in \mathbb{Q}$ es raíz de $p(x)$, con a, b primos relativos entonces $a|a_0$ y $b|a_n$.

Demostración: Si $\frac{a}{b}$ es una raíz de $p(x)$ entonces $p\left(\frac{a}{b}\right) = 0$. Como

$$p(x) = a_n x^n + \cdots + a_0$$

luego

$$\begin{aligned}
p\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + \cdots + a_0 &= 0 \\
a_n \frac{a^n}{b^n} + \cdots + a_0 &= 0 \quad / \cdot b^n \\
a_n \frac{a^n}{b^n} \cdot b^n + \cdots + a_0 \cdot b^n &= 0 \\
a_n a^n + \cdots + a_0 b^n &= 0 \\
a_n a^n + \cdots + a_1 a b^{n-1} &= -a_0 b^n \\
a(a_n a^{n-1} + \cdots + a_1 b^{n-1}) &= -a_0 b^n
\end{aligned}$$

Ya que $(a_n a^{n-1} + \cdots + a_1 b^{n-1}) \in \mathbb{Z}$ entonces

$$a| - a_0 b^n$$

como $(a, b^n) = 1$ por ser primos relativos entonces $a|a_0$ Tomando

$$\begin{aligned}
a(a_n a^{n-1} + \cdots + a_1 b^{n-1}) &= -a_0 b^n \\
a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n &= 0 \\
a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n &= -a_n a^n \\
b(a_{n-1} a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) &= -a_n a^n
\end{aligned}$$

Como $(a_{n-1} a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) \in \mathbb{Z}$ entonces

$$b| - a_n a^n$$

pero $(b, a^n) = 1$ por ser primos relativos entonces $b|a_n$. □

Teorema 173 *Sea $p(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ tal que α es una raíz de $p(x)$ entonces $\overline{\alpha}$ es raíz de $p(x)$.*

Demostración: Dado un $p(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ una raíz de $p(x)$, entonces $p(\alpha) = 0$

Sea $p(x) = a_n x^n + \cdots + a_0$ y calculamos $p(\alpha)$ tenemos

$$p(\alpha) \quad = \quad a_n(\alpha)^n + \cdots + a_0 = 0$$

Si aplicamos la función conjugado tenemos

$$\begin{aligned}
\overline{a_n(\alpha)^n + \cdots + a_0} &= \overline{0} \\
\overline{a_n(\alpha)^n + \cdots + a_0} &= 0 \\
\overline{a_n(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
\overline{a_n}\overline{(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
\overline{a_n}\overline{(\alpha)}^n + \cdots + \overline{a_0} &= 0
\end{aligned}$$

ya que $a_i \in \mathbb{R}$ con $i = 0, \cdots, n$ tenemos $\overline{a_i} = a_i$ entonces

$$\begin{aligned}
\overline{a_n}\overline{(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
a_n\overline{(\alpha)}^n + \cdots + a_0 &= 0
\end{aligned}$$

Por lo tanto $p(\overline{\alpha}) = 0$ entonces $\overline{\alpha}$ es raíz de $p(x)$.

Teorema 174 *Sea $p(x) \in \mathbb{R}[x]$ y si $\mathrm{gr}(p(x))$ es un número impar entonces $p(x)$ tiene una raíz real.*

Demostración: Como $\mathbb{R}[x] \subset \mathbb{C}[x]$ tenemos que si $p(x) \in \mathbb{R}[x]$ entonces $p(x) \in \mathbb{C}[x]$.

Luego por la teorema tenemos que $p(x)$ se descompone completamente, es decir, tiene todas sus raíces en $\mathbb{C}$, ya que $\mathrm{gr}(p(x))$ es un número impar, $p(x)$ tiene un número impar de raíces.

Por teorema tenemos que si α_i con $i = 1, \cdots, n$ es una raíz de $p(x)$ entonces $\overline{\alpha_i}$ también es raíz de $p(x)$. Entonces existe $\alpha_j \in \mathbb{C}$ raíz de $p(x)$ tal que

$$\overline{\alpha_j} = \alpha_j$$

Por lo tanto $\alpha_j \in \mathbb{R}$.

Teorema 175 *Sean $p(x) \in \mathbb{R}[x]$ donde $\mathrm{gr}(p(x)) \geq 1$ y $a, b \in \mathbb{R}$ tales que*

$$a < b \quad \wedge \quad p(a) \cdot p(b) < 0$$

entonces $p(x)$ tiene una raíz real en el intervalo $]a, b[$.

6.6. Polinomios Reducibles e Irreducibles.

Sea $p(x) \in \mathbb{K}[x]$ con $\mathrm{gr}(p(x)) \geq 1$ diremos que $p(x)$ es un `polinomio reducible` en $\mathbb{K}[x]$ si existen $q(x), r(x) \in \mathbb{K}[x]$ tales que

$$p(x) = q(x) \cdot r(x) \quad \text{con} \quad \mathrm{gr}(q(x)) \geq 1 \quad \text{y} \quad \mathrm{gr}(r(x)) \geq 1$$

se dice que $p(x)$ es `irreducible` si y sólo si $p(x)$ no es reducible $\mathrm{gr}(p(x)) \geq 1$

Teorema 176 *Sea $p(x) \in \mathbb{R}[x]$ y si $\text{gr}(p(x)) \geq 3$ entonces $p(x)$ es reducible.*

Demostración: Si $p(x)$ tiene una raíz real, entonces es reducible.

Si $p(x)$ no tiene raíces reales, luego son compleja y se encuentra también el conjugado

$$p(x) = (x-\alpha_1)(x-\overline{\alpha_1})(x-\alpha_2)(x-\overline{\alpha_2})\cdots(x-\alpha_r)(x-\overline{\alpha_r})$$

Luego multiplicando obtenemos

$$p(x) = (x^2-(\alpha_1+\overline{\alpha_1})x+\alpha_1)\overline{\alpha_1})(x^2-(\alpha_2+\overline{\alpha_2})x+\alpha_2)\overline{\alpha_2})\cdots(x^2-(\alpha_r+\overline{\alpha_r})x+\alpha_r)\overline{\alpha_r})$$

Factorización en $\mathbb{R}$. □

Propiedad 177 *Sea $p(x) \in \mathbb{R}[x]$ tenemos que $p(x)$ es irreducible si y sólo si*

1. $\text{gr}(p(x)) = 1$
2. $p(x) = ax^2+bx+c$ *tal que*
$$\Delta = b^2-4ac < 0$$

Propiedad 178 *Sea $p(x) \in \mathbb{C}[x]$ tenemos que $p(x)$ es irreducible si y sólo si* $\text{gr}(p(x)) = 1$

Teorema 179 *Sea $p(x) \in \mathbb{K}[x]$ y si $\text{gr}(p(x)) \geq 1$ entonces $p(x)$ es producto de polinomios irreducibles.*

Demostración: sea $p(x) \in \mathbb{K}[x]$, si $p(x)$ es irreducible, listo

Si $p(x)$ es reducible entonces existen $a(x), b(x) \in \mathbb{K}[x]$, tal que

$$p(x) = a(x)b(x) \qquad \text{con } \text{gr}(a(x)) < \text{gr}(p(x)) \wedge \text{gr}(b(x)) < \text{gr}(p(x))$$

si $a(x), b(x) \in \mathbb{K}[x]$, son irreducible listo, en caso contrario se sigue las descomposición □

6.7. Congruencia de Polinomio

Sean $a(x), b(x), p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$ entonces se define la relación de congruencia módulo $p(x)$

$$a(x) \equiv b(x)(\texttt{mod } p(x)) \;\Leftrightarrow\; p(x)|(a(x)-b(x))$$

Ejemplo 125 *Sea $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in \mathbb{K}[x]$ entonces*

1. $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \equiv a_0(\texttt{mod } x\ )$
2. $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \equiv a_1x+a_0(\texttt{mod } x^2\ )$

Teorema 180 *Sea $p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$ entonces la relación de congruencia módulo $p(x)$ en $\mathbb{K}[x]$ es una relación de equivalencia*

Demostración: Similar a la efectuada en $\mathbb{Z}$

6.7.1. Sistema de Representante

Sean $a(x), p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$,
Sea $\overline{a(x)}$ la clase de que contiene a $a(x)$,

$$\overline{a(x)} = \{b(x) \in \mathbb{K}[x] \mid a(x) \equiv b(x)(\mathtt{mod}\ p(x))\},$$

aplicando el algoritmo de la división, tenemos

$$a(x) = p(x)q(x) + r(x) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0.$$

luego tenemos

$$a(x) \equiv r(x)(\mathtt{mod}\ p(x)) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0.$$

es decir, $\overline{a(x)} = \overline{r(x)}$.
Notación: El conjunto de las clase de equivalencia módulo $p(x)$ se denota por

$$\mathbb{K}[x]/\!<p(x)>\, = \{\overline{r(x)} \mid r(x) \in \mathbb{K}[x], \text{ tal que } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0\}.$$

6.7.2. Suma y Producto

Sean $\overline{a(x)}, \overline{b(x)} \in \mathbb{K}[x]/\!<p(x)>$.

Suma

$$\overline{a(x)} + \overline{b(x)} = \overline{a(x) + b(x)}$$

Producto

$$\overline{a(x)} \cdot \overline{b(x)} = \overline{a(x) \cdot b(x)}$$

Teorema 181 *$(\mathbb{K}[x]/\!<p(x)>, +, \cdot)$ es un anillo conmutativo*

Demostración: La demostración, es similar a la efectuada en $\mathbb{Z}_n$, y los elementos notables están dado por:
El neutro aditivo es $\overline{0(x)}$, el inverso aditivo de $\overline{p(x)}$ es $\overline{-p(x)}$, el inverso multiplicativo es $\overline{1}$ y denotamos por $\mathcal{U}(\mathbb{K}[x]/\!<p(x)>)$ el conjunto de los elementos invertible por

Teorema 182 *Sea $r(x) \in \mathbb{K}[x]$ tal que es primo relativo con $p(x)$ entonces $\overline{r(x)}$ es invertible en $\mathbb{K}[x]/\!<p(x)>$*

Demostración: Como $r(x), p(x)$ son primos relativos entonces existen $q(x), s(x)$ tales que

$$\begin{aligned} 1 &= r(x)q(x) + p(x)s(x) \\ 1 &\equiv r(x)q(x)(\mathtt{mod}\ p(x)) \\ \overline{1} &= \overline{r(x)q(x)} \end{aligned}$$

Luego $\overline{r(x)}$ tiene inverso.

Teorema 183 *Si $p(x)$ polinomio irreducible en $\mathbb{K}[x]$, entonces $(\mathbb{K}[x]/< p(x) >, +, \cdot)$ es un cuerpo*

Demostración: Como $p(x)$ es irreducible y si $r(x) \in \mathbb{K}[x]$ no nulo, tal que

$$\text{gr}(r(x)) < \text{gr}(p(x)),$$

luego son primo relativos, por lo tanto $\overline{r(x)}$ es invertible. □

Ejemplo 126 *En $\mathbb{Z}_2[x]$ el polinomio x^2+x+1 es irreducible, luego*

$$\mathbb{Z}_2[x]/< x^2+x+1 >= \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$$

es un cuerpo con 4 elementos y las tabla de suma y producto son

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

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

Ejemplo 127 *En $\mathbb{R}[x]$ el polinomio x^2+1 es irreducible, luego*

$$\mathbb{R}[x]/< x^2+1 >= \{\overline{ax+b} \mid a, b \in \mathbb{R}\}$$

es un cuerpo

6.8. Ejercicios Desarrollados

Ejemplo 128 *Sea $p(x) = 3x^4 - 5ax^3 + 7cx^2 - 1$. Determinar $a, c \in \mathbb{R}$ tal que 1 es una raíz de $p(x)$ y al dividir $p(x)$ por $x+1$ el resto es 10*

Solución: Ya que 1 es una raíz de $p(x)$, luego $p(1) = 0$, además al dividir $p(x)$ por $x+1$ el resto 10, es decir, $p(-1) = 10$.

$$\begin{aligned} p(1) &= 3 - 5a + 7c - 1 = 0 \\ p(-1) &= 3 + 5a + 7c - 1 = 10 \end{aligned}$$

Luego tenemos

$$\left.\begin{aligned} -5a + 7c &= -2 \\ 5a + 7c &= 8 \end{aligned}\right|$$

Sumando la ecuaciones, obtenemos

$$\begin{aligned} 14c &= 6 \\ c &= \frac{6}{14} = \frac{3}{7} \end{aligned}$$

Reemplazando

$$5a = 8 - 7c = 8 - \frac{21}{7} = 8 - 3 = 5$$

Por lo tanto

$$a = 1, \qquad c = \frac{3}{7}$$

Ejemplo 129 *Sea $p(x) \in \mathbb{K}[x]$, tal que al dividir $p(x)$ por $x+2$ el resto es 4 y al dividir $p(x)$ por $x-3$ es resto es 5.*

Calcular el resto al dividir $p(x)$ por $(x+2)\cdot(x-3)$.

Solución: Como $\text{gr}((x+2)\cdot(x-3)) = 2$, luego el resto debe puede ser escrito de la forma $r(x) = ax + b$.

Sabemos que

$$\begin{aligned} p(x) &= q_1(x)\cdot(x+2)+4 \\ p(x) &= q_2(x)\cdot(x-3)+5 \end{aligned}$$

Además

$$p(x) = q(x)\cdot(x+2)\cdot(x-3)+ax+b$$

Evaluando tenemos

$$\begin{aligned} 4 = \quad p(-2) &= -2a+b \\ 5 = \quad p(3) &= 3a+b \end{aligned}$$

De lo cual, se obtiene el siguiente sistema

$$\begin{array}{rcl|} -2a+b & = & 4 \\ \hline 3a+b & = & 5 \\ \hline \end{array}$$

Cuya solución es:

$$a = \frac{1}{5} \qquad b = \frac{22}{5}$$

Por lo tanto $r(x) = \frac{1}{5}x + \frac{22}{5}$

Ejemplo 130 *Encontrar el valor de $a, b \in \mathbb{R}$ de manera que $(x-2)^2$ sea un factor del polinomio $p(x) = x^4 + (a-2)x^3 + bx^2 + (a+b)x + 4$*

Solución: Usemos división sintética, para obtener los resto que deben ser cero

2	1	$a-2$	b	$a+b$	4
		2	$2a$	$4a+2b$	$10a+6b$
2	1	a	$2a+b$	$5a+3b$	$\mathbf{10a+6b+4}$
		2	$2a+4$	$8a+2b+8$	
	1	$a+2$	$4a+b+4$	$\mathbf{13a+5b+8}$	

De lo cual tenemos el sistema

$$\begin{array}{rcl|} 10a+6b & = & -4 \\ \hline 13a+5b & = & -8 \\ \hline \end{array}$$

Cuya solución es:

$$a = -1 \qquad b = 1$$

Por lo tanto, el polinomio es $p(x) = x^4 - 3x^3 + x^2 + 4$.

Ejemplo 131 *Sea $p(x) \in \mathbb{R}[x]$, tal que al dividir $p(x)$ por $x-1$ el resto es 2, al dividir $p(x)$ por $x+2$ es resto es 4 y 2 es raíz de $p(x)$ Calcular el resto al dividir $p(x)$ por $(x-1)\cdot(x+2)\cdot(x-2)$.*

Solución: $\text{gr}((x-1)\cdot(x+2)\cdot(x-2)) = 3$, luego el resto debe tener la forma $r(x) = ax^2+bx+c$.
Sabemos que

$$\begin{aligned} p(x) &= q_1(x)\cdot(x-1)+2 \\ p(x) &= q_2(x)\cdot(x+2)+4 \\ p(x) &= q_3(x)\cdot(x-2)+0 \end{aligned}$$

Además

$$p(x) = q(x)\cdot(x-1)\cdot(x+2)\cdot(x-2)+ax^2+bx+c$$

Evaluando tenemos

$$\begin{aligned} 2 = \quad p(1) &= a+b+c \\ 0 = \quad p(2) &= 4a+2b+c \\ 4 = \quad p(-2) &= 4a-2b+c \end{aligned}$$

De lo cual tenemos el sistema

$$\left|\begin{array}{rcll} a+b+c &=& 2 & \\ 4a+2b+c &=& 0 & /\cdot -1 \\ 4a-2b+c &=& 4 & \end{array}\right|$$

Luego la solución es:

$$a = -\frac{1}{3}, \qquad b = -1, \qquad c = \frac{10}{3}$$

Por lo tanto $r(x) = -\frac{1}{3}x^2 - x + \frac{10}{3}$

Ejemplo 132 *Sea $p(x) = x^4-4$. Descomponer en factores irreducibles el polinomio $p(x)$ en $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$*

Solución:

a) En $\mathbb{Q}[x]$: $\quad x^4-4 = (x^2-2)\cdot(x^2+2)$

b) En $\mathbb{R}[x]$: $\quad x^4-4 = (x+\sqrt{2})\cdot(x-\sqrt{2})\cdot(x^2+2)$

c) En $\mathbb{C}[x]$: $\quad x^4-4 = (x+\sqrt{2})\cdot(x-\sqrt{2})\cdot(x+\sqrt{2}i)\cdot(x-\sqrt{2}i)$

Ejemplo 133 *Sea $p(x) = x^5+x^4+x^3+x^2+x+1$. Descomponer en factores irreducibles el polinomio $p(x)$ en $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$*

Solución: Como $p(-1) = 0$, luego tenemos $p(x) = (x+1)(x^4+x^2+1) = (x+1)((x^2+1)^2-x^2)$

a) En $\mathbb{Q}[x]$: $p(x) = (x+1)\cdot(x^2+x+1)\cdot(x^2-x+1)$

b) En $\mathbb{R}[x]$: $p(x) = (x+1)\cdot(x^2+x+1)\cdot(x^2-x+1)$

c) En $\mathbb{C}[x]$:

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

Ejemplo 134 *Sea* $p(x) = x^4+5x^3+12x^2+22x-40$

a) Determine las raíces racionales de $p(x)$.

b) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{Q}[x]$

c) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$

d) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{C}[x]$

Solución: Sea $p(x) = x^4+5x^3+12x^2+22x-40$

a) Determine las raíces racionales de $p(x)$.

La posibles raíces racionales $\frac{p}{q}$, tal que p, q primos relativos entonces $p|-40, \quad q|1$

$$p \in \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm20, \pm40\} \qquad q \in \{\pm1\}$$

Luego

$$\frac{p}{q} \in \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm20, \pm40\}$$

1	1	5	12	22	-40
		1	6	18	40
-4	1	6	18	40	0
		-4	-8	-40	
	1	2	10	0	

Por lo tanto las raíces racionales son: $1, -4$.

b) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{Q}[x]$

$p(x) = (x-1)\cdot(x+4)\cdot(x^2+2x+10)$

c) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{R}[x]$

$p(x) = (x-1)\cdot(x+4)\cdot(x^2+2x+10)$

d) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{C}[x]$

El discriminante de $x^2+2x+10$ es $\Delta=-36$, la raíces son $-1+3i,\ -1-3i$. por lo tanto

$$p(x)=(x-1)\cdot(x-4)\cdot(x-(-1+3i))\cdot(x-(-1-3i))$$

Ejemplo 135 *Factorizar $x^6-x^5+x^4-x^3+x^2-x$ como producto de polinomios irreducibles en $\mathbb{Z}_7[x]$*

Solución: $p(x)=x^6-x^5+x^4-x^3+x^2-x=x\cdot(x^5-x^4+x^3-x^2+x-1)$

1	1	-1	1	-1	1	-1
		1	0	1	0	1
2	1	0	1	0	1	0
		2	4	10	20	
-2	1	2	5	10	$21=0$	
		-2	0	-10		
3	1	0	5	0		
		3	9			
-3	1	3	$14=0$			
		-3				
	1	0				

Por lo tanto $p(x)=x\cdot(x-1)\cdot(x-2)\cdot(x+2)\cdot(x-3)\cdot(x+3)$

Ejemplo 136 *Encuentre los valores del parámetro k en la ecuación $x^3-7x+k=0$ de modo que una de sus raíces sea el doble de la otra. Y en cadas casos, determine las soluciones de la ecuación.*

Solución: Sean $a, 2a, c$ las distintas raíces

$$\begin{aligned}
x^3-7x+k &= (x-a)\cdot(x-2a)\cdot(x-c)\\
x^3-7x+k &= (x^2-2ax+2a^2-ax)\cdot(x-c)\\
x^3-7x+k &= x^3-x^2c-2ax^2+2acx+2a^2x-2a^2c-ax^2+acx\\
x^3-7x+k &= x^3+x^2\cdot(-c-3a)+x\cdot(3ac-2a^2)-2a^2c
\end{aligned}$$

De lo cual tenemos el sistema

$$\left.\begin{aligned}
-c-3a &= 0\\
3ac+2a^2 &= -7\\
-2a^2c &= k
\end{aligned}\right|$$

Luego la solución es:

$$((a=1\ \wedge\ c=-3\ \wedge\ k=6)\ \ \vee\ \ (a=-1\ \wedge\ c=3\ \wedge\ k=-6))$$

Por lo tanto, los polinomio se factorizan

$$x^3-7x+6=(x-1)(x-2)(x+3),\qquad x^3-7x-6=(x+1)(x+2)(x-3),$$

Ejemplo 137 *Dadas las raíces a, b, c de $x^3 - px + q = 0$, construya un polinomio de grado 3 cuyas raíces son a^2, b^2, c^2*

Solución: Como son las raíces luego tenemos

$$\begin{aligned} x^3 - px + q &= (x-a)\cdot(x-b)\cdot(x-c) \\ x^3 - px + q &= x^3 + (-a-b-c)\cdot x^2 + (ab+bc+ac)\cdot x - abc \end{aligned}$$

Igualando coeficiente se obtiene

$$\begin{aligned} -a-b-c &= 0 \\ ab+bc+ac &= -p \\ -abc &= q \end{aligned}$$

Por otra parte el polinomio construir

$$\begin{aligned} (x-a^2)(x-b^2)(x-c^2) &= (x^2 - a^2x - b^2x + a^2b^2)(x-c^2) \\ (x-a^2)(x-b^2)(x-c^2) &= x^3 + x^2(-a^2-b^2-c^2) + x(a^2b^2+b^2c^2+a^2c^2) - a^2b^2c^2 \end{aligned}$$

Necesitamos determinar los coeficiente en termino de p, q, el coeficiente constante del nuevo polinomio es

$$-a^2b^2c^2 = -(abc)^2 = -q^2$$

El coeficiente cuadrático

$$-a^2 - b^2 - c^2 = -(a-b-c)^2 + 2(ab+ac+bc) = 0 - 2p = -2p$$

El coeficiente lineal

$$a^2b^2 + b^2c^2 + a^2c^2 = (ab+bc+ac)^2 - 2(acb^2 + bca^2 + bac^2) = p^2 - 2abc(b+a+c) = p^2$$

Por lo tanto el polinomio pedido es

$$x^3 - 2px^2 + p^2x - q^2.$$

Ejemplo 138 *Sea $\mathbb{F}_9 = \mathbb{Z}_3[x]/< x^2+1 >$. Calcule $[x^5 + 2x^2 + 1]^{-1}$*

Solución: Sabemos que

$$\mathbb{F}_9 = \{\overline{ax+b} \quad | \quad a, b \in \mathbb{Z}_3\} = \mathbb{Z}_3[x]/< x^2+1 >$$

Además, aplicando el algoritmo de la división se tiene

$$x^5 + 2x^2 + 1 = (x^2+1)(x^3 - x + 2) + (x-1)$$

Luego

$$\overline{x^5 + 2x^2 + 1} = \overline{x-1} \in \mathbb{F}_9$$

Ahora debemos determinar

$$(x-1)Y \equiv 1(\texttt{mod}\ x^2+1)$$

Pero notemos que

$$x^2+1=(x-1)(x+1)+2$$

De lo cual obtenemos

$$\overline{(x-1)(x+1)}=1$$

de esta manera tenemos

$$[x^5+2x^2+1]^{-1}=[x-1]^{-1}=[x+1]$$

Ejemplo 139 *Sea* $\mathbb{F}_9=\mathbb{Z}_3/<x^2+1>$ *y* $\overline{x^6+x^3+2}\in\mathbb{F}_9$. *Calcular* $\overline{x^6+x^3+2}^{-1}$

Solución: Sabemos que

$$\mathbb{F}_9 \quad = \quad \{\overline{ax+b} \quad | \quad a,b\in\mathbb{Z}_3\}=\mathbb{Z}_3/<x^2+1>$$

Además

$$x^6+x^3+2=(x^2+1)(x^4-x^2+x+1)+(-x+1)$$

Luego

$$\overline{x^6+x^3+2}=\overline{2x+1}\in\mathbb{F}_9$$

Ahora aplicando el algoritmo de la división tenemos

$$x^2+1=(2x+1)(2x-1)+2$$

De lo cual obtenemos

$$\overline{(2x+1)(2x-1)}=1$$

de esta manera tenemos

$$\overline{x^6+x^3+2}^{-1}=\overline{2x+1}^{-1}=\overline{2x-1}$$

Apéndice A

EJERCICIOS

A.1. Ejercicios Propuestos

A.1.1. Números Enteros

Ejercicio 1 *Demostrar que* $\forall n \in \mathbb{N}: \quad 6|(n(n+1)(n^2+n+1))$.

Ejercicio 2 *Demostrar que* $\forall n \in \mathbb{N}: \quad 30|(n^5-n)$.

Ejercicio 3 *Demostrar que* $\forall n \in \mathbb{Z}: \quad 4$ *no divide a* n^2-n.

Ejercicio 4 *Demostrar que el producto de dos números enteros impares da un entero impar.*

Ejercicio 5 *Si* $b|c$ *y* $(a,c)=1$ *entonces* $(a,b)=1$.

Ejercicio 6 *Sean* $x,y,r \in \mathbb{Z}$ *tales que* $(r,11)=1$, $r|(2x-y)$, $r|(x+5y)$. *Demuestre que* $r|x$

Ejercicio 7 *Si* $n \in \mathbb{Z}^+$. *Calcular* $(n,n+1), \quad [n,n+1]$

Ejercicio 8 *Encontrar el máximo común divisor MCD en los siguientes caso:*

i) $(232,548)$

ii) $(54,138,1104)$

Ejercicio 9 *Determinar la solución general de cada ecuación diofántica lineal.*

i) $598 \cdot x + 767 \cdot y = 26$

ii) $3 \cdot x + 9 \cdot y + 13 \cdot z = 1$

A.1.2. Números Enteros Módulo m

Ejercicio 10 *Calcular el orden de:*

I) $\overline{3} \in (\mathbb{Z}_{69}, +)$

II) $\overline{5} \in (\mathcal{U}(\mathbb{Z}_{31}), \cdot)$

III) $\overline{7} \in (\mathcal{U}(\mathbb{Z}_{29}), \cdot)$

Ejercicio 11 *Hacer la tabla del grupo:*

I) $(\mathbb{Z}_8, +)$

II) $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$

Ejercicio 12 *Hacer la tabla y determinar los generadores de* $\mathcal{U}(\mathbb{Z}_{10})$

Ejercicio 13 *Calcular el número y las raíces primitivas o los generadores:*

I) $(\mathbb{Z}_{24}, +)$

II) $(\mathbb{Z}_{30}, +)$

III) $(\mathbb{Z}_{300}, +)$

IV) $(\mathbb{Z}_{890}, +)$

V) $(\mathcal{U}(\mathbb{Z}_{11}), \cdot)$

VI) $(\mathcal{U}(\mathbb{Z}_{12}), \cdot)$

VII) $(\mathcal{U}(\mathbb{Z}_{18}), \cdot)$

VIII) $(\mathcal{U}(\mathbb{Z}_{25}), \cdot)$

IX) $(\mathcal{U}(\mathbb{Z}_{43}), \cdot)$

Ejercicio 14 *Determinar generadores y subgrupos de:*

I) $\mathcal{C}_{13} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{13})\}$

II) $\mathcal{C}_{31} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{31})\}$

Ejercicio 15 *Calcular el reticulado de los subgrupos de* $(\mathbb{Z}_{16}, +)$

Ejercicio 16 *Sea* $\mathcal{G} =< g >$ *grupo cíclico tal que* $|\mathcal{G}| = 12$. *Calcular el reticulado de los subgrupos de* $\mathcal{G}$.

Ejercicio 17 *Determine si* $(\mathcal{U}(\mathbb{Z}_{23}), \cdot)$ *es un grupo cíclico, en caso afirmativo encuentre un generador.*

Ejercicio 18 *Determinar el resto al dividir:*

I) 7^{2702} *por* 31

II) $2^{100} + 3^{20} + 7^{89}$ *por* 19

III) 473^{38} *por* 5

Ejercicio 19 *¿Cuál es el dígito de las unidades en la representación decimal de* 3^{400}*?*

Ejercicio 20 *Encontrar el menor entero positivo que deja restos* $2, 3, 2$ *cuando es divido por* $3, 5, 7$ *respectivamente.*

Ejercicio 21 *Calcular los elementos, generadores y hacer la tabla de:*

I) $\square_{17}$

II) $\square_{22}$

Ejercicio 22 *Determine el número de soluciones en cada caso*

I) $x^2 \equiv 5(\texttt{mod } 73)$

II) $x^2 \equiv 226(\texttt{mod } 563)$

III) $x^3 \equiv 8(\texttt{mod } 719)$

IV) $x^2 \equiv 150(\texttt{mod } 1009)$

V) $x^4 \equiv 9(\texttt{mod } 4003)$

VI) $x^6 \equiv 1(\texttt{mod } 19)$

Ejercicio 23 *Resolver las siguientes ecuaciones*

I) $x^2 \equiv 5(\texttt{mod } 29)$

II) $x^2 \equiv 2(\texttt{mod } 97)$

III) $x^{954} + 2x - 1 \equiv 0(\texttt{mod } 953)$

IV) $x^3 \equiv 8(\texttt{mod } 31)$

V) $x^6 + 2x^3 + 3 \equiv 0(\texttt{mod } 23)$

VI) $x^{15} - x^{10} + 4x - 3 \equiv 0(\texttt{mod } 7)$

VII) $x^8 + x^2 \equiv 0(\texttt{mod } 7) \quad 0 \leq x \leq 30$

VIII) $x^5 - x^3 \equiv 0(\texttt{mod } 43)$

Ejercicio 24 *Resolver en* $\mathbb{Z}_{21}$*:*

$$\overline{x} + \overline{73} = \overline{68}$$

Ejercicio 25 *Determinar todos los* $\overline{x} \in \mathbb{Z}_7$ *tal que*

$$\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$$

Ejercicio 26 *Demostrar que para todo entero* a, n *tales que son primo relativos con* 31 *entonces* $31 | n^{30} - a^{30}$

Ejercicio 27 *Determinar todos los* p *primos impares tal que* $\left(\frac{5}{p}\right) = -1$

Ejercicio 28 *Resolver:*

a.
$$\begin{array}{rcl} 3x + 2y & \equiv & 1 (\mathtt{mod}\ 7) \\ 2x + 5y & \equiv & 2 (\mathtt{mod}\ 7) \end{array}$$

b.
$$\begin{array}{rcl} x + 12y & \equiv & 9 (\mathtt{mod}\ 13) \\ 3x + 11y & \equiv & 8 (\mathtt{mod}\ 13) \end{array}$$

c.
$$\begin{array}{rcl} x + y + z & \equiv & 2 (\mathtt{mod}\ 7) \\ x + 2y + 3z & \equiv & 3 (\mathtt{mod}\ 7) \\ 2x + y + 4z & \equiv & 1 (\mathtt{mod}\ 7) \end{array}$$

d.
$$\begin{array}{rcl} x + 2y + 4z & \equiv & 5 (\mathtt{mod}\ 13) \\ 5x + y + 8z & \equiv & 7 (\mathtt{mod}\ 13) \\ 6x + 8y + 7z & \equiv & 1 (\mathtt{mod}\ 13) \end{array}$$

e.
$$\begin{array}{rcl} x & \equiv & 7 (\mathtt{mod}\ 9) \\ x & \equiv & 10 (\mathtt{mod}\ 4) \\ x & \equiv & 1 (\mathtt{mod}\ 7) \end{array}$$

f.
$$\begin{array}{rcl} x & \equiv & 1 (\mathtt{mod}\ 4) \\ x & \equiv & 0 (\mathtt{mod}\ 3) \\ x & \equiv & 5 (\mathtt{mod}\ 7) \end{array}$$

g.
$$\begin{array}{rcl} 3x & \equiv & 1 (\mathtt{mod}\ 5) \\ 4x & \equiv & 6 (\mathtt{mod}\ 14) \\ 5x & \equiv & 11 (\mathtt{mod}\ 3) \end{array}$$

h.
$$\begin{array}{rcl} x - y & \equiv & 5 (\mathtt{mod}\ 47) \\ xy & \equiv & 6 (\mathtt{mod}\ 47) \end{array}$$

i.
$$\begin{array}{rcl} x^2 + y^2 & \equiv & 1 (\mathtt{mod}\ 13) \\ xy & \equiv & 2 (\mathtt{mod}\ 13) \end{array}$$

Ejercicio 29 *Determinar los* $\alpha \in \mathbb{Z}_{41}$ *tal que*

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

el sistema no tenga solución.

Ejercicio 30 *Si* $p \equiv 3 (\mathtt{mod}\ 4)$*. Determine si existen* $x, y \in \mathbb{Z}$ *tal que* $x^2 + y^2 = p$

Ejercicio 31 *Sea* p *primo impar. Demostrar:* $\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} \equiv 0 (mod, p)$

Ejercicio 32 *Sea* p *primo impar. Calcular* $\prod_{\overline{x} \in \square_p} \overline{x}$

Ejercicio 33 *Calcular* $\sum_{\overline{x} \in \square_p} \overline{x}$

Ejercicio 34 *Determinar todos los* $x, y \in \mathbb{Z}$ *que cumplan con:* $x, y \in \mathbb{Z}^+$, $x + y = 100$ *y* $(x, y) = 5$

Ejercicio 35 *Probar que si* x, y *son impares entonces* $x^2 + y^2$ *es par pero no divisible por cuatro.*

Ejercicio 36 *Sean* $a, b \in \mathbb{Z}$ *entonces demuestre que:*
Si $a^2 = 2 \cdot b^2$ *entonces* a *y* b *son pares.*

Ejercicio 37 *Sean* $a, b \in \mathbb{Z}$ *entonces demuestre que:*
Si $(a, 4) = 2, \quad (b, 4) = 2$ *entonces* $(a + b, 4) = 4$

A.1.3. Números Complejos

Ejercicio 38 *Determinar* $z \in \mathbb{C}$ *tal que:*

I) $\overline{z} + 2z = 4 + i$

II) $\overline{z} + 5z + 6 = z^2$

III) $z^2 + |z| = 0$

IV) $\left|\frac{z-12}{z-8i}\right| = \frac{5}{3}$

Ejercicio 39 *Demostrar:*

I) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

II) $|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2|z_1|^2 + 2|z_2|^2$

Ejercicio 40 *Determinar el lugar geométrico de:*

I) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 4 \leq |z - 1| + |z + 1| \leq 8\}$

II) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad \frac{1}{2} \leq |z| \leq 1\}$

III) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 1 + i| = 4\}$

IV) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 2| = |1 - 2\overline{z}|\}$

V) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad Re(\overline{z} - i) = 2\}$

VI) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Im(z) \leq 2\}$

VII) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Re(z) \leq 2\}$

VIII) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 4i| + |z + 4i| = 10\}$

IX) *Sean* $a, c \in \mathbb{R}, b \in \mathbb{C}$ *fijos* $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c = 0\}$

Ejercicio 41 *Sean* $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z| = 3\}, \quad \mathcal{B} = \{z \in \mathbb{C} \quad | \quad |z-1| = |z-i|\}$. *Calcular* $\mathcal{A} \cap \mathcal{B}$

Ejercicio 42 *Si* $|z| = 1$ *y* $w, z \in \mathbb{C}$, *demuestre que* $|z+w| = |\overline{z}w + 1|$

Ejercicio 43 *Encontrar el Arg(z) cuando:*

I) $z = -2 + 2\sqrt{3}i$

II) $z = -\frac{2}{1+\sqrt{3}i}$

Ejercicio 44 *Escriba en forma polar:*

I) $-\sqrt{2} - \sqrt{2}i$

II) $z = -\frac{2}{1+\sqrt{3}i}$

Ejercicio 45 *Encuentre el valor de:*

I) $\frac{(-\sqrt{2}-\sqrt{2}i)^{16}}{(-1+i)^4}$

II) $\left(\frac{1+\sqrt{3}i}{1-i}\right)^{40}$

III) $(1+i)^n + (1-i)^n$

Ejercicio 46 *Determinar todos los* $z \in \mathbb{C}$ *tal que:* $\left(\frac{1-z}{i+z}\right)^3 = 1$

Ejercicio 47 *Encuentre en cada caso, las siguientes raíces n-esima de:*

I) $-i \qquad n = 3$

II) $-1 \qquad n = 4$

III) $2 - 2\sqrt{3}i \qquad n = 2$

IV) $-\frac{\sqrt{3}}{2} + \frac{1}{2}i \qquad n = 3$

Ejercicio 48 *Determine si* $2 + 3i$ *divide* $4 + 8i$ *en* $\mathbb{Z}[i]$ *Justifique.*

Ejercicio 49 *Determine si* $7 + 5i$ *es primo en* $\mathbb{Z}[i]$ *Justifique*

Ejercicio 50 *Determine si* 7 *es primo en* $\mathbb{Z}[i]$*? Justifique*

Ejercicio 51 *Sea* $p(x) = x^4 + ax^2 + bx + 5$. *Determinar* a, b *si* 1 *y* -2 *son raíces de* $p(x)$.

A.1.4. Polinomios

Ejercicio 52 *Determinar todas las raíces de* $x^8 + x^4 + 1$

Ejercicio 53 *Sea* $p(x) = 3x^3 + 2x^2 + cx - k$. *Determinar* $c, k \in \mathbb{R}$ *tal que al dividir* $p(x)$ *por* $x + 2$ *el resto es* 37 *y al dividir* $p(x)$ *por* $x - 1$ *el resto es* -2.

Ejercicio 54 *Sea* $p(x) = 2x^3 + bx^2 + cx + d$. *Determinar los valores de* $b, c, \in \mathbb{R}$ *de modo que se cumplan. El resto al dividir* $p(x)$ *por* x *es* $2 + b$, *el resto al dividir* $p(x)$ *por* $x + 1$ *es* $b + d$, 1 *es raíz de* $p(x)$

Ejercicio 55 *Sea* $p(x) \in \mathbb{R}[x]$. *Al dividir* $p(x)$ *por* $x-3$ *el resto es 2. Al dividir* $p(x)$ *por* $x-4$ *es resto es 6 y 2 es raíz de* $p(x)$ *Calcular el resto al dividir* $p(x)$ *por* $(x-2)\cdot(x-3)\cdot(x-4)$.

Ejercicio 56 *Determinar* $a, b \in \mathbb{R}$ *para que* -1 *sea raíz doble (o de multiplicidad dos) de* $p(x) = x^4 + ax^3 + (a-b)x^2 + bx + 1$

Ejercicio 57 *Sea* $p(x) = 6x^3 + tx^2 + kx - 3t$ *encontrar los valores de* $t, k \in \mathbb{R}$ *tal que al dividir* $p(x)$ *por* $x - 2$ *el resto es* 21 *y* 1 *es raíz de* $p(x)$.

Ejercicio 58 *Sea* $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$. *Determine los valores de* $a, b \in \mathbb{R}$ *para que* 1 *y* $\frac{1}{2}$ *sean raíces de* $p(x)$.

Ejercicio 59 *Sea* $p(x) \in \mathbb{R}[x]$. *Al dividir* $p(x)$ *por* $x + 1$ *el resto es 2. Al dividir* $p(x)$ *por* $x - 1$ *es resto es 3. Calcular el resto al dividir* $p(x)$ *por* $(x+1)\cdot(x-1)$.

Ejercicio 60 *Sea* $p(x) = x^6 - 1$. *Descomponer en factores irreducibles el polinomio* $p(x)$ *en* $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

Ejercicio 61 *Sea* $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$. *Determinar los valores de* $a, b \in \mathbb{R}$ *para que* 1 *y* $\frac{1}{2}$ *sean raíces de* $p(x)$ *y factoricé* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$.

Ejercicio 62 *Sea* $p(x) = x^6 - x^5 - 5x^4 + 5x^3 - 36x^2 + 36x$

I) *Determine las raíces racionales de* $p(x)$

II) *Factorize* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$

III) *Factorize* $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{C}[x]$

Ejercicio 63 *Descomponer* $x^8 + x^4 + \overline{1} \in \mathbb{Z}_7[x]$ *en factores irreducibles.*

Ejercicio 64 *Exprese* $x^4 + \overline{4} \in \mathbb{Z}_5[x]$ *como el producto de polinomios irreducibles.*

Ejercicio 65 *Sea* $p(x) = x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$. *Descomponer* $p(x)$ *en factores irreducibles.*

Ejercicio 66 *Dadas las raíces a, b, c de $x^3+x^2+x+1=0$, construya un polinomio de grado 3 cuyas raíces son a^2, b^2, c^2*

Ejercicio 67 *Dadas las raíces a, b, c de $x^3+2x^2+3x+1=0$, construya un polinomio de grado 3 cuyas raíces son a^2, b^2, c^2*

Ejercicio 68 *Si a, b, c son las raíces del polinomio x^3-x^2-1. Determine el polinomio de grado 3 cuyas raíces son $a+b, a+c, b+c$*

Ejercicio 69 *Exprese $x^8+\overline{4} \in \mathbb{Z}_5[x]$ como el producto de polinomios irreducibles.*

Ejercicio 70 *Hacer la tabla de suma y multiplicación del siguiente anillo $\mathbb{Z}_3[x]/ < x^2-\overline{1} >$*

Ejercicio 71 *Sea el cuerpo $\mathbb{F}_{27} = \mathbb{Z}_3[x]/ < x^3+2x+1 >$. Sea $\overline{x^4+\overline{1}} \in \mathbb{F}_{27}$. Calcule $\overline{x^4+\overline{1}}^{-1}$*

Ejercicio 72 *Sea $\mathbb{F}_{25} = \mathbb{Z}_5[x]/ < x^2+x+1 >$. Calcule $[x^7+x^5+x^4+4]^{-1}$*

Ejercicio 73 *$\mathbb{F}_8^* = \mathcal{U}(\mathbb{Z}_2[x]/ < x^3+x+1 >)$ es cíclico?*

Ejercicio 74 *Sea $\mathbb{F}_9 = \mathbb{Z}_3[x]/ < x^2+1 >$. En el grupo $(\mathbb{F}_9^*, \cdot)$. Determine el orden de cada elemento.*

Ejercicio 75 *$\mathbb{Z}_{19}[x]/ < x^2-8 >$ es un cuerpo?*

Ejercicio 76 *Hacer la tabla del grupo de los cuadrados de $\mathbb{F}_9$*

Ejercicio 77 *Determine α para que $\mathbb{Z}_7[x]/ < x^2-\alpha >$ no sea un cuerpo.*

A.2. Respuesta Ejercicios Propuestos

A.2.1. Números Enteros

Solución 1. La demostración se realizar usando el principio de inducción.

Sea $p(n) : 6|n(n+1)(n^2+n+1)$

Primer paso: $p(0) : 6|0$, es verdadero.

Segundo paso: Supongamos $p(n) : 30|(n(n+1)(n^2+n+1)$ es verdadero, y demostremos que $p(n+1)$ es verdadero

Para ello notemos primero que

$$6|(n+1)(n+2)((n+1)^2+(n+1)+1) \Leftrightarrow (n+1)(n+2)(n^2+3n+3) = 6 \cdot q; \quad q \in \mathbb{Z}.$$

de otro modo tenemos

$$\begin{aligned} & (n+1)(n+2)(n^2+3n+3) \\ = \; & n(n+1)(n^2+3n+3) + 2(n+1)(n^2+3n+3) \\ = \; & n(n+1)(n^2+n+1) + 2(n+1)n(n+1) + 2(n+1)(n^2) + 6(n+1)^2 \\ = \; & n(n+1)(n^2+n+1) + 2(n+1)(n^2+n+n^2) + 6(n+1)^2 \\ = \; & n(n+1)(n^2+n+1) + 2(n+1)n(2n+1) + 6(n+1)^2 \end{aligned}$$

Por hipótesis de inducción el primer sumando es múltiplo de 6, el segundo es 12 veces la suma de los primeros naturales al cuadrado, y el tercero es múltiplo de 6, luego $p(n+1)$ es verdadero y por el principio de inducción se tiene que:

$$\forall n \in \mathbb{N}: \quad 6|(n(n+1)(n^2+n+1)).$$

♡

Solución 2. La demostración se realizar usando el principio de inducción.

Sea $p(n) : 30|(n^5 - n)$

Primer paso: $p(0) : 30|0$, es verdadero.

Segundo paso: Supongamos $p(n) : 30|(n^5 - n)$ es verdadero, y demostremos que $p(n+1)$ es verdadero.

Para ello notemos primero que

$$30|((n+1)^5 - (n+1)) \Leftrightarrow (n+1)^5 - (n+1) = 30 \cdot q; \quad q \in \mathbb{Z}.$$

Desarrollando el binomio obtenemos

$$\begin{aligned}(n+1)^5 - (n+1) &= n^5 + 5 \cdot n^4 + 10 \cdot n^3 + 10 \cdot n^2 + 5 \cdot n + 1 - n - 1 \\ &= n^5 - n + 5 \cdot (n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n)\end{aligned}$$

Aplicando hipótesis de inducción tenemos

$$(n+1)^5 - (n+1) = 30 \cdot k + 5 \cdot (n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n)$$

Para poder concluir necesitamos que

$$\forall n \in \mathbb{N}: \quad 6|(n^4 + 2 \cdot n^3 + 2 \cdot n^2 + n) \Leftrightarrow n(n+1)(n^2+n+1) = 6 \cdot r; \quad r \in \mathbb{Z},$$

lo cuál esta demostrado en el ejercicio anterior, por ello obtenemos

$$\begin{aligned}(n+1)^5 - (n+1) &= 30 \cdot k + 5 \cdot 6 \cdot r \\ &= 30 \cdot k + 30 \cdot r \\ &= 30 \cdot (k + r)\end{aligned}$$

De este modo obtenemos que $p(n+1)$ es verdadero y por el principio de inducción se obtiene que

$$\forall n \in \mathbb{N}: \quad 30|(n^5 - n).$$

♡

Solución 3. La demostración se realizara por el método del absurdo.

Para ello supongamos que existe $n \in \mathbb{Z}$ tal que $4|(n^2+2) \Leftrightarrow n^2 + 2 = 4 \cdot q; \quad q \in \mathbb{Z}$.

Notemos que al dividir un número por 2 se obtiene 2 posibles resto $0, 1$, lo cual significa que

$$\mathbb{Z} = \{2 \cdot k \mid k \in \mathbb{Z}\} \cup \{2 \cdot k + 1 \mid k \in \mathbb{Z}\}$$

Recordemos que $a|b \wedge a|c$ entonces $a|(bx+cy)$

Caso Supongamos $n = 2 \cdot k$ de lo cual obtenemos $n^2 = 4 \cdot k^2$, reemplazando obtenemos

$$4|(4 \cdot k^2 + 2) \Rightarrow 4|2.$$

lo que es una contradicción.

Por lo tanto 4 no divide a n^2+2, con $n = 2 \cdot k$.

Caso Supongamos $n = 2 \cdot k+1$ de lo cual $n^2 = (2 \cdot k+1)^2 = 4k^2+4k+1$, reemplazando obtenemos

$$4|(4 \cdot k^2 + 4k + 1 + 2) \Rightarrow 4|3$$

lo que es una contradicción.

Por lo tanto 4 no divide a n^2+2 con $n = 2 \cdot k+1$

Por ello se tiene que $\forall n \in \mathbb{Z}:$ 4 no divide a n^2+2. ♡

Solución 4. Sean m, n números impares, luego $m = 2 \cdot k+1; \quad k \in \mathbb{Z}$, $n = 2 \cdot q+1; \quad q \in \mathbb{Z}$

$$\begin{aligned} m \cdot n &= (2 \cdot k+1) \cdot (2 \cdot q+1) \\ &= 4 \cdot k \cdot q + 2 \cdot q + 2 \cdot q + 1 \\ &= 2 \cdot (2 \cdot q \cdot k + q + k) + 1 \\ &= 2 \cdot r + 1; \quad \text{con } r = 2 \cdot q \cdot k + q + k \end{aligned}$$

Por lo tanto, el producto de dos números enteros impares es un entero impar. ♡

Solución 5. Supongamos que $b|c$ y $(a,c) = 1$, como $b|c \Leftrightarrow c = b \cdot r; \quad r \in \mathbb{Z}$, además existen $x, y \in \mathbb{Z}$ tales que $1 = a \cdot x + c \cdot y$.

$$\begin{aligned} 1 &= a \cdot x + c \cdot y \\ &= a \cdot x + b \cdot r \cdot y \\ &= a \cdot x + b \cdot y_0; \quad y_0 = r \cdot y, \end{aligned}$$

es decir, existen $x_0, y_0 \in \mathbb{Z}$, tales que $a \cdot x + b \cdot y_0 = 1$, por ende, se tiene que $(a,b) = 1$. ♡

Solución 6. Sean $x, y, r \in \mathbb{Z}$ tales que $(r, 11) = 1$, $r|(2x-y)$, $r|(x+5y)$. Por demostrar $r|x$

Como

$$r|(2x-y) \quad \wedge \quad r|(x+5y)$$

Luego existen $q_1, q_2 \in \mathbb{Z}$, tale que

$$2x - y = r \cdot q_1; \quad x + 5y = r \cdot q_2$$

Además $(r, 11) = 1$, por lo cual, existen $a, b \in \mathbb{Z}$ tal que $ra + 11b = 1$. Es decir,

$$\begin{array}{|rcl} 1 &=& ra + 11b \\ 2x - y &=& r \cdot q_1 \\ x + 5y &=& r \cdot q_2 \end{array}$$

Amplificando por 5, la segunda ecuación y sumando a la tercera obtenemos

$$11x = r \cdot (5q_1 + q_2) = r \cdot k; \quad k = 5q_1 + q_2$$

Ahora amplificando por x la primera ecuación y reemplazando $11x$

$$\begin{aligned} x &= rax + 11xb \\ x &= rax + rkb = r \cdot (ax + kb) \end{aligned}$$

Por lo tanto $r|x$ ♡

Solución 7. Dado $n \in \mathbb{Z}^+$. Calcular $(n, n+1),\ [n, n+1]$.

Para ello notemos que

$$(n+1) \cdot (1) + n \cdot (-1) = 1$$

Por lo tanto $(n, n+1) = 1$

$$[n, n+1] = \frac{n \cdot (n+1)}{(n, n+1)}$$

Por lo tanto $[n, n+1] = n \cdot (n+1)$. ♡

Solución 8.

i) Calcular $(232, 548)$, para ello

$$\begin{array}{lll} 548 = 232 \cdot 2 + 84; & 232 = 84 \cdot 2 + 64; & 84 = 64 \cdot 1 + 20; \\ 64 = 20 \cdot 3 + 4; & 20 = 4 \cdot 5 + 0. & \end{array}$$

Por lo tanto $(232, 548) = 4$

ii) Calcular $(54, 138, 1104)$, para ello

$$\begin{array}{lll} 138 = 54 \cdot 2 + 30; & 54 = 30 \cdot 1 + 24; & 30 = 24 \cdot 1 + 6; \\ 24 = 6 \cdot 4; & 1104 = 6 \cdot 184. & \end{array}$$

Por lo tanto $(54, 138, 1104) = ((54, 138), 1104) = (6, 1104) = 6$

♡

Solución 9.

i) Resolver $598 \cdot x + 767 \cdot y = 26$

$$\begin{array}{lll} 767 = 598 \cdot 1 + 169; & 598 = 169 \cdot 3 + 91; & 169 = 91 \cdot 1 + 78; \\ 91 = 78 \cdot 1 + 13; & 78 = 13 \cdot 6. & \end{array}$$

Por lo tanto $(598, 767) = 13$, determines una solución

$$\begin{aligned} 13 &= 91 - 78 \cdot 1 = 91 - 1 \cdot (169 - 91 \cdot 1) \\ &= 91 - 169 \cdot 1 + 91 \cdot 1 = 91 \cdot 2 - 169 \cdot 1 \\ &= 2 \cdot (598 - 169 \cdot 3) - 169 \cdot 1 = 598 \cdot 2 - 169 \cdot 6 - 169 \cdot 1 \\ &= 598 \cdot 2 - 169 \cdot 7 = 598 \cdot 2 - 7 \cdot (767 - 598 \cdot 1) \\ &= 598 \cdot 2 - 767 \cdot 7 + 598 \cdot 7 = 598 \cdot (9) + 767 \cdot (-7) \end{aligned}$$

Luego amplificando por 2 obtenemos

$$26 = 598 \cdot (18) + 767 \cdot (-14)$$

Por lo tanto, una solución particular es $x_0 = 18$, $y_0 = -14$

Solución general:

$$\begin{aligned} x &= 18 + \frac{767}{13} \cdot t \qquad & y &= -14 - \frac{598}{13} \cdot t \quad t \in \mathbb{Z} \\ x &= 18 + 59 \cdot t \qquad & y &= -14 - 46 \cdot t \quad t \in \mathbb{Z} \end{aligned}$$

II) Resolver $3 \cdot x + 9 \cdot y + 13 \cdot z = 1$.

Notemos que $(3, 9) = 3$, luego la ecuación

$$3 \cdot x + 9 \cdot y = 3 \cdot t; \Longleftrightarrow x + 3 \cdot y = t; \quad t \in \mathbb{Z},$$

siempre tiene solución.

Primero resolvemos: $3 \cdot t + 13 \cdot z = 1$

$$13 = 3 \cdot 4 + 1; \qquad 3 = 1 \cdot 3 + 0.$$

Por lo tanto $(3, 13) = 1$.

$$1 = 3 \cdot (-4) + 13 \cdot (1),$$

luego una solución particular es $t_0 = -4,\ z_0 = 1$.

Veamos la solución general de la primera parte

$$t = -4 + 13 \cdot s \qquad z = 1 - 3 \cdot s \quad s \in \mathbb{Z}.$$

Ahora veremos la solución del problema original $x + 3 \cdot y = -4 + 13 \cdot s$. Pero

$$\begin{aligned} 1 &= 1 \cdot (-2) + 3 \cdot (1) \quad / \cdot -4 + 13 \cdot s \\ -4 + 13 \cdot s &= 1 \cdot (8 - 26 \cdot s) + 3 \cdot (-4 + 13 \cdot s) \end{aligned}$$

Por lo tanto $x_0 = 8 - 26 \cdot s$, $y_0 = -4 + 13 \cdot s$

Solución general es:

$$x = 8 - 26s + 3r, \quad y = -4 + 13s - r, \quad z = 1 - 3s, \quad \text{con } r, s \in \mathbb{Z}$$

o bien

$$S = \{\ (8 - 26s + 3r, -4 + 13s - r, 1 - 3s) \mid r, s \in \mathbb{Z}\}$$

♡

A.2.2. Números Enteros Módulo m

Solución 10.

I) $\overline{3} \in (\mathbb{Z}_{69}, +)$, el orden aditivo de un elemento esta dado por $|\overline{x}| = \frac{n}{(n,x)}$. Veamos el máximo común divisor

$$69 = 3 \cdot 23 + 0; \quad (69, 3) = 3$$

Luego

$$|3| = \frac{69}{(69, 3)} = \frac{69}{3} = 23$$

Por lo tanto, el orden de $\overline{3}$ es 23.

II) $\overline{5} \in (\mathcal{U}(\mathbb{Z}_{31}), \cdot)$ Veamos el subgrupo generador por el elemento

$$< \overline{5} > \ = \ \{\overline{5}, \overline{25}, \overline{1}\}$$

Por lo tanto el orden multiplicativo de $\overline{5}$ es 3

III) $\overline{7} \in (\mathcal{U}(\mathbb{Z}_{29}), \cdot)$

$$< \overline{7} > \ = \ \{\overline{7}, \overline{20}, \overline{24}, \overline{23}, \overline{16}, \overline{25}, \overline{1}\}$$

Por lo tanto el orden de $\overline{7}$ es 7

Solución 11.

$+_8$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

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

♡

Solución 12. Ya que $10 = 2 \cdot 5$, por lo tanto $\mathcal{U}(\mathbb{Z}_{10})$ es un grupo cíclico, luego $|\mathcal{U}(\mathbb{Z}_{10})| = \phi(10) = 4$.

$$\mathcal{U}(\mathbb{Z}_{10}) = \{\overline{a} \in \mathbb{Z}_{10} \quad | \quad (\overline{a}, 10) = 1\} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

Como $\mathcal{U}(\mathbb{Z}_{10})$ es cíclico, las raíces primitivas es lo mismo que los generadores.

$$\phi(\phi(10)) = \phi(4) = \phi(2^2) = 2^2 \cdot \left(1 - \frac{1}{2}\right) = 2^2 \cdot \frac{1}{2} = 2$$

Por lo tanto $\mathcal{U}(\mathbb{Z}_{10})$ tiene dos raíces primitivas. Ahora buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{10})$.

$$< \overline{3} >= \{\overline{3}, \overline{9}, \overline{7}, \overline{1}\}$$

Por otro lado necesitamos determinar los primos relativos con $\phi(10)$, lo cuales son: $1, 3$

Por lo tanto las raíces primitivas de $\mathcal{U}(\mathbb{Z}_{10})$ son, $\overline{3}^1 = \overline{3}, \quad \overline{3}^3 = \overline{7}$. ♡

Solución 13.

I) Veremos el número de generadores de $(\mathbb{Z}_{24}, +)$, para ello $24 = 2^3 \cdot 3$

$$\phi(24) = 2^3 \cdot 3 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2^3 \cdot 3 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

Por lo tanto $(\mathbb{Z}_{24}, +)$ tiene 8 generadores, que van a hacer los primos relativos con 24.

Luego, los generadores de $(\mathbb{Z}_{24}, +)$ son:

$$\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}.$$

II) Veremos el número de generadores de $(\mathbb{Z}_{30}, +)$, para ello $30 = 2 \cdot 3 \cdot 5$

$$\phi(30) = 2 \cdot 3 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 2 \cdot 3 \cdot 5 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

Por lo tanto $(\mathbb{Z}_{30}, +)$ tiene 8 generadores, que van a hacer los primos relativos con 30.

Los generadores de $(\mathbb{Z}_{30}, +)$ son:

$$\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}.$$

III) Veremos el número de generadores de $(\mathbb{Z}_{300}, +)$, para ello $300 = 2^2 \cdot 3 \cdot 5^2$

$$\phi(300) = 2^3 \cdot 3 \cdot 5^2 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 2^3 \cdot 3 \cdot 5^2 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 80$$

Por lo tanto $(\mathbb{Z}_{300}, +)$ tiene 80 generadores.

IV) Veremos el número de generadores de $(\mathbb{Z}_{890},+)$, para ello $890 = 2\cdot 5\cdot 89$

$$\phi(890) = 2\cdot 5\cdot 89\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{89}\right) = 2^3\cdot 5^3\cdot\frac{1}{2}\cdot\frac{4}{5}\cdot\frac{88}{89} = 352$$

Por lo tanto $(\mathbb{Z}_{890},+)$ tiene 352 generadores.

V) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{11}),\cdot)$, como 11 es primo es cíclico. $\phi(11) = 10$ y $\phi(10) = 4$, luego tiene cuatro generadores

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

Los primos relativos con 10 son $1,3,7,9$, por lo tanto los generadores son

$$\overline{2}^1 = \overline{2},\ \overline{2}^3 = \overline{8},\ \overline{2}^7 = \overline{7},\ \overline{2}^9 = \overline{6}$$

Por lo tanto generadores de $(\mathcal{U}(\mathbb{Z}_{11}),\cdot)$ son $\overline{2},\overline{6},\overline{7},\overline{8}$. ♡

VI) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{12}),\cdot)$, las unidades de $\mathbb{Z}_{12}$, son los primos relativos con el 12.

$$< \overline{5} >= \{\overline{5},\overline{1}\};\quad < \overline{7} >= \{\overline{7},\overline{1}\};\quad < \overline{11} >= \{\overline{11},\overline{1}\}.$$

Por lo tanto $(\mathcal{U}(\mathbb{Z}_{12}),\cdot)$ no tiene generadores.

VII) Veremos los generadores de $(\mathcal{U}(\mathbb{Z}_{18}),\cdot)$, las unidades de $\mathbb{Z}_{18}$, son lo primos relativos con el 18. además $18 = 2\cdot 3^2$ luego es cíclico. $\phi(18) = 6$ y $\phi(6) = 2$, luego tiene dos generadores

$$< \overline{5} >= \{\overline{5},\overline{7},\overline{17},\overline{13},\overline{11},\overline{1}\}$$

Por lo tanto $(\mathcal{U}(\mathbb{Z}_{18}),\cdot)$ tiene dos generadores $\overline{5},\overline{11}$

VIII) $\mathcal{U}(\mathbb{Z}_{25})$, como $25 = 5^2$, luego $\mathcal{U}(\mathbb{Z}_{25})$ es cíclico, y el numero de elementos esta dado por:

$$\phi(25) = \phi\left(5^2\cdot\left(1-\frac{1}{5}\right)\right) = \left(5^2\cdot\frac{4}{5}\right) = 20$$

y estos son

$$\mathcal{U}(\mathbb{Z}_{25}) = \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16},\overline{17},\overline{18},\overline{19},\overline{20},\overline{21},\overline{22},\overline{23},\overline{24}\}$$

El número de generados

$$\phi(20) \;=\; \phi(2^2\cdot 5) = 2^2\cdot 5\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right) = 2^2\cdot 5\cdot\frac{1}{2}\cdot\frac{4}{5} = 8$$

Por lo tanto $\mathbb{Z}_{25}$ tiene 8 raíces primitivas.

Buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{25})$.

$$< \overline{2} > \;=\; \{\overline{2},\overline{4},\overline{8},\overline{16},\overline{7},\overline{14},\overline{3},\overline{6},\overline{12},\overline{24},\overline{23},\overline{21},\overline{17},\overline{9},\overline{18},\overline{11},\overline{22},\overline{19},\overline{13},\overline{1}\}$$

Luego, buscamos los primos relativos con $\phi(25) = 20$ que son: $1,3,7,9,11,13,17,19$.

Por lo tanto las raíces primitivas módulo 25 son:

$$\overline{2}^1 = \overline{2},\quad \overline{2}^3 = \overline{8},\quad \overline{2}^7 = \overline{3},\quad \overline{2}^9 = \overline{12},\quad \overline{2}^{11} = \overline{23},\quad \overline{2}^{13} = \overline{17},\quad \overline{2}^{17} = \overline{22},\quad \overline{2}^{19} = \overline{13}$$

IX) $\mathcal{U}(\mathbb{Z}_{43})$, como 43 es primo entonces $\mathcal{U}(\mathbb{Z}_{43})$ es cíclico.

$$\begin{aligned}\mathcal{U}(\mathbb{Z}_{43}) &= \{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16},\overline{17},\overline{18},\overline{19},\overline{20},\overline{21},\overline{22},\overline{23},\\ &\quad \cdots,\overline{24},\overline{25},\overline{26},\overline{27},\overline{28},\overline{29},\overline{30},\overline{31},\overline{32},\overline{33},\overline{34},\overline{35},\overline{36},\overline{37},\overline{38},\overline{39},\overline{40},\overline{41},\overline{42}\}\end{aligned}$$

Veremos la cantidad de generadores, ara ello calculemos $\phi(43) = 42 = 2 \cdot 3 \cdot 7$

$$\phi(\phi(43)) = 2 \cdot 3 \cdot 7 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) = 12$$

Por lo tanto $\mathbb{Z}_{43}$ tiene 12 raíces primitivas. Buscamos el primer generador de $\mathcal{U}(\mathbb{Z}_{43})$.

$$\begin{aligned}<\overline{2}> &= \{\overline{2},\overline{4},\overline{8},\overline{16},\overline{32},\overline{21},\overline{42},\overline{41},\overline{39},\overline{35},\overline{27},\overline{11},\overline{22},\overline{1}\}\\ <\overline{3}> &= \{\overline{3},\overline{9},\overline{27},\overline{38},\overline{28},\overline{41},\overline{37},\overline{25},\overline{32},\overline{10},\overline{30},\overline{4},\overline{12},\overline{36},\overline{22},\overline{23},\overline{26},\overline{35},\overline{19},\overline{14},\overline{42},\overline{40},\overline{34},\\ &\quad \overline{16},\overline{5},\overline{15},\overline{2},\overline{6},\overline{18},\overline{11},\overline{33},\overline{13},\overline{39},\overline{31},\overline{7},\overline{21},\overline{20},\overline{17},\overline{8},\overline{24},\overline{29},\overline{1}\}\end{aligned}$$

Luego, buscamos los primos relativos con $\phi(43) = 42$ que son: $1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$.

Por lo tanto las raíces primitivas módulo 43 son:

$$\begin{gathered}\overline{3}^1 = \overline{3}, \quad \overline{3}^5 = \overline{28}, \quad \overline{3}^{11} = \overline{30}, \quad \overline{3}^{13} = \overline{12}, \quad \overline{3}^{17} = \overline{26}, \quad \overline{3}^{19} = \overline{19},\\ \overline{3}^{23} = \overline{34}, \quad \overline{3}^{25} = \overline{5}, \quad \overline{3}^{29} = \overline{18}, \quad \overline{3}^{31} = \overline{33}, \quad \overline{3}^{37} = \overline{20}, \quad \overline{3}^{41} = \overline{29}\end{gathered}$$

♡

Solución 14.

I) $\mathcal{C}_{13} = \{\overline{x}^3 \mid \overline{x} \in \mathcal{U}(\mathbb{Z}_{13})\}$. Como 13 es primo luego $\mathcal{U}(\mathbb{Z}_{13})$ es cíclico, además $13 \equiv 1(\texttt{mod } 3)$, luego $|\mathcal{C}_{13}| = \frac{13-1}{3} = 4$, $\phi(4) = 2$ por lo tanto tiene dos generadores

$$\mathcal{C}_{13} = \{\overline{1},\overline{8},\overline{12},\overline{5}\}$$

Veremos los generados

$$<\overline{8}> = \{\overline{8},\overline{12},\overline{5},\overline{1}\}; \quad <\overline{12}> = \{\overline{12},\overline{1}\}; \quad <\overline{5}> = \{\overline{5},\overline{12},\overline{8},\overline{1}\}.$$

Por lo tanto los generadores de $\mathcal{C}_{13}$ son $\overline{8}, \overline{5}$

orden	subgrupo
1	$<\overline{1}>$
2	$<\overline{12}>$
4	$<\overline{8}>, <\overline{5}>$

II) $\mathcal{C}_{31} = \{\overline{x}^3 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{31})\}$. Como 31 es primo luego $\mathcal{U}(\mathbb{Z}_{31})$ es cíclico, además $31 \equiv 1(\texttt{mod } 3)$, luego $|\mathcal{C}_{31}| = \frac{31-1}{3} = 10$,$\phi(10) = 4$ por lo tanto tiene cuatro generadores

$$\mathcal{C}_{31} = \{\overline{1}, \overline{8}, \overline{27}, \overline{2}, \overline{30}, \overline{16}, \overline{29}, \overline{23}, \overline{4}, \overline{15}\}$$

Veremos los generados

$$\begin{aligned} <\overline{8}> &= \{\overline{8}, \overline{2}, \overline{16}, \overline{4}, \overline{1}\}; & <\overline{27}> &= \{\overline{27}, \overline{16}, \overline{29}, \overline{8}, \overline{30}, \overline{4}, \overline{15}, \overline{2}, \overline{23}, \overline{1}\};\\ <\overline{2}> &= \{\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{1}\}; & <\overline{23}> &= \{\overline{23}, \overline{2}, \overline{15}, \overline{9}, \overline{30}, \overline{8}, \overline{29}, \overline{16}, \overline{27}, \overline{1}\};\\ <\overline{16}> &= \{\overline{16}, \overline{8}, \overline{4}, \overline{2}, \overline{1}\}; & <\overline{29}> &= \{\overline{29}, \overline{4}, \overline{23}, \overline{16}, \overline{30}, \overline{2}, \overline{27}, \overline{8}, \overline{15}, \overline{1}\};\\ <\overline{4}> &= \{\overline{4}, \overline{16}, \overline{2}, \overline{8}, \overline{1}\}; & <\overline{15}> &= \{\overline{15}, \overline{8}, \overline{27}, \overline{2}, \overline{30}, \overline{16}, \overline{23}, \overline{4}, \overline{29}, \overline{1}\};\\ <\overline{30}> &= \{\overline{30}, \overline{1}\}; & <\overline{1}> &= \{\overline{1}\}. \end{aligned}$$

Por lo tanto los generadores de $\mathcal{C}_{31}$ son $\overline{15}, \overline{23}, \overline{27}, \overline{29}$

orden	subgrupo
1	$<\overline{1}>$
2	$<\overline{30}>$
5	$<\overline{2}>, <\overline{4}>, <\overline{8}>, <\overline{16}>$
10	$<\overline{15}>, <\overline{23}>, <\overline{27}>, <\overline{29}>$

♡

Solución 15.

$\mathcal{H} \leq \mathcal{G} = (\mathbb{Z}_{16}, +) \Leftrightarrow |\mathcal{H}|\ |16$ luego $|\mathcal{H}| \in \{1, 2, 4, 8, 16\}$, además existe sólo un subgrupo de orden un divisor de 16 y es cíclico.

$$\mathbb{Z}_{16} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}\}$$

El orden de $\overline{2}$ es $16/(16, 2) = 8$, el orden $\overline{4}$ es $16/(16, 4) = 4$ y el orden $\overline{8}$ es $16/(16, 8) = 2$ Resumiendo tenemos

orden	subgrupo
1	$<\overline{0}>$
2	$<\overline{8}>$
4	$<\overline{4}>, <\overline{12}>$
8	$<\overline{2}>, <\overline{6}>, <\overline{10}>, <\overline{14}>$
16	$<\overline{1}>, <\overline{3}>, <\overline{5}>, <\overline{7}>, <\overline{9}>, <\overline{13}>, <\overline{15}>$

$$<\overline{0}> \subset <\overline{8}> \subset <\overline{4}> \subset <\overline{2}> \subset <\overline{1}>$$

Reticulado:

$$<\overline{0}> \to <\overline{8}> \to <\overline{4}> \to <\overline{2}> \to <\overline{1}>$$

Solución 16.

$\mathcal{H} \leq \mathcal{G}$, luego $|\mathcal{H}|$ $|12$ es decir $|\mathcal{H}| \in \{1, 2, 3, 4, 6, 12\}$. además existe un solo subgrupo de orden un divisor de 12 y es cíclico.

$$\mathcal{G} = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, e\}$$

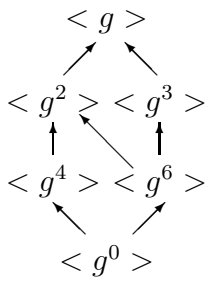
Calculemos directamente los subgrupos

$$\begin{aligned}
< g > &= \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, e\} \\
< g^2 > &= \{g^2, g^4, g^6, g^8, g^{10}, e\} \\
< g^3 > &= \{g^3, g^6, g^9, e\} \\
< g^4 > &= \{g^4, g^8, e\} \\
< g^5 > &= \{g^5, g^{10}, g^3, g^8, g, g^6, g^{11}, g^4, g^9, g^2, g^7, e\} \\
< g^6 > &= \{g^6, e\} \\
< g^7 > &= \{g^7, g^2, g^9, g^4, g^{11}, g^6, g, g^8, g^3, g^{10}, g^5, e\} \\
< g^8 > &= \{g^8, g^4, e\} \\
< g^9 > &= \{g^9, g^6, g^3, e\} \\
< g^{10} > &= \{g^{10}, g^8, g^6, g^4, g^2, e\} \\
< g^{11} > &= \{g^{11}, g^{10}, g^9, g^8, g^7, g^6, g^5, g^4, g^3, g^2, g^1, e\} \\
< e > &= \{e\}
\end{aligned}$$

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

$$\begin{aligned}
< e > \ \subset \ < g^6 > \ \subset \ < g^3 > \ \subset \ < g > \\
< e > \ \subset \ < g^4 > \ \subset \ < g^2 > \ \subset \ < g > \\
< e > \ \subset \ < g^6 > \ \subset \ < g^2 > \ \subset \ < g >
\end{aligned}$$

Reticulado:



♡

Solución: 17 Ya que 23 es un número primo entonces el grupo es cíclico.

$\mathcal{U}(\mathbb{Z}_{23}) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}, \overline{20}, \overline{21}, \overline{22}\}$

$$\begin{aligned}
<\overline{1}> &= \{\overline{1}\} \\
<\overline{2}> &= \{\overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{9}, \overline{18}, \overline{13}, \overline{3}, \overline{6}, \overline{12}, \overline{1}\} \\
<\overline{3}> &= \{\overline{3}, \overline{9}, \overline{4}, \overline{12}, \overline{13}, \overline{16}, \overline{2}, \overline{6}, \overline{18}, \overline{8}, \overline{1}\} \\
<\overline{4}> &= \{\overline{4}, \overline{16}, \overline{18}, \overline{3}, \overline{12}, \overline{2}, \overline{8}, \overline{9}, \overline{13}, \overline{6}, \overline{1}\} \\
<\overline{5}> &= \{\overline{5}, \overline{2}, \overline{10}, \overline{4}, \overline{20}, \overline{8}, \overline{17}, \overline{16}, \overline{11}, \overline{9}, \overline{22}, \overline{18}, \overline{21}, \overline{13}, \overline{19}, \overline{3}, \overline{15}, \overline{6}, \overline{7}, \overline{12}, \overline{14}, \overline{1}\}
\end{aligned}$$

Por lo tanto $\mathcal{U}(\mathbb{Z}_{23}) =< \overline{5} >$, es decir, $(\mathcal{U}(\mathbb{Z}_{23}), \cdot)$ es cíclico y esta generado por $\overline{5}$ es un generador. ♡

Solución: 18

I) 7^{2702} por 31, como $(7, 31) = 1$, luego $7^{\phi(31)} \equiv 1(\texttt{mod } 31)$. Se tiene que $\phi(31) = 30$ y además $2702 = 30 \cdot 90 + 2$

$$7^{2702} \equiv 7^{30\cdot 90+2} \equiv (7^{30})^{90}7^2 \equiv 49 \equiv 18(\texttt{mod } 31)$$

Por lo tanto el resto al dividir 7^{2702} por 31 es 18

II) $2^{100} + 3^{20} + 7^{89}$ por 19, como $(2, 19) = 1$, luego $2^{\phi(19)} \equiv 2^{18} \equiv 1(\texttt{mod } 19)$, además $100 = 18 \cdot 5 + 10$.

$$\begin{aligned}
2^{100} &\equiv 2^{18\cdot 5+10} \equiv (2^{18})^5 2^{10} \equiv 2^{10}(\texttt{mod } 19) \\
&\equiv 2^{2\cdot 5} \equiv (32)^2 \equiv 13^2 \equiv 169 \equiv 17(\texttt{mod } 19)
\end{aligned}$$

De modo similar tenemos que $(3, 19) = 1$, es decir, $3^{18} \equiv 1(\texttt{mod } 19)$, además $20 = 18 \cdot 1 + 2$

$$3^{20} \equiv 3^{18}3^2 \equiv 9(\texttt{mod } 19)$$

También tenemos $(7, 19) = 1$, luego $7^{18} \equiv 1(\texttt{mod } 19)$, además $89 = 18 \cdot 4 + 17$, es decir, necesitamos calcular 7^{17}, para ello veremos

$$<\overline{7}>= \{\overline{7}, \overline{11}, \overline{1}\},$$

de lo cual obtenemos $89 = 3 \cdot 29 + 2$

$$7^{89} \equiv 7^{3\cdot 29+2} \equiv 7^2 \equiv 11(\texttt{mod } 19)$$

Reemplazando los valores obtenidos

$$\begin{aligned}
2^{100} + 3^{20} + 7^{89} &\equiv 17 + 9 + 11(\texttt{mod } 19) \\
2^{100} + 3^{20} + 7^{89} &\equiv 37 \equiv 18(\texttt{mod } 19)
\end{aligned}$$

Por lo tanto el resto al dividir $2^{100} + 3^{20} + 7^{89}$ por 19 es 18.

III) 473^{38} por 5, notemos que $473 \equiv 3(\texttt{mod}\ 5)$, luego

$$473^{38} \equiv 3^{38} \equiv 3^{4\cdot 9+2} \equiv 3^2 \equiv 9 \equiv 4(\texttt{mod}\ 5)$$

Por lo tanto el resto al dividir 473^{38} por 5 es 4

♡

Solución 19. ¿Cuál es el dígito de las unidades en la representación decimal de 3^{400}?
Ya que $(3, 10) = 1$, y

$$\phi(10) = 2 \cdot 5 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 2 \cdot 5 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$$

luego $3^{\phi(10)} \equiv 3^4 \equiv 1(\texttt{mod}\ 10)$

$$3^{400} \equiv (3^4)^{100} \equiv 1(\texttt{mod}\ 10)$$

Por lo tanto, el último dígito de 3^{400} es 1. ♡

Solución 20.

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

Primero verifiquemos que los módulo, son primos dos a dos

$$(3, 7) = 1, \quad (5, 7) = 1, \quad (3, 5) = 1$$

Los coeficientes del teorema Chino de los Restos

$$a_1 = 2, a_2 = 3, a_3 = 2, \quad m_1 = 3, m_2 = 5, m_3 = 7, \quad m = m_1 \cdot m_2 \cdot m_3 = 105,$$

ahora calculemos los coeficientes b_i,

$$\begin{array}{rcl|rcl|rcl} \frac{m}{m_1} \cdot b_1 & \equiv & 1(\texttt{mod}\ m_1) & \frac{m}{m_2} \cdot b_2 & \equiv & 1(\texttt{mod}\ m_2) & \frac{m}{m_3} \cdot b_3 & \equiv & 1(\texttt{mod}\ m_3) \\ 35 \cdot b_1 & \equiv & 1(\texttt{mod}\ 3) & 21 \cdot b_2 & \equiv & 1(\texttt{mod}\ 5) & 15 \cdot b_3 & \equiv & 1(\texttt{mod}\ 7) \\ 2b_1 & \equiv & 1(\texttt{mod}\ 3) & b_2 & \equiv & 1(\texttt{mod}\ 5) & b_3 & \equiv & 3(\texttt{mod}\ 7) \\ 2b_1 & \equiv & 4(\texttt{mod}\ 3) & & & & & & \\ b_1 & \equiv & 2(\texttt{mod}\ 3) & & & & & & \end{array}$$

Luego una solución particular es

$$\begin{array}{rcl} x_0 & = & a_1 \cdot b_1 \cdot \frac{m}{m_1} + a_2 \cdot b_2 \cdot \frac{m}{m_2} + a_3 \cdot b_3 \cdot \frac{m}{m_3} \\ x_0 & = & 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 2331 \end{array}$$

$$x \equiv x_0 \equiv 233 \equiv 23(\texttt{mod}\ 105)$$

El menor entero positivo es 23. ♡

Solución 21.

I) $\square_{17} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{17})\}$

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{17}) &= \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}\} \\ \square_{17} &= \{\overline{1}, \overline{4}, \overline{9}, \overline{16}, \overline{8}, \overline{2}, \overline{15}, \overline{13}\} \end{aligned}$$

$|\square_{17}| = 8$ y $\phi(8) = 4$. Por lo tanto hay 4 generadores de $\square_{17}$. Buscamos el primer generador:

$$\begin{aligned} <\overline{1}> &= \{\overline{1}\} \\ <\overline{4}> &= \{\overline{4}, \overline{16}, \overline{13}, \overline{1}\} \\ <\overline{9}> &= \{\overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}, \overline{1}\} \end{aligned}$$

Ahora necesitamos los primos relativos a 8, que son: $1, 3, 5, 7$.

Generadores del grupo de los $\square_{17}$ son: $\overline{9}^1 = \overline{9}, \quad \overline{9}^3 = \overline{15}, \quad \overline{9}^5 = \overline{8}, \quad \overline{9}^7 = \overline{2}$.

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{9}$	$\overline{13}$	$\overline{15}$	$\overline{16}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{9}$	$\overline{13}$	$\overline{15}$	$\overline{16}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{1}$	$\overline{9}$	$\overline{13}$	$\overline{15}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{15}$	$\overline{2}$	$\overline{1}$	$\overline{9}$	$\overline{13}$
$\overline{8}$	$\overline{8}$	$\overline{16}$	$\overline{15}$	$\overline{13}$	$\overline{4}$	$\overline{2}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{13}$	$\overline{15}$	$\overline{16}$	$\overline{8}$
$\overline{13}$	$\overline{13}$	$\overline{9}$	$\overline{1}$	$\overline{2}$	$\overline{15}$	$\overline{16}$	$\overline{8}$	$\overline{4}$
$\overline{15}$	$\overline{15}$	$\overline{13}$	$\overline{9}$	$\overline{1}$	$\overline{16}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{16}$	$\overline{16}$	$\overline{15}$	$\overline{13}$	$\overline{9}$	$\overline{8}$	$\overline{4}$	$\overline{2}$	$\overline{13}$

II) Ya que $22 = 2 \cdot 11$ se tiene que $\mathcal{U}(\mathbb{Z}_{22})$ es cíclico, luego $\square_{22} = \{\overline{x}^2 \quad | \quad \overline{x} \in \mathcal{U}(\mathbb{Z}_{22})\}$ es cíclico.

$$\begin{aligned} \mathcal{U}(\mathbb{Z}_{22}) &= \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{21}\} \\ \square_{22} &= \{\overline{1}, \overline{9}, \overline{3}, \overline{5}, \overline{15}\} \end{aligned}$$

$|\square_{22}| = 5$ y $\phi(5) = 4$. Por lo tanto hay 4 generadores de $\square_{22}$, es decir son todo salvo el neutro.

Generadores del grupo de los $\square_{22}$ son $\overline{3}, \overline{5}, \overline{9}, \overline{15}$, y la tabla de multiplicar

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{15}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{15}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{15}$	$\overline{5}$	$\overline{1}$
$\overline{5}$	$\overline{5}$	$\overline{15}$	$\overline{3}$	$\overline{1}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{5}$	$\overline{1}$	$\overline{15}$	$\overline{3}$
$\overline{15}$	$\overline{15}$	$\overline{1}$	$\overline{9}$	$\overline{3}$	$\overline{5}$

♡

Solución 22. Determine el número de soluciones en cada caso

i) $x^2 \equiv 5(\texttt{mod } 73)$

$$\begin{aligned}\left(\frac{5}{73}\right)\cdot\left(\frac{73}{5}\right) &= (-1)^{\frac{73-1}{2}\cdot\frac{5-1}{2}}; \quad 73 \equiv 3(\texttt{mod } 5)\\ \left(\frac{5}{73}\right)\cdot\left(\frac{3}{5}\right) &= 1\end{aligned}$$

Pero,

$$\begin{aligned}\left(\frac{3}{5}\right)\cdot\left(\frac{5}{3}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}}; \quad 5 \equiv 2(\texttt{mod } 3)\\ \left(\frac{3}{5}\right)\cdot\left(\frac{2}{3}\right) &= 1\end{aligned}$$

Además

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

Por lo tanto, $\left(\frac{3}{5}\right) = -1$, luego $\left(\frac{5}{73}\right) = -1$, de lo cual obtenemos $5 \notin \square_{73}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 73)$ no tiene solución.

ii) $x^2 \equiv 226(\texttt{mod } 563)$, sabemos que $226 = 2 \cdot 113$, donde 2 y 113 son primos

$$\begin{aligned}\left(\frac{226}{563}\right) &= \left(\frac{2}{563}\right)\cdot\left(\frac{113}{563}\right)\\ &= (-1)^{\frac{563^2-1}{8}}\cdot(-1)^{\frac{563-1}{2}\cdot\frac{113-1}{2}}\cdot\left(\frac{563}{113}\right); \quad 563 \equiv 111(\texttt{mod } 113)\\ &= (-1)(1)\left(\frac{111}{113}\right)\\ &= (-1)(-1)^{\frac{113-1}{2}\cdot\frac{111-1}{2}}\left(\frac{113}{111}\right); \quad 113 \equiv 2(\texttt{mod } 111)\\ &= (-1)\left(\frac{2}{111}\right)\\ &= (-1)(-1)^{\frac{111^2-1}{8}} = -1\end{aligned}$$

De lo cual obtenemos

$$\left(\frac{226}{563}\right) = -1$$

Por lo tanto $226 \notin \square_{563}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 73)$ no tiene solución.

III) $x^3 \equiv 8(\texttt{mod } 719)$, notemos que 719 es un número primo

$$\begin{aligned} x^3 &\equiv 8(\texttt{mod } 719) \\ x^3 - 8 &\equiv 0(\texttt{mod } 719) \\ x^3 - 2^3 &\equiv 0(\texttt{mod } 719) \\ (x-2)\cdot(x^2+2x+4) &\equiv 0(\texttt{mod } 719) \end{aligned}$$

Luego $x - 2 \equiv 0(\texttt{mod } 719)$ o $x^2 + 2x + 4 \equiv 0(\texttt{mod } 719)$.

de la primera ecuación obtenemos

$$x - 2 \equiv 0(\texttt{mod } 719) \Longleftrightarrow x \equiv 2(\texttt{mod } 719)$$

Para la otro ecuación $x^2 + 2x + 4 \equiv 0(\texttt{mod } 719)$, debemos calcular su discriminante

$$\Delta = 2^2 - 4 \cdot 1 \cdot 4 = 4 - 16 = -12 = -1 \cdot 2^2 \cdot 3$$

Ahora veremos si el discriminante es un cuadrado, para ello veremos los factores

$$\left(\frac{-1}{719}\right) = (-1)^{\frac{719-1}{2}} = -1$$

También tenemos

$$\left(\frac{2^2}{719}\right) = 1$$

Nos falta ver el último factor

$$\begin{aligned} \left(\frac{3}{719}\right) &= (-1)^{\frac{719-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{719}{3}\right); \quad 719 \equiv 2(\texttt{mod } 3) \\ \left(\frac{3}{719}\right) &= -1 \cdot \left(\frac{2}{3}\right) = (-1)\cdot(-1)^{\frac{3^2-1}{8}} = 1 \end{aligned}$$

Luego $\left(\frac{3}{719}\right) = 1$

$$\left(\frac{-12}{719}\right) = \left(\frac{-1}{719}\right)\cdot\left(\frac{2^2}{719}\right)\cdot\left(\frac{3}{719}\right) = -1\cdot 1\cdot 1 = -1$$

Por lo tanto $-12 \notin \square_{719}$, es decir, la ecuación $x^2 + 2x + 4 \equiv 0(\texttt{mod } 719)$ no tiene solución.

De lo cual, se obtiene que $x^3 \equiv 8(\texttt{mod } 719)$ tiene exactamente una solución.

IV) $x^2 \equiv 150(\texttt{mod } 1009)$, notemos que 1009 es primo,y que $150 = 2 \cdot 3 \cdot 5^2$ analizaremos los factores

$$\begin{aligned}\left(\frac{150}{1009}\right) &= \left(\frac{2}{1009}\right)\cdot\left(\frac{3}{1009}\right)\cdot\left(\frac{5^2}{1009}\right)\\ &= (-1)^{\frac{1009^2-1}{8}}\cdot(-1)^{\frac{1009-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{1009}{3}\right)\cdot(1)\\ &= \left(\frac{1}{3}\right)=1\end{aligned}$$

Por lo tanto $150\in\square_{1009}$, es decir, la ecuación $x^2\equiv 150(\texttt{mod}\ 1009)$ tiene dos soluciones módulo 1009.

v) $x^4\equiv 9(\texttt{mod}\ 4003)$, notemos que 4003 es un número primo.

$$\begin{aligned}x^4 &\equiv 9(\texttt{mod}\ 4003)\\ x^4-9 &\equiv 0(\texttt{mod}\ 4003)\\ (x^2-3)\cdot(x^2+3) &\equiv 0(\texttt{mod}\ 4003)\end{aligned}$$

Luego tenemos que

$$\begin{aligned}(x^2-3)\equiv 0(\texttt{mod}\ 4003) \quad &\vee \quad (x^2+3)\equiv 0(\texttt{mod}\ 4003)\\ x^2\equiv 3(\texttt{mod}\ 4003) \quad &\vee \quad x^2\equiv -3(\texttt{mod}\ 4003)\end{aligned}$$

Debemos determinar si 3 o -3 son cuadrado.

$$\begin{aligned}\left(\frac{3}{4003}\right) &= (-1)^{\frac{4003-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{4003}{3}\right);\quad 4003\equiv 1(\texttt{mod}\ 3)\\ &= -1\cdot\left(\frac{1}{3}\right)=-1\end{aligned}$$

Para el otro valor

$$\left(\frac{-3}{4003}\right)=\left(\frac{-1}{4003}\right)\cdot\left(\frac{3}{4003}\right)=(-1)\cdot(-1)=1$$

Por lo tanto $3\notin\square_{4003}$ y $-3\in\square_{4003}$, es decir, la ecuación $x^4\equiv 9(\texttt{mod}\ 4003)$ tiene dos soluciones.

vi) $x^6\equiv 1(\texttt{mod}\ 19)$

$$\begin{aligned}x^6 &\equiv 1(\texttt{mod}\ 19)\\ x^6-1 &\equiv 0(\texttt{mod}\ 19)\\ (x^3-1)\cdot(x^3+1) &\equiv 0(\texttt{mod}\ 19)\\ (x+1)\cdot(x^2-x+1)\cdot(x-1)\cdot(x^2+x+1) &\equiv 0(\texttt{mod}\ 19)\end{aligned}$$

Debemos resolver los cuatro factores, par los lineales tenemos

$$\begin{aligned} x+1 &\equiv 0(\texttt{mod } 19) & x-1 &\equiv 0(\texttt{mod } 19) \\ x &\equiv -1(\texttt{mod } 19) & x &\equiv 1(\texttt{mod } 19) \\ x &\equiv 18(\texttt{mod } 19) & x &\equiv 1(\texttt{mod } 19) \end{aligned}$$

Ahora las cuadráticas $x^2 - x + 1 \equiv 0(\texttt{mod } 19)$ y su discriminante es

$$\Delta = 1 - 4 = -3 = -1 \cdot 3$$

Determine si es un cuadrado, analizando los factores

$$\begin{aligned} \left(\frac{-3}{19}\right) &= \left(\frac{-1}{19}\right) \cdot \left(\frac{3}{19}\right) \\ &= (-1)^{\frac{19-1}{2}} \cdot (-1)^{\frac{19-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{19}{3}\right); \quad 19 \equiv 1(\texttt{mod } 3) \\ &= (-1) \cdot (-1) \cdot \left(\frac{1}{3}\right) = 1 \end{aligned}$$

Así tenemos que $\left(\frac{-3}{19}\right) = 1$, luego $-3 \in \square_{19}$, es decir, la ecuación $x^2 - x + 1 \equiv 0(\texttt{mod } 19)$ tiene dos soluciones y son distintas a las anteriores

Ahora la cuadrática $x^2 + x + 1 \equiv 0(\texttt{mod } 19)$ tiene el mismo discriminante $\Delta = -3$, por tanto tiene dos soluciones distintas, es fácil notar que las soluciones de una cuadrática son distintas a la de la otra (basta restar las ecuaciones). Por lo tanto $x^6 \equiv 1(\texttt{mod } 19)$ tiene 6 soluciones.

♡

Solución 23.

i) $x^2 \equiv 5(\texttt{mod } 29)$, notemos que 29 es primo

$$\begin{aligned} \left(\frac{5}{29}\right) &= (-1)^{\frac{29-1}{2}\cdot\frac{5-1}{2}} \cdot \left(\frac{29}{5}\right); \quad 29 \equiv 2^2(\texttt{mod } 5) \\ \left(\frac{5}{29}\right) &= 1 \cdot \left(\frac{4}{5}\right) = 1 \end{aligned}$$

Por lo tanto $5 \in \square_{29}$, es decir, la ecuación $x^2 \equiv 5(\texttt{mod } 29)$ tiene dos soluciones.

Determinemos las soluciones

$$\begin{aligned} x^2 &\equiv 5(\texttt{mod } 29); \quad 5 \equiv 121(\texttt{mod } 29) \\ x^2 &\equiv 121(\texttt{mod } 29) \\ x^2 - 121 &\equiv 0(\texttt{mod } 29) \\ x^2 - 11^2 &\equiv 0(\texttt{mod } 29) \\ (x-11)\cdot(x+11) &\equiv 0(\texttt{mod } 29) \end{aligned}$$

Luego tenemos

$$\begin{aligned} x - 11 \equiv 0(\texttt{mod } 29) \qquad & x + 11 \equiv 0(\texttt{mod } 29) \\ x \equiv 11(\texttt{mod } 29) \qquad & x \equiv -11 \equiv 18(\texttt{mod } 29) \end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 5(\texttt{mod } 29)$ son:

$$x \equiv 11(\texttt{mod } 29), \quad x \equiv 18(\texttt{mod } 29)$$

II) $x^2 \equiv 2(\texttt{mod } 97)$, Notemos que 97 es primo.

$$\left(\frac{2}{97}\right) = (-1)^{\frac{97^2-1}{8}} = 1$$

Por lo tanto $2 \in \square_{97}$, es decir, la ecuación $x^2 \equiv 2(\texttt{mod } 97)$ tiene dos soluciones.

$$\begin{aligned} x^2 &\equiv 2(\texttt{mod } 97); \quad 2 \equiv 196(\texttt{mod } 97) \\ x^2 &\equiv 196(\texttt{mod } 97) \\ x^2 - 196 &\equiv 0(\texttt{mod } 97) \\ x^2 - 14^2 &\equiv 0(\texttt{mod } 97) \\ (x - 14) \cdot (x + 14) &\equiv 0(\texttt{mod } 97) \end{aligned}$$

De lo cual,

$$\begin{aligned} x - 14 \equiv 0(\texttt{mod } 97) \qquad & x + 14 \equiv 0(\texttt{mod } 97) \\ x \equiv 14(\texttt{mod } 97) \qquad & x \equiv -14 \equiv 83(\texttt{mod } 97) \end{aligned}$$

Por lo tanto las soluciones de $x^2 \equiv 2(\texttt{mod } 397)$ son:

$$x \equiv 14(\texttt{mod } 97), \quad x \equiv 83(\texttt{mod } 97)$$

III) $x^{954} + 2x - 1 \equiv 0(\texttt{mod } 953)$. Notemos que 953 es un primo y que cero no es solución.

$$\begin{aligned} x^{953} &\equiv x(\texttt{mod } 953) \quad / \cdot x \\ x^{954} &\equiv x^2(\texttt{mod } 953) \\ x^2 + 2x - 1 &\equiv 0(\texttt{mod } 953) \end{aligned}$$

El discriminante es

$$\Delta = 2^2 - 4 \cdot 1 \cdot -1 = 4 + 4 = 8 = 2^2 \cdot 2$$

Falta determinar si 2 es un cuadrado

$$\left(\frac{8}{953}\right) = \left(\frac{2^2}{953}\right) \cdot \left(\frac{2}{953}\right) = 1 \cdot \left(\frac{2}{953}\right) = (-1)^{\frac{953^2-1}{8}} = 1$$

Por lo tanto $8 \in \square_{953}$, es decir, la ecuación $x^{953} + 2x - 1 \equiv 0(\texttt{mod}\ 953)$ tiene dos soluciones.

Para determinar las soluciones sea $z = 2ax + b = 2x + 2$, luego

$$\begin{aligned} z^2 &\equiv \Delta(\texttt{mod}\ 953) \\ z^2 &\equiv 8(\texttt{mod}\ 953) \quad 8 \equiv 961(\texttt{mod}\ 953) \\ z^2 &\equiv 961(\texttt{mod}\ 953) \\ z^2 - 961 &\equiv 0(\texttt{mod}\ 953) \\ z^2 - 31^2 &\equiv 0(\texttt{mod}\ 953) \\ (z-31)\cdot(z+31) &\equiv 0(\texttt{mod}\ 953) \end{aligned}$$

De lo cual obtenemos,

$$\begin{aligned} z - 31 &\equiv 0(\texttt{mod}\ 953) & z + 31 &\equiv 0(\texttt{mod}\ 953) \\ z &\equiv 31(\texttt{mod}\ 953) & z &\equiv -31(\texttt{mod}\ 953) \\ 2\cdot x + 2 &\equiv 31(\texttt{mod}\ 953) & 2\cdot x + 2 &\equiv -31(\texttt{mod}\ 953) \\ 2\cdot x &\equiv 29(\texttt{mod}\ 953) & 2\cdot x &\equiv -33(\texttt{mod}\ 953) \\ 2\cdot x &\equiv 982(\texttt{mod}\ 953) & 2\cdot x &\equiv 920(\texttt{mod}\ 953) \\ x &\equiv 491(\texttt{mod}\ 953) & x &\equiv 460(\texttt{mod}\ 953) \end{aligned}$$

Por lo tanto las soluciones de $x^{954} + 2x - 1 \equiv 0(\texttt{mod}\ 953)$ son:

$$x \equiv 491(\texttt{mod}\ 953), \quad x \equiv 460(\texttt{mod}\ 953)$$

IV) $x^3 \equiv 8(\texttt{mod}\ 31)$, notemos que 31 es primo,

$$\begin{aligned} x^3 &\equiv 8(\texttt{mod}\ 31) \\ x^3 - 8 &\equiv 0(\texttt{mod}\ 31) \\ x^3 - 2^3 &\equiv 0(\texttt{mod}\ 31) \\ (x-2)\cdot(x^2 + 2x + 4) &\equiv 0(\texttt{mod}\ 31) \end{aligned}$$

De lo cual obtenemos

$$(x-2) \equiv 0(\texttt{mod}\ 31) \quad \vee \quad x^2 + 2x + 4 \equiv 0(\texttt{mod}\ 31)$$

De la ecuación lineal obtenemos

$$x - 2 \equiv 0(\texttt{mod}\ 31) \Longleftrightarrow x \equiv 2(\texttt{mod}\ 31)$$

Ahora veremos la ecuación cuadrática $x^2 + 2x + 4 \equiv 0(\texttt{mod}\ 31)$, para ello, calculemos el discriminate

$$\Delta = 2^2 - 4\cdot 1\cdot 4 = 4 - 16 = -12 = -1\cdot 2^2\cdot 3$$

Veremos si es un cuadrado

$$\begin{aligned}\left(\frac{-12}{31}\right) &= \left(\frac{-1}{31}\right)\cdot\left(\frac{2^2}{31}\right)\cdot\left(\frac{3}{31}\right)\\ &= (-1)^{\frac{31-1}{2}}\cdot(1)\cdot(-1)^{\frac{31-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{31}{3}\right);\quad 31\equiv 1(\mathtt{mod}\ 3)\\ &= (-1)(-1)\left(\frac{1}{3}\right)=1\end{aligned}$$

Por lo tanto $-12\in\square_{31}$, es decir, la ecuación $x^2+2x+4\equiv 0(\mathtt{mod}\ 31)$ tiene dos soluciones.

Usando el cambio de Variable $z=2ax+b=2x+2$ Obtenemos

$$\begin{aligned}z^2 &\equiv -12(\mathtt{mod}\ 31) \quad -12\equiv 81(\mathtt{mod}\ 31)\\ z^2 &\equiv 81(\mathtt{mod}\ 31)\\ z^2-81 &\equiv 0(\mathtt{mod}\ 31)\\ (z-9)\cdot(z+9) &\equiv 0(\mathtt{mod}\ 31)\end{aligned}$$

De este modo obtenemos,

$$\begin{aligned}z-9\equiv 0(\mathtt{mod}\ 31) \qquad & z+9\equiv 0(\mathtt{mod}\ 31)\\ 2\cdot x+2\equiv 9(\mathtt{mod}\ 31) \qquad & 2\cdot x+2\equiv -9(\mathtt{mod}\ 31)\\ 2\cdot x\equiv 7(\mathtt{mod}\ 31) \qquad & 2\cdot x\equiv -11(\mathtt{mod}\ 31)\\ 2\cdot x\equiv 38(\mathtt{mod}\ 31) \qquad & 2\cdot x\equiv 20(\mathtt{mod}\ 31)\\ x\equiv 19(\mathtt{mod}\ 31) \qquad & x\equiv 10(\mathtt{mod}\ 31)\end{aligned}$$

Por lo tanto las soluciones de $x^3\equiv 8(\mathtt{mod}\ 31)$ son:

$$x\equiv 2(\mathtt{mod}\ 31),\quad x\equiv 10(\mathtt{mod}\ 31),\quad x\equiv 19(\mathtt{mod}\ 31)$$

v) $x^6+2x^3+3\equiv 0(\mathtt{mod}\ 23)$, realicemos el siguiente cambio de variable

$$\begin{aligned}u &= x^3\\ u^2 &= x^6\\ u^2+2u+3 &\equiv 0(\mathtt{mod}\ 23)\end{aligned}$$

El discriminante de la ecuación cuadrática es

$$\Delta=2^2-4\cdot 3=4-12=-8=-1\cdot 2^2\cdot 2$$

Veremos si los factores son cuadrados

$$\left(\frac{-1}{23}\right)=(-1)^{\frac{23-1}{2}}=-1;\quad \left(\frac{2^2}{23}\right)=1;\quad \left(\frac{2}{23}\right)=(-1)^{\frac{23^2-1}{8}}=1.$$

Por último tenemos

$$\left(\frac{-8}{23}\right) = \left(\frac{-1}{23}\right)\cdot\left(\frac{2^2}{23}\right)\cdot\left(\frac{2}{23}\right) = -1\cdot 1\cdot 1 = -1$$

Por lo tanto, $-8 \notin \square_{23}$, es decir $u^2+2u+3 \equiv 0(\texttt{mod } 23)$ no tiene solución, de lo cual obtenemos $x^6+2x^3+3 \equiv 0(\texttt{mod } 23)$ no tiene solución.

VI) $x^{15}-x^{10}+4x-3 \equiv 0(\texttt{mod } 7)$, como 7 es primo y cero no es solución de la ecuación tenemos que $x^6 \equiv 1(\texttt{mod } 7)$.

De lo cual obtenemos que

$$x^{10} \equiv x^4(\texttt{mod } 7); \quad x^{15} \equiv x^3(\texttt{mod } 7)$$

Luego la ecuación es equivalente a

$$x^3-x^4+4x-3 \equiv 0(\texttt{mod } 7)$$

El desarrollo de este ejercicio será por evaluación,

$$\begin{array}{rcrcrcll}
x & = & 0 & : & 0^3-0^4+4\cdot 0-3 & = & -3=4 \not\equiv 0(\texttt{mod } 7) & \\
x & = & 1 & : & 1^3-1^4+4\cdot 1-3 & = & 1 \not\equiv 0(\texttt{mod } 7) & \\
x & = & 2 & : & 2^3-2^4+4\cdot 2-3 & = & -3=4 \not\equiv 0(\texttt{mod } 7) & \\
x & = & 3 & : & 3^3-3^4+4\cdot 3-3 & = & -45=4 \not\equiv 0(\texttt{mod } 7) & \\
x & = & 4 & : & 4^3-4^4+4\cdot 4-3 & = & -179=3 \not\equiv 0(\texttt{mod } 7) & \\
x & = & 5 & : & 5^3-5^4+4\cdot 5-3 & = & -483 \equiv 0(\texttt{mod } 7) & \checkmark \\
x & = & 6 & : & 6^3-6^4+4\cdot 6-3 & = & -1059=5 \not\equiv 0(\texttt{mod } 7) &
\end{array}$$

Por lo tanto la solución de $x^{15}-x^{10}+4x-3 \equiv 0(\texttt{mod } 7)$ es

$$x \equiv 5(\texttt{mod } 7)$$

VII) $x^8+x^2 \equiv 0(\texttt{mod } 7) \quad 0 \leq x \leq 30$, notemos que $x^7 \equiv x(\texttt{mod } 7)$

$$\begin{array}{rcl}
x^8+x^2 & \equiv & 0(\texttt{mod } 7) \\
x^2+x^2 & \equiv & 0(\texttt{mod } 7) \\
2x^2 & \equiv & 0(\texttt{mod } 7) \\
x^2 & \equiv & 0(\texttt{mod } 7) \\
x & \equiv & 0(\texttt{mod } 7)
\end{array}$$

Por lo tanto $x \in \{0,7,14,21,28\}$

VIII) $x^5-x^3 \equiv 0(\texttt{mod } 43)$, recuerde que 43 es primo

$$\begin{array}{rcl}
x^5-x^3 & \equiv & 0(\texttt{mod } 43) \\
x^3\cdot(x^2-1) & \equiv & 0(\texttt{mod } 43) \\
x^3\cdot(x-1)\cdot(x+1) & \equiv & 0(\texttt{mod } 43)
\end{array}$$

$$\begin{array}{ccc} x^3 \equiv 0(\texttt{mod } 43) & x-1 \equiv 0(\texttt{mod } 43) & x+1 \equiv 0(\texttt{mod } 43) \\ x \equiv 0(\texttt{mod } 43) & x \equiv 1(\texttt{mod } 43) & x \equiv -1(\texttt{mod } 43) \\ x \equiv 0(\texttt{mod } 43) & x \equiv 1(\texttt{mod } 43) & x \equiv 42(\texttt{mod } 43) \end{array}$$

Por lo tanto las soluciones de $x^5 - x^3 \equiv 0(\texttt{mod } 43)$ son:

$$x \equiv 0(\texttt{mod } 43), \quad x \equiv 1(\texttt{mod } 43), \quad x \equiv 42(\texttt{mod } 43)$$

Solución 24. Resolver $\overline{x} + \overline{73} = \overline{68}$ en $\mathbb{Z}_{21}$

$$\begin{array}{rcl} \overline{x} + \overline{73} & = & \overline{68} \\ \overline{x} & = & \overline{68} - \overline{73} \\ \overline{x} & = & -\overline{5}; \quad -5 + 21 = 16 \\ \overline{x} & = & \overline{16} \end{array}$$

♡

Solución 25. Resolver $\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$ en $\mathbb{Z}_7$, recordemos que $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

$$\begin{array}{rcccl} \overline{x} = \overline{0} & : & \overline{2} \cdot \overline{0}^2 + \overline{0} + \overline{6} = \overline{6} \neq \overline{0} & & \\ \overline{x} = \overline{1} & : & \overline{2} \cdot \overline{1}^2 + \overline{1} + \overline{6} = \overline{9} = \overline{2} \neq \overline{0} & & \\ \overline{x} = \overline{2} & : & \overline{2} \cdot \overline{2}^2 + \overline{2} + \overline{6} = \overline{16} = \overline{2} \neq \overline{0} & & \\ \overline{x} = \overline{3} & : & \overline{2} \cdot \overline{3}^2 + \overline{3} + \overline{6} = \overline{27} = \overline{6} \neq \overline{0} & & \\ \overline{x} = \overline{4} & : & \overline{2} \cdot \overline{4}^2 + \overline{4} + \overline{6} = \overline{42} = \overline{0} & & \checkmark \\ \overline{x} = \overline{5} & : & \overline{2} \cdot \overline{5}^2 + \overline{5} + \overline{6} = \overline{61} = \overline{5} \neq \overline{0} & & \\ \overline{x} = \overline{6} & : & \overline{2} \cdot \overline{6}^2 + \overline{6} + \overline{6} = \overline{84} = \overline{0} & & \checkmark \end{array}$$

Por lo tanto todos los $\overline{x} \in \mathbb{Z}_7$ tal que $\overline{2} \cdot \overline{x}^2 + \overline{x} + \overline{6} = \overline{0}$ son $\overline{x} = \overline{4}, \overline{x} = \overline{6}$ ♡

Solución 26. Demostrar que $\forall a, n \in \mathbb{Z}$ tal que a, n son primo relativos con 31 entonces $31|n^{30} - a^{30}$, para ello tenemos que

$$n^{\phi(31)} \equiv 1(\texttt{mod } 31) \quad a^{\phi(31)} \equiv 1(\texttt{mod } 31)$$

Luego

$$n^{30} \equiv 1(\texttt{mod } 31) \quad a^{30} \equiv 1(\texttt{mod } 31)$$

Restando obtenemos

$$n^{30} - a^{30} \equiv 1 - 1 \equiv 0(\texttt{mod } 31)$$

De lo cual obtenemos $31|(n^{30} - a^{30})$ ♡

Solución: 27 Sea p un número primo impar

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

Como $\left(\frac{5}{p}\right) = -1$, luego $\left(\frac{p}{5}\right) = -1$, analicemos los casos

i) $p \equiv 1(\texttt{mod } 5)$, luego
$\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$, lo que es una contradicción

ii) $p \equiv 2(\texttt{mod } 5)$
$\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$

iii) $p \equiv 3(\texttt{mod } 5)$, luego $\left(\frac{p}{5}\right) = \left(\frac{3}{5}\right)$. Calculemos

$$\begin{aligned}\left(\frac{3}{5}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{5}{3}\right); \quad 5 \equiv 2(\texttt{mod } 3)\\ \left(\frac{3}{5}\right) &= 1 \cdot \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} - 1\end{aligned}$$

Por lo tanto $\left(\frac{3}{5}\right) = -1$.

iv) $p \equiv 4(\texttt{mod } 5)$
$\left(\frac{p}{5}\right) = \left(\frac{4}{5}\right) = 1$, lo que es una contradicción

De este modo todos los primos impares p, tal que $\left(\frac{5}{p}\right) = -1$ son

$$p \equiv 2(\texttt{mod } 5) \vee p \equiv 3(\texttt{mod } 5)$$

♡

Solución 28.

i) $\begin{array}{rcl} 3x + 2y & \equiv & 1(\texttt{mod } 7) \\ 2x + 5y & \equiv & 2(\texttt{mod } 7) \end{array}$

Note que 7 es un numero primo, todos lo números salvo los múltiplo de 7 son invertibles. Amplificamos las ecuaciones

$$\begin{array}{rcll} 3x + 2y & \equiv & 1(\texttt{mod } 7) & /\cdot 2 \\ 2x + 5y & \equiv & 2(\texttt{mod } 7) & /\cdot -3 \end{array}$$

$$\begin{array}{rcr} 6x + 4y & \equiv & 1(\texttt{mod } 7) \\ -6x - 15y & \equiv & -6(\texttt{mod } 7) \end{array}$$

Sumando las ecuaciones, se obtiene

$$\begin{aligned} -11y &\equiv -4(\texttt{mod } 7) \\ 3y &\equiv 3(\texttt{mod } 7) \\ y &\equiv 1(\texttt{mod } 7) \end{aligned}$$

Reemplazando en $2x \equiv 2 - 5y(\texttt{mod } 7)$

$$\begin{aligned} 2x &\equiv 2 - 5(\texttt{mod } 7) \\ 2x &\equiv -3 \equiv 4(\texttt{mod } 7) \\ x &\equiv 2(\texttt{mod } 7) \end{aligned}$$

$$S = \{\ (x, y) \mid x \equiv 2(\texttt{mod } 7) \quad y \equiv 1(\texttt{mod } 7)\}$$

II)
$$\begin{array}{rcl} x + 12y & \equiv & 9(\texttt{mod } 13) \\ 3x + 11y & \equiv & 8(\texttt{mod } 13) \end{array}$$

De manera análoga tenemos que 13 es primo.

$$\begin{array}{rcll} x + 12y & \equiv & 9(\texttt{mod } 13) & / \cdot -3 \\ 3x + 11y & \equiv & 8(\texttt{mod } 13) & \end{array}$$

$$\begin{array}{rcl} -3x - 36y & \equiv & -27(\texttt{mod } 13) \\ 3x + 11y & \equiv & 8(\texttt{mod } 13) \end{array}$$

sumando obtenemos

$$\begin{aligned} -25y &\equiv -19(\texttt{mod } 13) \\ y &\equiv 7(\texttt{mod } 13) \end{aligned}$$

Reemplazando en $x \equiv 9 - 12y(\texttt{mod } 13)$

$$\begin{aligned} x &\equiv 9 - 12 \cdot 7(\texttt{mod } 13) \\ x &\equiv -75 \equiv 3(\texttt{mod } 13) \end{aligned}$$

$$S = \{\ (x, y) \mid x \equiv 3(\texttt{mod } 13) \quad y \equiv 7(\texttt{mod } 13)\}$$

III)
$$\begin{array}{rcl} x + y + z & \equiv & 2(\texttt{mod } 7) \\ x + 2y + 3z & \equiv & 3(\texttt{mod } 7) \\ 2x + y + 4z & \equiv & 1(\texttt{mod } 7) \end{array}$$

Despejando obtenemos $x \equiv 3 - 2y - 3z(\texttt{mod } 7)$ y reemplazando en

$$\begin{aligned} 2x + y + 4z &\equiv 1(\texttt{mod } 7) \\ 2 \cdot (3 - 2y - 3z) + y + 4z &\equiv 1(\texttt{mod } 7) \\ -3y &\equiv -5 + 2z(\texttt{mod } 7) \\ 4y &\equiv 2 + 2z(\texttt{mod } 7) \quad / \cdot 2 \\ y &\equiv 4 + 4z(\texttt{mod } 7) \end{aligned}$$

En la ecuación original

$$\begin{aligned} x &\equiv 3-2y-3z(\mathtt{mod}\ 7) \\ x &\equiv 3-2\cdot(4+4z)-3z(\mathtt{mod}\ 7) \\ x &\equiv -5-11z(\mathtt{mod}\ 7) \\ x &\equiv 2+3z(\mathtt{mod}\ 7) \end{aligned}$$

Reemplazando en la primera ecuación

$$\begin{aligned} x+y+z &\equiv 2(\mathtt{mod}\ 7) \\ (2+3z)+(4+4z)+z &\equiv 2(\mathtt{mod}\ 7) \\ z &\equiv 3(\mathtt{mod}\ 7) \end{aligned}$$

Reemplazando el valor de z

$$\begin{aligned} x &\equiv 2+3z(\mathtt{mod}\ 7) & y &\equiv 4+4z(\mathtt{mod}\ 7) \\ x &\equiv 2+3\cdot 3(\mathtt{mod}\ 7) & y &\equiv 4+4\cdot 3(\mathtt{mod}\ 7) \\ x &\equiv 11(\mathtt{mod}\ 7) & y &\equiv 16(\mathtt{mod}\ 7) \\ x &\equiv 4(\mathtt{mod}\ 7) & y &\equiv 2(\mathtt{mod}\ 7) \end{aligned}$$

La solución del sistema es:

$$x\equiv 4(\mathtt{mod}\ 7) \quad \wedge \quad y\equiv 2(\mathtt{mod}\ 7) \quad \wedge \quad z\equiv 3(\mathtt{mod}\ 7)$$

o bien

$$S=\{\ (x,y,z)\mid x\equiv 4(\mathtt{mod}\ 7) \quad y\equiv 2(\mathtt{mod}\ 7) \quad z\equiv 3(\mathtt{mod}\ 7)\}$$

iv)
$$\begin{aligned} x+2y+4z &\equiv 5(\mathtt{mod}\ 13) \\ 5x+y+8z &\equiv 7(\mathtt{mod}\ 13) \\ 6x+8y+7z &\equiv 1(\mathtt{mod}\ 13) \end{aligned}$$

Despejando obtenemos $x\equiv 5-2y-4z(\mathtt{mod}\ 13)$ y reemplazando en

$$\begin{aligned} 5x+y+8z &\equiv 7(\mathtt{mod}\ 13) \\ 5(5-2y-4z)+y+8z &\equiv 7(\mathtt{mod}\ 13) \\ -9y &\equiv -18+12z(\mathtt{mod}\ 13) \\ 4y &\equiv 8+12z(\mathtt{mod}\ 13) \\ y &\equiv 2+3z(\mathtt{mod}\ 13) \end{aligned}$$

En la ecuación original

$$\begin{aligned} x &\equiv 5-2y-4z(\mathtt{mod}\ 13) \\ x &\equiv 5-2\cdot(2+3z)-4z(\mathtt{mod}\ 13) \\ x &\equiv 1+3z(\mathtt{mod}\ 13) \end{aligned}$$

Reemplazando en la tercera ecuación

$$\begin{aligned} 6x+8y+7z &\equiv 1(\texttt{mod } 13) \\ 6\cdot(1+3z)+8\cdot(2+3z)+7z &\equiv 1(\texttt{mod } 13) \\ 10z &\equiv 5(\texttt{mod } 13) \quad /\cdot 4 \\ 40z &\equiv 20(\texttt{mod } 13) \\ z &\equiv 7(\texttt{mod } 13) \end{aligned}$$

Reemplazando el valor de z en

$$\begin{aligned} x &\equiv 1+3z(\texttt{mod } 13) & y &\equiv 2+3z(\texttt{mod } 13) \\ x &\equiv 1+3\cdot 7(\texttt{mod } 13) & y &\equiv 2+3\cdot 7(\texttt{mod } 13) \\ x &\equiv 22(\texttt{mod } 13) & y &\equiv 23(\texttt{mod } 13) \quad 23-13=10 \\ x &\equiv 9(\texttt{mod } 13) & y &\equiv 10(\texttt{mod } 13) \end{aligned}$$

La solución del sistema es:

$$x\equiv 9(\texttt{mod } 13) \quad \wedge \quad y\equiv 10(\texttt{mod } 13) \quad \wedge \quad z\equiv 7(\texttt{mod } 13)$$

o bien

$$S=\{\ (x,y,z)\mid x\equiv 9(\texttt{mod } 13) \quad y\equiv 10(\texttt{mod } 13) \quad z\equiv 7(\texttt{mod } 13)\}$$

v)
$$\begin{array}{|rcl} x &\equiv& 7(\texttt{mod } 9) \\ x &\equiv& 10(\texttt{mod } 4) \\ x &\equiv& 1(\texttt{mod } 7) \end{array}$$

Como $(9,4)=1, \quad (9,7)=1, \quad (4,7)=1$, luego tenemos

$$a_1=7, a_2=10, a_3=1,\ m_1=9, m_2=4, m_3=7,\ m=m_1\cdot m_2\cdot m_3=252$$

calculemos los coeficiente de la solución particular

$$\begin{array}{ccc} \frac{m}{m_1}\cdot b_1\equiv 1(\texttt{mod } m_1) & \frac{m}{m_2}\cdot b_2\equiv 1(\texttt{mod } m_2) & \frac{m}{m_3}\cdot b_3\equiv 1(\texttt{mod } m_3) \\ 28\cdot b_1\equiv 1(\texttt{mod } 9) & 63\cdot b_2\equiv 1(\texttt{mod } 4) & 36\cdot b_3\equiv 1(\texttt{mod } 7) \\ b_1\equiv 1(\texttt{mod } 9) & -1\cdot b_2\equiv 1(\texttt{mod } 4) & b_3\equiv 1(\texttt{mod } 7) \\ & b_2\equiv 3(\texttt{mod } 4) & \end{array}$$

Luego la solución particular

$$\begin{aligned} x_0 &= a_1\cdot b_1\cdot\frac{m}{m_1}+a_2\cdot b_2\cdot\frac{m}{m_2}+a_3\cdot b_3\cdot\frac{m}{m_3} \\ x_0 &= 7\cdot 1\cdot 28+10\cdot 3\cdot 63+1\cdot 1\cdot 36=2122 \end{aligned}$$

y la solución general

$$\begin{aligned} x &\equiv x_0(\texttt{mod } m) \\ x &\equiv 2122\equiv 106(\texttt{mod } 252) \end{aligned}$$

VI) $\begin{array}{rcl} x & \equiv & 1(\mathtt{mod}\ 4) \\ x & \equiv & 0(\mathtt{mod}\ 3) \\ x & \equiv & 5(\mathtt{mod}\ 7) \end{array}$

Como $(3,7)=1, \quad (4,7)=1, \quad (3,4)=1$, luego tenemos

$$a_1=1, a_2=0, a_3=5,\ m_1=4, m_2=3, m_3=7,\ m=m_1\cdot m_2\cdot m_3=84$$

Los coeficiente de para obtener la solución particular

$$\begin{array}{lll} \frac{m}{m_1}\cdot b_1\equiv 1(\mathtt{mod}\ m_1) & \frac{m}{m_2}\cdot b_2\equiv 1(\mathtt{mod}\ m_2) & \frac{m}{m_3}\cdot b_3\equiv 1(\mathtt{mod}\ m_3) \\ 21\cdot b_1\equiv 1(\mathtt{mod}\ 4) & 28\cdot b_2\equiv 1(\mathtt{mod}\ 3) & 12\cdot b_3\equiv 1(\mathtt{mod}\ 7) \\ b_1\equiv 1(\mathtt{mod}\ 4) & b_2\equiv 1(\mathtt{mod}\ 3) & 5\cdot b_3\equiv 15(\mathtt{mod}\ 7) \\ & & b_3\equiv 3(\mathtt{mod}\ 7) \end{array}$$

Luego la solución particular

$$\begin{array}{rcl} x_0 & = & a_1\cdot b_1\cdot\dfrac{m}{m_1}+a_2\cdot b_2\cdot\dfrac{m}{m_2}+a_3\cdot b_3\cdot\dfrac{m}{m_3} \\ x_0 & = & 1\cdot 1\cdot 21+0\cdot 1\cdot 28+5\cdot 3\cdot 12=201 \end{array}$$

y la solución general

$$\begin{array}{rcl} x & \equiv & x_0(\mathtt{mod}\ m) \\ x & \equiv & 201\equiv 33(\mathtt{mod}\ 84) \end{array}$$

VII) $\begin{array}{rcl} 3x & \equiv & 1(\mathtt{mod}\ 5) \\ 4x & \equiv & 6(\mathtt{mod}\ 14) \\ 5x & \equiv & 11(\mathtt{mod}\ 3) \end{array}$

Simplifiquemos

$$\begin{array}{lll} 3x\equiv 1(\mathtt{mod}\ 5) & 2x\equiv 3(\mathtt{mod}\ 7) & 5x\equiv 11(\mathtt{mod}\ 3) \\ 3x\equiv 6(\mathtt{mod}\ 5) & 2x\equiv 10(\mathtt{mod}\ 7) & 2x\equiv 2(\mathtt{mod}\ 3) \\ x\equiv 2(\mathtt{mod}\ 5) & x\equiv 5(\mathtt{mod}\ 7) & x\equiv 1(\mathtt{mod}\ 3) \end{array}$$

Por lo tanto hay que resolver:

$$\begin{array}{rcl} x & \equiv & 2(\mathtt{mod}\ 5) \\ x & \equiv & 5(\mathtt{mod}\ 7) \\ x & \equiv & 1(\mathtt{mod}\ 3) \end{array}$$

Como $(5,14)=1, \quad (3,5)=1, \quad (14,3)=1$, luego tenemos

$$a_1=2, a_2=5, a_3=1,\ m_1=5, m_2=7, m_3=3,\ m=m_1\cdot m_2\cdot m_3=105$$

Los coeficiente de para obtener la solución particular

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

Luego debemos determinar la solución particular

$$\begin{aligned} x_0 &= a_1\cdot b_1\cdot\frac{m}{m_1}+a_2\cdot b_2\cdot\frac{m}{m_2}+a_3\cdot b_3\cdot\frac{m}{m_3} \\ x_0 &= 2\cdot 1\cdot 21+15\cdot 1\cdot 15+1\cdot 2\cdot 35=187 \end{aligned}$$

y la solución general

$$\begin{aligned} x &\equiv x_0(\texttt{mod}\ m) \\ x &\equiv 187\equiv 82(\texttt{mod}\ 105) \end{aligned}$$

VIII) $\begin{array}{rcl} x-y &\equiv& 5(\texttt{mod}\ 47) \\ xy &\equiv& 6(\texttt{mod}\ 47) \end{array}$

Notemos que 47 es un número primo y amplifiquemos por $-y$ la primera ecuación y sumando obtenemos

$$y^2+5y-6\equiv 0(\texttt{mod}\ 47)$$

El discriminante es

$$\Delta = 5^2-4\cdot 1\cdot 6=25-24=1=1^2$$

luego debemos resolver

$$(2y+5)^2\equiv 1^2(\texttt{mod}\ 47)$$

$$\begin{array}{ll} 2y+5\equiv 1(\texttt{mod}\ 47) & 2y+5\equiv -1(\texttt{mod}\ 47) \\ 2y\equiv -4(\texttt{mod}\ 47) & 2y\equiv -6(\texttt{mod}\ 47) \\ y\equiv -2(\texttt{mod}\ 47) & y\equiv -3(\texttt{mod}\ 47) \\ y\equiv 45(\texttt{mod}\ 47) & y\equiv 44(\texttt{mod}\ 47) \end{array}$$

Reemplazando en la ecuación lineal obtenemos que la solución del sistema es

$$(x\equiv 3(\texttt{mod}\ 47)\wedge y\equiv 45(\texttt{mod}\ 47))\vee(x\equiv 2(\texttt{mod}\ 47)\wedge y\equiv 44(\texttt{mod}\ 47))$$

IX) $\begin{array}{rcl} x^2+y^2 &\equiv& 1(\texttt{mod}\ 13) \\ xy &\equiv& 2(\texttt{mod}\ 13) \end{array}$

Eliminemos una variable del sistema

$\begin{array}{rcll} x^2+y^2 &\equiv& 1(\texttt{mod}\ 13) & /\cdot -x^2 \\ xy &\equiv& 2(\texttt{mod}\ 13) & /()^2 \end{array}$

Recuerde que el paso anterior, no es una equivalencia, pero si una implicación

$$\begin{array}{|rcl} -x^4 - x^2y^2 & \equiv & -x^2 (\texttt{mod } 13) \\ x^2y^2 & \equiv & 4 (\texttt{mod } 13) \end{array}$$

Luego

$$x^4 - x^2 + 4 \equiv 0 (\texttt{mod } 13)$$

Cuyo discriminante es

$$\Delta = 1 - 16 = -15 = -2 = (-1) \cdot 2$$

Para determinar si -2 es un cuadrado, veremos

$$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right) = (-1)^{\frac{13-1}{2}} \cdot (-1)^{\frac{13^2-1}{8}} = -1$$

Por lo tanto $-2 \notin \square_{13}$, es decir, $\begin{array}{|rcl} x^2 + y^2 & \equiv & 1 (\texttt{mod } 13) \\ xy & \equiv & 2 (\texttt{mod } 13) \end{array}$ no tiene solución.

♡

Solución 29.

Determinar los $\alpha \in \mathbb{Z}_{41}$ tal que

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

el sistema no tenga solución. Para ello amplificando por x, la primera ecuación obtenemos

$$\begin{array}{|rcl} x^2 - x \cdot y & = & \alpha \cdot x \\ x \cdot y & = & 1 \end{array}$$

Sumando las ecuaciones tenemos

$$x^2 - \alpha \cdot x - 1 = 0$$

El valor del discriminante es

$$\Delta = \alpha^2 + 4 \notin \square_{41} \cup \{0\}$$

Además los cuadrado son

$$\begin{aligned} \square_{41} &= \{\overline{1}, \overline{4}, \overline{9}, \overline{16}, \overline{25}, \overline{36}, \overline{8}, \overline{23}, \overline{40}, \overline{18}, \overline{39}, \overline{21}, \overline{5}, \overline{32}, \overline{20}, \overline{10}, \overline{2}, \overline{37}, \overline{33}, \overline{31}\} \\ &= \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{9}, \overline{10}, \overline{16}, \overline{18}, \overline{20}, \overline{21}, \overline{23}, \overline{25}, \overline{31}, \overline{32}, \overline{33}, \overline{36}, \overline{37}, \overline{39}, \overline{40}\} \end{aligned}$$

Ahora veremos

$$\square_{41} + \overline{4} = \{\overline{5}, \overline{6}, \overline{8}, \overline{9}, \overline{12}, \overline{13}, \overline{14}, \overline{20}, \overline{22}, \overline{24}, \overline{25}, \overline{27}, \overline{29}, \overline{35}, \overline{36}, \overline{37}, \overline{40}, \overline{0}, \overline{2}, \overline{3}\}$$

por intersección tenemos que

$$\alpha^2 \in \{\overline{2}, \overline{8}, \overline{9}, \overline{10}, \overline{18}, \overline{20}, \overline{23}, \overline{25}, \overline{31}, \overline{40}\}$$

Por lo tanto

$$\alpha \in \{\overline{3}, \overline{5}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{15}, \overline{16}, \overline{17}, \overline{20}, \overline{21}, \overline{24}, \overline{25}, \overline{26}, \overline{31}, \overline{32}, \overline{33}, \overline{34}, \overline{36}, \overline{38}\}$$

♡

Solución 30. Sea $p \equiv 3(\texttt{mod}\ 4)$ y supongamos que existen $x, y \in \mathbb{Z}$ tal que $x^2 + y^2 = p$. Note que si uno de ellos es múltiplo de p entonces el otro también, clo cual nos conduce a una contradicción.

$$\begin{aligned}
x^2 + y^2 &= p \\
x^2 + y^2 &\equiv 0(\texttt{mod}\ p) \\
x^2 &\equiv -y^2(\texttt{mod}\ p) \quad y \neq 0 \\
\left(\frac{x}{y}\right)^2 &\equiv -1(\texttt{mod}\ p) \\
\left(\frac{-1}{p}\right) &= 1 \\
(-1)^{\frac{p-1}{2}} &= 1 \\
\frac{p-1}{2} &= 2 \cdot t \quad t \in \mathbb{Z} \\
p - 1 &= 4 \cdot t \\
p &\equiv 1(\texttt{mod}\ 4)
\end{aligned}$$

Pero $p \equiv 3(\texttt{mod}\ 4)$. Por lo tanto no existen $x, y \in \mathbb{Z}$ tal que $x^2 + y^2 = p$ ♡

Solución 31. Sea p primo impar, luego $p \neq 2$, y además $p - 1$ es par, por lo tanto $p - 1 = 2 \cdot k; \quad k \in \mathbb{Z}$.

Sea $\overline{x} \in \mathcal{U}(\mathbb{Z}_p)$ luego existe un único $\overline{x}^{-1} \in \mathcal{U}(\mathbb{Z}_p)$

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = \sum_{\overline{y} \in \mathbb{Z}_p^*} \overline{y}$$

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = \overline{1} + \overline{2} + \cdots + \overline{p-1} = \frac{\overline{p \cdot (p-1)}}{2} = \frac{\overline{2 \cdot k \cdot p}}{2} = \overline{k \cdot p}$$

De lo obtenemos

$$\sum_{\overline{x} \in \mathbb{Z}_p^*} \overline{x}^{-1} = 0(\texttt{mod}\ p)$$

♡

Solución: 32 Veamos unos ejemplos primero

$$\square_3 = \{\overline{1}\}; \qquad \prod_{\overline{x}\in\square_3} \overline{x} = \overline{1}$$
$$\square_5 = \{\overline{1}, \overline{4}\}; \qquad \prod_{\overline{x}\in\square_5} \overline{x} = \overline{1}\cdot\overline{4} = \overline{4}$$
$$\square_7 = \{\overline{1}, \overline{4}, \overline{2}\}; \qquad \prod_{\overline{x}\in\square_7} \overline{x} = \overline{1}\cdot\overline{4}\cdot\overline{2} = \overline{8} = \overline{1}$$

Note que $\square_p$ es un subgrupo multiplicativo y en este producto esta el inverso de cada elemento, además los únicos elementos que son su propio inverso son $\overline{1}, \overline{-1}$ por lo tanto, el resultado depende solamente si $\overline{-1}$ es un cuadrado

Conclusión:

Si $p = 4\cdot t - 1 \quad t \in \mathbb{Z}$ entonces $\prod_{\overline{x}\in\square_p} \overline{x} = \overline{1}$

Si $p = 4\cdot t + 1 \quad t \in \mathbb{Z}$ entonces $\prod_{\overline{x}\in\square_p} \overline{x} = \overline{p-1}$ ♡

Solución 33.

$$\square_2 = \{\overline{1}\}; \qquad \sum_{\overline{x}\in\square_2} \overline{x} = \overline{1}$$
$$\square_3 = \{\overline{1}\}; \qquad \sum_{\overline{x}\in\square_3} \overline{x} = \overline{1}$$
$$\square_5 = \{\overline{1}, \overline{4}\}; \qquad \sum_{\overline{x}\in\square_5} \overline{x} = \overline{1} + \overline{4} = \overline{5} = \overline{0}$$
$$\square_7 = \{\overline{1}, \overline{4}, \overline{2}\}; \qquad \sum_{\overline{x}\in\square_7} \overline{x} = \overline{1} + \overline{4} + \overline{2} = \overline{7} = \overline{0}$$

Sea p un primo mayor que 3, y δ un no cuadrado distinto de -1, luego $\delta\square_p$ es el conjunto de los no cuadrado y recordemos el ejemplo 102

$$0 = \sum_{\overline{x}\in\mathbb{Z}_p^*} \overline{x} = \sum_{\overline{y}\in\square_p} \overline{y} + \sum_{\overline{z}\in\delta\square_p} \overline{z}$$

Simplificando

$$\begin{aligned} 0 &= \sum_{\overline{y}\in\square_p} \overline{y} + \delta \sum_{\overline{y}\in\square_p} \overline{y} \\ 0 &= (1+\delta) \sum_{\overline{y}\in\square_p} \overline{y} \end{aligned}$$

De lo cual obtenemos la siguiente conclusión:

Si $p = 2$ ó 3 entonces $\sum_{\overline{x}\in\square_p} \overline{x} = \overline{1}$

Si $p \neq 2$ y 3 entonces $\sum_{\overline{x}\in\square_p} \overline{x} = \overline{0}$ ♡

Solución: 34 Sean $x, y \in \mathbb{Z}^+$ tales que $(x, y) = 5$, luego $5|x$ y $5|y$

Como $5|x \Leftrightarrow x = 5\cdot q; \quad q \in \mathbb{Z}$ y $5|y \Leftrightarrow y = 5\cdot k; \quad k \in \mathbb{Z}$, con k, q primos relativos.

Además $x + y = 100$, luego reemplazando obtenemos $5(q + k) = 100$ y simplificando obtenemos $q + k = 20$

q	k	x	y	(x, y)	$x + y$	
1	19	5	95	5	100	✓
2	18	10	90	10	100	
3	17	15	85	5	100	✓
4	16	20	80	20	100	
5	15	25	75	25	100	
6	14	30	70	10	100	
7	13	35	65	5	100	✓
8	12	40	60	20	100	
9	11	45	55	5	100	✓
10	10	50	50	50	100	

Por lo tanto hay 8 soluciones que están dadas por:

$$S = \{\ (5, 95), (15, 85), (35, 65), (45, 55), (55, 45), (65, 35), (85, 15), (95, 5)\ \} \subset \mathbb{Z} \times \mathbb{Z}$$

♡

Solución 35.

Sean x, y números impares luego $y = 2 \cdot k + 1; \quad k \in \mathbb{Z}, \quad x = 2 \cdot q + 1; \quad q \in \mathbb{Z}$, reemplazando y simplificando obtenemos

$$\begin{aligned} x^2 + y^2 &= (2 \cdot k + 1)^2 + (2 \cdot q + 1)^2 \\ &= 4 \cdot k^2 + 4 \cdot k + 1 + 4 \cdot q^2 + 4 \cdot q + 1 \\ &= 2 \cdot (2 \cdot k^2 + 2 \cdot k + 2 \cdot q^2 + 2 \cdot q + 1) \\ &= 2 \cdot r; \quad r = 2 \cdot k^2 + 2 \cdot k + 2 \cdot q^2 + 2 \cdot q + 1 \end{aligned}$$

Por lo tanto $x^2 + y^2$ es par.

Ahora supongamos que $4|(x^2+y^2)$ luego $x^2+y^2 = 4 \cdot a$ con $a \in \mathbb{Z}$, volviendo a la identidad anterior tenemos

$$\begin{aligned} x^2 + y^2 &= 4 \cdot a \\ 4 \cdot k^2 + 4 \cdot k + 1 + 4 \cdot q^2 + 4 \cdot q + 1 &= 4 \cdot a \\ 4 \cdot (k^2 + k + q^2 + q - a) &= -2 \end{aligned}$$

Por lo tanto $4|2$, lo que es una contradicción, lo que implica que 4 no divide a $x^2 + y^2$

♡

Solución 36. Sean $a, b \in \mathbb{Z}$ tales que $a^2 = 2 \cdot b^2$, luego $2|a^2$ lo que implica que $2|a$, por tanto a es par. Reemplazando $a = 2k$, obtenemos

$$\begin{aligned} a^2 &= 2 \cdot b^2 \\ (2k)^2 &= 2 \cdot b^2 \\ 4k^2 &= 2b^2 \\ 2k^2 &= b^2 \end{aligned}$$

De igual manera $2|b^2$ por ende $2|b$, lo cual determina que b es par. ♡

Solución 37. Sean $a, b \in \mathbb{Z}$ tales que $(a, 4) = 2, \quad (b, 4) = 2$, luego a divisible por 2 y no por 4, de igual manera b

Por lo anterior tenemos $a = 2 \cdot k_1$ y $b = 2 \cdot k_2$, donde k_1, k_2 son impares es decir,

$$k_1 = 2 \cdot q_1 + 1, \quad k_2 = 2 \cdot q_2 + 1, \quad q_1, q_2 \in \mathbb{Z}$$

Reemplazando tenemos

$$a + b \;=\; 2k_1 + 2k_2 = 2(2q_1 + 1) + 2(2q_2 + 1) = 4(q_1 + q_2 + 1)$$

Por lo tanto $4|a + b$, luego $(a + b, 4) = 4$. ♡

A.2.3. Números Complejos

Solución: 38

I) $\overline{z} + 2z = 4 + i$

Sea $z = a + bi, \quad \overline{z} = a - bi$, luego $\overline{z} + 2z = a - bi + 2a + 2bi$.

Reemplazando se tiene

$$3a + bi \;=\; 4 + i$$

Luego

$$3a = 4; \quad b = 1$$

Por lo tanto $z = \frac{4}{3} + i$

II) $\overline{z} + 5z + 6 = z^2$

Sea $z = a + bi$, con $a, b \in \mathbb{R}$ luego $\overline{z} = a - bi, \quad z^2 = a^2 - b^2 + 2abi$, reemplazando

$$\begin{aligned} \overline{z} + 5z + 6 &= z^2 \\ a - bi + 5a + 5bi + 6 &= a^2 - b^2 + 2abi \end{aligned}$$

de lo cual tenemos

$$\begin{array}{|rcr} 6a + 6 &=& a^2 - b^2 \\ 4b &=& 2ab \end{array}$$

De la segunda ecuación

$$\begin{aligned} 2ab - 4b &= 0 \\ b(2a - 4) &= 0 \end{aligned}$$

luego

$$b = 0 \quad \vee \quad a = 2$$

Si $b = 0$ entonces

$$\begin{aligned} a^2 - b^2 - 6a &= 6 \\ a^2 - 6a - 6 &= 0 \\ a &= \frac{6 \pm \sqrt{36 + 4 \cdot 6}}{2} \\ a &= \frac{6 \pm \sqrt{60}}{2} \\ a &= 3 \pm \sqrt{15} \end{aligned}$$

Si $a = 2$ entonces

$$\begin{aligned} a^2 - b^2 - 6a &= 6 \\ 4 - b^2 - 12 &= 6 \\ b^2 &= -14 \end{aligned}$$

Imposible, ya que b es real. Por lo tanto $z_1 = 3 + \sqrt{15} + 0i, \quad z_2 = 3 - \sqrt{15} + 0i$

III) $z^2 + |z| = 0$

Sea $z = a + bi, \quad z^2 = a^2 + 2abi - b^2, \quad |z| = \sqrt{a^2 + b^2}$

$$\begin{aligned} z^2 + |z| &= 0 \\ a^2 + 2abi - b^2 + \sqrt{a^2 + b^2} &= 0 \\ a^2 - b^2 + \sqrt{a^2 + b^2} + 2abi &= 0 \end{aligned}$$

De lo cual, obtenemos

$$\begin{array}{|rcl} a^2 - b^2 + \sqrt{a^2 + b^2} &=& 0 \\ 2ab &=& 0 \\ \hline \end{array}$$

De la segunda ecuación obtenemos

$$a = 0 \quad \vee \quad b = 0$$

Si $a = 0$

$$\begin{aligned} -b^2 + b &= 0 \\ b \cdot (1 - b) &= 0 \\ b = 0 \quad &\vee \quad b = 1 \end{aligned}$$

Si $b = 0$

$$\begin{aligned} a^2 + a &= 0 \\ a \cdot (1 - a) &= 0 \\ a = 0 \quad &\vee \quad a = -1 \end{aligned}$$

Por lo tanto $z \in \{i, -1, 0\}$

IV) $\left|\frac{z-12}{z-8i}\right| = \frac{5}{3}$

Sea $z = a + bi$

$$\begin{aligned}
\frac{|z-12|}{|z-8i|} &= \frac{5}{3} \\
3 \cdot |z-12| &= 5 \cdot |z-8i| \\
3 \cdot |a+bi-12| &= 5 \cdot |a+bi-8i| \\
3 \cdot |a-12+bi| &= 5 \cdot |a+(b-8)i| \\
3 \cdot \sqrt{(a-12)^2+b^2} &= 5 \cdot \sqrt{a^2+(b-8)^2} \quad /()^2 \\
9 \cdot (a^2-24a+144+b^2) &= 25 \cdot (a^2+b^2-16b+64) \\
9a^2-216a+1296+9b^2 &= 25a^2+25b^2-400b+1600 \\
16a^2+216a+16b^2-400b+304 &= 0 \quad / \div 16 \\
a^2+\frac{27}{2}a+b^2-25b &= -19
\end{aligned}$$

Para determinar cuales son estos puntos, completemos cuadrado

$$\begin{aligned}
\left(a+\frac{27}{4}\right)^2-\left(\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2-\left(\frac{25}{2}\right)^2 &= -19 \\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= -19+\frac{729}{16}+\frac{625}{4} \\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= \frac{2925}{16} \\
\left(a+\frac{27}{4}\right)^2+\left(b-\frac{25}{2}\right)^2 &= \left(\frac{5\cdot\sqrt{117}}{4}\right)^2
\end{aligned}$$

representa una circunferencia en el plano cartesiano. ♡

Solución 39.

I) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

Sean $z_1 = a + bi, \quad z_2 = c + di$

$$\begin{aligned}
\overline{z_1 \cdot z_2} &= \overline{(a+bi)\cdot(c+di)} \\
\overline{z_1 \cdot z_2} &= \overline{ac+adi+bci-bd} \\
\overline{z_1 \cdot z_2} &= \overline{ac-bd+(ad+bc)i} \\
\overline{z_1 \cdot z_2} &= ac-bd-adi-bci \\
\overline{z_1 \cdot z_2} &= (a-bi)\cdot(c-di) \\
\overline{z_1 \cdot z_2} &= \overline{z_1} \cdot \overline{z_2}
\end{aligned}$$

II) $|z_1+z_2|^2+|z_1-z_2|^2=2|z_1|^2+2|z_2|^2$

Sean $z_1=a+bi, \quad z_2=c+di$

$$\begin{aligned}
|z_1+z_2|^2+|z_1-z_2|^2 &= |a+bi+c+di|^2+|a+bi-c-di|^2\\
|z_1+z_2|^2+|z_1-z_2|^2 &= |a+c+(b+d)i|^2+|a-c+(b-d)i|^2\\
|z_1+z_2|^2+|z_1-z_2|^2 &= \sqrt{(a+c)^2+(b+d)^2}^2+\sqrt{(a-c)^2+(b-d)^2}^2\\
|z_1+z_2|^2+|z_1-z_2|^2 &= (a+c)^2+(b+d)^2+(a-c)^2+(b-d)^2\\
|z_1+z_2|^2+|z_1-z_2|^2 &= 2(a^2+b^2)+2(c^2+d^2)\\
|z_1+z_2|^2+|z_1-z_2|^2 &= 2\sqrt{a^2+b^2}^2+2\sqrt{c^2+d^2}^2\\
|z_1+z_2|^2+|z_1-z_2|^2 &= 2|z_1|^2+2|z_2|^2
\end{aligned}$$

♡

Solución 40.

I) $\mathcal{A}=\{z\in\mathbb{C} \quad | \quad 4\leq|z-1|+|z+1|\leq 8\}$

Sea $z=a+bi$

$$\begin{aligned}
|a+bi-1|+|a+bi+1| &\leq 8\\
|a-1+bi|+|a+1+bi| &\leq 8\\
\sqrt{(a-1)^2+b^2}+\sqrt{(a+1)^2+b^2} &\leq 8\\
\sqrt{(a-1)^2+b^2} &\leq 8-\sqrt{(a+1)^2+b^2} \quad /()^2 \qquad (*)\\
a^2-2a+1+b^2 &\leq 64-16\sqrt{(a+1)^2+b^2}+a^2+2a+1+b^2\\
16\sqrt{(a+1)^2+b^2} &\leq 64+4a \quad /\div 4\\
4\sqrt{(a+1)^2+b^2} &\leq 16+a \quad /()^2\\
16a^2+32a+16+16b^2 &\leq 256+32a+a^2\\
15a^2+16b^2 &\leq 240 \quad /\div 240\\
\frac{a^2}{16}+\frac{b^2}{15} &\leq 1
\end{aligned}$$

Tenga presente que falta analizar una restricción $(*)$, luego $0\leq 8-\sqrt{(a+1)^2+b^2}$, es decir $(a+1)^2+b^2\leq 8^2$, es un disco de radio 8 y centro $(-1,0)$, donde la elipse esta contenida en el disco.

veamos la otra condición

$$\begin{aligned}
4 &\leq |a+bi-1|+|a+bi+1|\\
4 &\leq |a-1+bi|+|a+1+bi|\\
4 &\leq \sqrt{(a-1)^2+b^2}+\sqrt{(a+1)^2+b^2}\\
4-\sqrt{(a+1)^2+b^2} &\leq \sqrt{(a-1)^2+b^2} \quad /()^2 \qquad (*)\\
16-8\sqrt{(a+1)^2+b^2}+a^2+2a+1+b^2 &\leq a^2-2a+1+b^2\\
16+4a &\leq 8\sqrt{(a+1)^2+b^2} \quad /\div 2
\end{aligned}$$

$$\begin{aligned} 4+a &\leq 2\sqrt{(a+1)^2+b^2} \quad /()^2 \\ 16+8a+a^2 &\leq 4a^2+8a+4+4b^2 \\ 12 &\leq 3a^2+4b^2 \quad / \div 12 \\ 1 &\leq \frac{a^2}{4}+\frac{b^2}{3} \end{aligned}$$

Falta analizar $(*)$, en este caso ha dos posibilidades, si $4^2 < \sqrt{(a+1)^2+b^2}$, cumple todo los valores y si es interior al disco $4^2 \geq (a+1)^2+b^2$ se tiene que $1 \leq \frac{a^2}{4}+\frac{b^2}{3}$, pero la elipse esta contenida en el disco, luego los valores que obtenemos son los exteriores a la elipse.

De este modo obtenemos.

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C}^2 \quad | \quad 1 \leq \frac{a^2}{4}+\frac{b^2}{3} \quad \wedge \quad \frac{a^2}{16}+\frac{b^2}{15} \leq 1\}$.

II) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad \frac{1}{2} \leq |z| \leq 1\}$

Sea $z = a+bi$

$$\begin{aligned} \frac{1}{2} \leq & \quad |z| \quad \leq 1 \\ \frac{1}{2} \leq & \quad |a+bi| \quad \leq 1 \\ \frac{1}{2} \leq & \quad \sqrt{a^2+b^2} \quad \leq 1 \quad /()^2 \\ \frac{1}{4} \leq & \quad a^2+b^2 \quad \leq 1 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad \frac{1}{4} \leq a^2+b^2 \leq 1\}$.

III) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z-1+i| = 4\}$

Sea $z = a+bi$

$$\begin{aligned} |z-1+i| &= 4 \\ |a+bi-1+i| &= 4 \\ |a-1+(b+1)i| &= 4 \\ \sqrt{(a-1)^2+(b+1)^2} &= 4 \quad /()^2 \\ (a-1)^2+(b+1)^2 &= 4^2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad (a-1)^2+(b+1)^2 = 16\}$, $\mathcal{A}$ es una circunferencia en $\mathbb{R}^2$.

IV) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z-2| = |1-2\overline{z}|\}$

Sea $z = a + bi, \quad \overline{z} = a - bi$

$$\begin{aligned} |z-2| &= |1-2\overline{z}| \\ |a+bi-2| &= |1-2a+2bi| \\ |a-2+bi| &= |1-2a+2bi| \\ \sqrt{(a-2)^2+b^2} &= \sqrt{(1-2a)^2+4b^2} \quad /()^2 \\ a^2-4a+4+b^2 &= 1-4a+4a^2+4b^2 \\ 3 &= 3a^2+3b^2 \quad / \div 3 \\ 1 &= a^2+b^2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad a^2 + b^2 = 1\}$, $\mathcal{A}$ es una circunferencia en $\mathbb{R}^2$.

v) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad Re(\overline{z} - i) = 2\}$

Sea $z = a + bi, \quad \overline{z} = a - bi$

$$\begin{aligned} Re(\overline{z}-i) &= 2 \\ Re(a-bi-i) &= 2 \\ a &= 2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad a = 2\}$, $\mathcal{A}$ es una recta en $\mathbb{R}^2$.

vi) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Im(z) \leq 2\}$

Sea $z = a + bi$

$$\begin{aligned} 0 \leq \quad & Im(z) \quad && \leq 2 \\ 0 \leq \quad & Im(a+bi) \quad && \leq 2 \\ 0 \leq \quad & b \quad && \leq 2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad 0 \leq b \leq 2\}$, $\mathcal{A}$ es la intersección de dos semi planos en $\mathbb{R}^2$.

vii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad 0 \leq Re(z) \leq 2\}$

Sea $z = a + bi$

$$\begin{aligned} 0 \leq \quad & Re(z) \quad && \leq 2 \\ 0 \leq \quad & Re(a+bi) \quad && \leq 2 \\ 0 \leq \quad & a \quad && \leq 2 \end{aligned}$$

Por lo tanto $\mathcal{A} = \{a + bi \in \mathbb{C} \quad | \quad 0 \leq a \leq 2\}$, $\mathcal{A}$ es la intersección de dos semiplanos en $\mathbb{R}^2$.

viii) $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z - 4i| + |z + 4i| = 10\}$

Sea $z = a + bi$

$$\begin{aligned}
|z-4i| + |z+4i| &= 10 \\
|a+bi-4i| + |a+bi+4i| &= 10 \\
\sqrt{a^2+(b-4)^2} + \sqrt{a^2+(b+4)^2} &= 10 \\
\sqrt{a^2+(b-4)^2} &= 10 - \sqrt{a^2+(b+4)^2} \quad /()^2 \qquad (*) \\
a^2+b^2-8b+16 &= 100 - 20\sqrt{a^2+(b+4)^2} + a^2+b^2+8b+16 \\
20\sqrt{a^2+(b+4)^2} &= 100+16b \quad / \div 4 \\
5\sqrt{a^2+(b+4)^2} &= 25+4b \quad /()^2 \\
25a^2+25b^2+200b+400 &= 625+200b+16b^2 \\
25a^2+9b^2 &= 225 \quad / \div 225 \\
\frac{a^2}{9}+\frac{b^2}{25} &= 1
\end{aligned}$$

Tenga presente, que falta analizar una restricción $(*)$, debe ser interior a la circunferencia de radio 1 y centro $(0,-4)$, lo cual esta considerada en la conclusión

Por lo tanto $\mathcal{A} = \{a+bi \in \mathbb{C} \quad | \quad \frac{a^2}{9}+\frac{b^2}{25} = 1\}$, $\mathcal{A}$ es representa una elipse en $\mathbb{R}^2$.

IX) Sean $a, c \in \mathbb{R}, b \in \mathbb{C}$ fijos

$$a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c = 0$$

Sea $z = x+yi, \quad \overline{z} = x-yi, \quad b = d+ei$

$$\begin{aligned}
a \cdot z \cdot \overline{z} + Re(b \cdot \overline{z}) + c &= 0 \\
a \cdot (x+yi) \cdot (x-yi) + Re((d+ei) \cdot (x-yi)) + c &= 0 \\
a \cdot (x^2+y^2) + xd + ye + c &= 0 \quad / \div a \\
x^2+y^2+\frac{xd}{a}+\frac{ye}{a} &= -\frac{c}{a} \\
\left(x+\frac{d}{2a}\right)^2 - \frac{d^2}{4a^2} + \left(y+\frac{e}{2a}\right)^2 - \frac{e^2}{4a^2} &= -\frac{c}{a} \\
\left(x+\frac{d}{2a}\right)^2 + \left(y+\frac{e}{2a}\right)^2 &= -\frac{c}{a} + \frac{1}{4a^2} \cdot \left(d^2+e^2\right) \\
\left(x+\frac{d}{2a}\right)^2 + \left(y+\frac{e}{2a}\right)^2 &= \left(\sqrt{\frac{1}{4a^2} \cdot |b|^2 - \frac{c}{a}}\right)^2
\end{aligned}$$

Condición:

$$\begin{aligned}
\frac{1}{4a^2} \cdot |b|^2 - \frac{c}{a} &\geq 0 \\
|b|^2 &\geq 4ac
\end{aligned}$$

Por lo tanto. Si $|b|^2 > 4ac$ entonces el lugar geométrico es una circunferencia. Si $|b|^2 = 4ac$ entonces el lugar geométrico es un punto. Y en los otros caso es vacío. ♡

Solución 41. Sean $\mathcal{A} = \{z \in \mathbb{C} \quad | \quad |z| = 3\}, \quad \mathcal{B} = \{z \in \mathbb{C} \quad | \quad |z-1| = |z-i|\}$, denotemos $z = a + bi$.

Como $z \in \mathcal{A}$, luego

$$\begin{aligned} |z| &= \sqrt{a^2+b^2} \\ 3 &= \sqrt{a^2+b^2} \quad /()^2 \\ 3^2 &= a^2+b^2 \end{aligned}$$

Además $z \in \mathcal{B}$, luego

$$\begin{aligned} |z-1| &= |z-i| \\ |a+bi-1| &= |a+bi-i| \\ |a-1+bi| &= |a+(b-1)i| \\ \sqrt{(a-1)^2+b^2} &= \sqrt{a^2+(b-1)^2} \quad /()^2 \\ a^2-2a+1+b^2 &= a^2+b^2-2b+1 \\ a &= b \end{aligned}$$

Por lo tanto

$$\begin{aligned} \mathcal{A}\cap\mathcal{B} &= \{a+bi \in \mathbb{C} \quad | \quad a^2+b^2 = 3^2 \wedge a = b\} \\ \mathcal{A}\cap\mathcal{B} &= \{a+bi \in \mathbb{C} \quad | \quad 2b^2 = 3^2 \wedge a = b\} \\ \mathcal{A}\cap\mathcal{B} &= \left\{a+bi \in \mathbb{C} \quad | \quad b = \pm\frac{3}{\sqrt{2}} \wedge a = b\right\} \\ \mathcal{A}\cap\mathcal{B} &= \left\{\frac{3}{\sqrt{2}}+\frac{3}{\sqrt{2}}i, -\frac{3}{\sqrt{2}}-\frac{3}{\sqrt{2}}i\right\} \end{aligned}$$

♡

Solución 42. Sea $|z| = 1$ y $w, z \in \mathbb{C}$, si $z = a+bi, \quad \overline{z} = a-bi, \quad w = c+di$

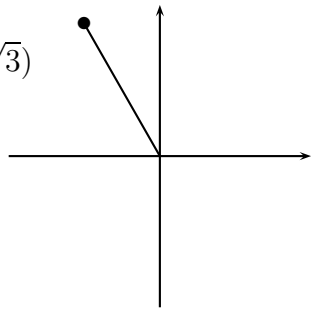
$$\begin{aligned} |\overline{z}w+1| &= |(a-bi)\cdot(c+di)+1| \\ |\overline{z}w+1| &= |ac+adi-cbi+bd+1| \\ |\overline{z}w+1| &= |(ac+bd+1)+(ad-bc)i| \\ |\overline{z}w+1| &= \sqrt{(ac+bd+1)^2+(ad-bc)^2} \\ |\overline{z}w+1| &= \sqrt{a^2c^2+b^2d^2+1+2abcd+2bd+2ac+a^2d^2-2abcd+c^2d^2} \\ |\overline{z}w+1| &= \sqrt{a^2\cdot(c^2+d^2)+b^2\cdot(c^2+d^2)+2ac+2bd+1} \\ |\overline{z}w+1| &= \sqrt{(a^2+b^2)\cdot(c^2+d^2)+2ac+2bd+1}; \quad |z| = 1 \\ |\overline{z}w+1| &= \sqrt{c^2+d^2+2ac+2bd+a^2+b^2} \\ |\overline{z}w+1| &= \sqrt{(a+c)^2+(b+d)^2} \\ |\overline{z}w+1| &= |z+w| \end{aligned}$$

♡

Solución 43. Encontrar el Arg(z)

I) $z = -2 + 2\sqrt{3}i$

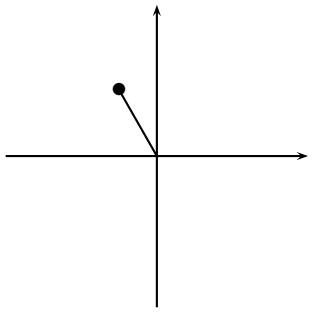
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{2\sqrt{3}}{-2}\right) = \text{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= = -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \end{aligned}$$



II) $z = -\dfrac{2}{1+\sqrt{3}i}$

$$\begin{aligned} z &= -\frac{2}{1+\sqrt{3}i} \cdot \frac{1-\sqrt{3}i}{1-\sqrt{3}i} \\ z &= \frac{-2+2\sqrt{3}i}{1+3} \\ z &= -\frac{1}{2} + \frac{1\sqrt{3}i}{2} \end{aligned}$$

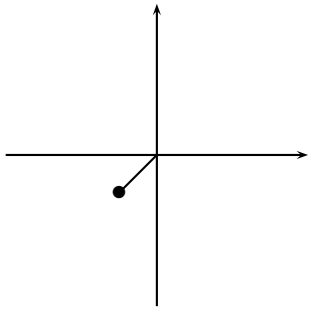
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{\frac{1}{2}\sqrt{3}}{-\frac{1}{2}}\right) = \text{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \end{aligned}$$



Solución 44.

I) $-\sqrt{2} - \sqrt{2}i$

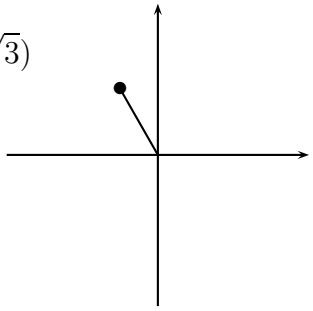
$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{-\sqrt{2}}{-\sqrt{2}}\right) = \text{tg}^{-1}(1) \\ Arg(z) &= 45 \\ Arg(z) &= \frac{\pi}{4} + \pi = \frac{5\pi}{4} \\ |z| &= \sqrt{2+2} = 2 \\ z &= 2 \cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



II) $z = -\dfrac{2}{1+\sqrt{3}i}$

$$\begin{aligned} z &= -\frac{2}{1+\sqrt{3}i}\cdot\frac{1-\sqrt{3}i}{1-\sqrt{3}i} \\ z &= \frac{-2+2\sqrt{3}i}{1+3} \\ z &= -\frac{1}{2}+\frac{1\sqrt{3}i}{2} \end{aligned}$$

$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{\frac{1}{2}\sqrt{3}}{-\frac{1}{2}}\right) = \text{tg}^{-1}(-\sqrt{3}) \\ Arg(z) &= -60 \\ Arg(z) &= -\frac{\pi}{3}+\pi = \frac{2\pi}{3} \\ |z| &= \sqrt{\frac{1}{4}+\frac{3}{4}} = 1 \\ z &= 1\cdot cis\left(\frac{2\pi}{3}\right) \end{aligned}$$

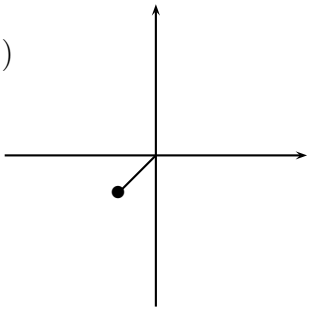


Solución: 45

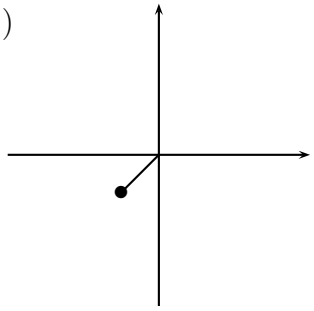
I) $\frac{(-\sqrt{2}-\sqrt{2}i)^{16}}{(-1+i)^4}$

Sean $z_1 = -\sqrt{2}-\sqrt{2}i, \quad z_2 = -1+i$

$$\begin{aligned} Arg(z_1) &= \text{tg}^{-1}\left(\frac{-\sqrt{2}}{-\sqrt{2}}\right) = \text{tg}^{-1}(1) \\ Arg(z_1) &= 45 \\ Arg(z_1) &= \frac{\pi}{4}+\pi = \frac{5\pi}{4} \\ |z_1| &= \sqrt{2+2} = 2 \\ z_1 &= 2\cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



$$\begin{aligned} Arg(z_2) &= \text{tg}^{-1}\left(\frac{1}{-1}\right) = \text{tg}^{-1}(-1) \\ Arg(z_2) &= -45 \\ Arg(z_2) &= -\frac{\pi}{4}+\pi = \frac{3\pi}{4} \\ |z_2| &= \sqrt{2} \\ z_2 &= 2^{\frac{1}{2}}\cdot cis\left(\frac{5\pi}{4}\right) \end{aligned}$$



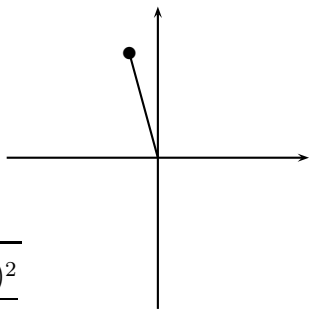
$$\begin{aligned}
\frac{z_1^{16}}{z_2^4} &= \frac{\left(2\cdot cis\left(\frac{5\pi}{4}\right)\right)^{16}}{\left(2^{\frac{1}{2}}\cdot cis\left(\frac{3\pi}{4}\right)\right)^4} = \frac{2^{16}\cdot cis\left(\frac{16\cdot 5\pi}{4}\right)}{2^{\frac{4}{2}}\cdot cis\left(\frac{4\cdot 3\pi}{4}\right)} \\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot cis(20\pi - 3\pi) \\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot(\cos(17\pi) + i\,\mathrm{sen}(17\pi)) \\
\frac{z_1^{16}}{z_2^4} &= 2^{14}\cdot(-1+0i) \\
\frac{z_1^{16}}{z_2^4} &= -2^{14}
\end{aligned}$$

II) $\left(\frac{1+\sqrt{3}i}{1-i}\right)^{40}$

Sea $z = \frac{1+\sqrt{3}i}{1-i}$

$$\begin{aligned}
z &= \frac{1+\sqrt{3}i}{1-i}\cdot\frac{1+i}{1+i} \\
z &= \frac{1+i+\sqrt{3}i-\sqrt{3}}{2} \\
z &= \frac{1-\sqrt{3}}{2} + i\frac{1+\sqrt{3}}{2}
\end{aligned}$$

$$\begin{aligned}
Arg(z) &= \mathrm{tg}^{-1}\left(\frac{\frac{1+\sqrt{3}}{2}}{\frac{1-\sqrt{3}}{2}}\right) \\
Arg(z) &= -75 \\
Arg(z) &= -\frac{5\pi}{12} + \pi = \frac{7\pi}{12} \\
|z| &= \sqrt{\frac{(1-\sqrt{3})^2}{4} + \frac{(1+\sqrt{3})^2}{4}} \\
|z| &= \sqrt{2}
\end{aligned}$$



Luego, se tiene que

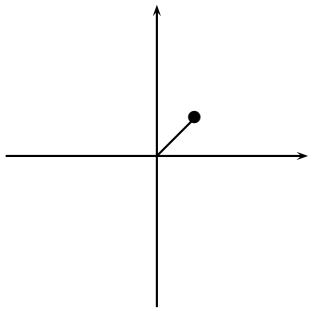
$$z = \left(2^{\frac{1}{2}}\cdot cis\left(\frac{7\pi}{12}\right)\right)$$

$$\begin{aligned} z^{40} &= 2^{\frac{40}{2}} \cdot cis\left(\frac{40 \cdot 7\pi}{12}\right) = 2^{20} \cdot cis\left(\frac{70\pi}{3}\right) \\ z^{40} &= 2^{20} \cdot \left(\cos\left(\frac{70\pi}{3}\right) + \operatorname{sen}\left(\frac{70\pi}{3}\right)\right) \\ z^{40} &= 2^{20} \cdot \left(-\frac{1}{2} - \frac{\sqrt{3}i}{2}\right) \\ z^{40} &= -2^{19} \cdot (1 + \sqrt{3}i) \end{aligned}$$

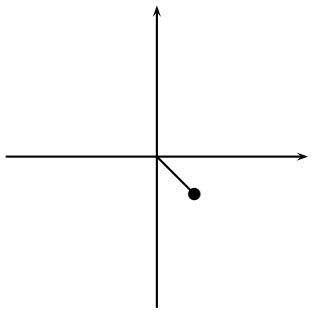
III) $(1+i)^n + (1-i)^n$

Sea $z_1 = 1 + i, \quad z_2 = 1 - i$

$$\begin{aligned} Arg(z_1) &= \operatorname{tg}^{-1}\left(\frac{1}{1}\right) \\ Arg(z_1) &= 45 \\ Arg(z_1) &= \frac{\pi}{4} \\ |z_1| &= \sqrt{1^2 + 1^2} = \sqrt{2} \\ z_1 &= 2^{\frac{1}{2}} \cdot cis\left(\frac{\pi}{4}\right) \end{aligned}$$



$$\begin{aligned} Arg(z_2) &= \operatorname{tg}^{-1}\left(\frac{1}{-1}\right) \\ Arg(z_2) &= -45 \\ Arg(z_2) &= \frac{-\pi}{4} \\ |z_2| &= \sqrt{2} \\ z_2 &= 2^{\frac{1}{2}} \cdot cis\left(\frac{-\pi}{4}\right) \end{aligned}$$



$$\begin{aligned} z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(cis\left(\frac{n\pi}{4}\right) + cis\left(\frac{-n\pi}{4}\right)\right) \\ z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(\cos\left(\frac{n\pi}{4}\right) + i\operatorname{sen}\left(\frac{n\pi}{4}\right) + \cos\left(\frac{-n\pi}{4}\right) + i\left(\frac{-n\pi}{4}\right)\right) \\ \cos(-x) &= \cos(x) \\ \operatorname{sen}(-x) &= -\operatorname{sen}(x) \\ z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot \left(\cos\left(\frac{n\pi}{4}\right) + i\operatorname{sen}\left(\frac{n\pi}{4}\right) + \cos\left(\frac{n\pi}{4}\right) - i\left(\frac{n\pi}{4}\right)\right) \\ z_1^n + z_2^n &= 2^{\frac{n}{2}} \cdot 2 \cdot \cos\left(\frac{n\pi}{4}\right) \end{aligned}$$

Solución 46.

$$\left(\frac{1-z}{z+i}\right)^3 = 1 = cis(0)$$

Las raíces cubica de uno son:

$$cis\left(\frac{2k\pi}{3}\right) \quad k = 0, 1, 2$$

- $k = 0: \quad cis(0) = 1$

$$\begin{aligned} \frac{1-z}{z+i} &= 1 \\ 1-z &= z+i \\ 2z &= 1-i \\ z &= \frac{1}{2} - \frac{1}{2}i \end{aligned}$$

- $k = 1: \quad cis(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$$\begin{aligned} \frac{1-z}{z+i} &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i \quad / \cdot 2(z+i) \\ 2(1-z) &= (z+i) \cdot \left(-1 + \sqrt{3}i\right) \\ 2-2z &= -i - z - \sqrt{3} + z\sqrt{3}i \\ z \cdot (1+\sqrt{3}i) &= 2 + \sqrt{3} + i \\ z &= (2+\sqrt{3}+i) \cdot (1+\sqrt{3}i)^{-1} \\ z &= (2+\sqrt{3}+i) \cdot \left(\frac{1}{4} - \frac{\sqrt{3}}{4}i\right) \\ z &= \frac{1}{2} - \frac{\sqrt{3}}{2}i + \frac{\sqrt{3}}{4} - \frac{3}{4}i + \frac{1}{4}i + \frac{\sqrt{3}}{4} \\ z &= \frac{1}{2} + \frac{\sqrt{3}}{2} - \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right) i \end{aligned}$$

- $k = 2: \quad cis(\frac{4\pi}{3}) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$

$$\begin{aligned} \frac{1-z}{z+i} &= -\frac{1}{2} - \frac{\sqrt{3}}{2}i \quad / \cdot 2(z+i) \\ 2(1-z) &= (z+i) \cdot \left(-1 - \sqrt{3}i\right) \\ 1-z &= -i - z + \sqrt{3} - z\sqrt{3}i \\ z \cdot (1-\sqrt{3}i) &= 2 - \sqrt{3} + i \\ z &= (2-\sqrt{3}+i) \cdot (1-\sqrt{3}i)^{-1} \end{aligned}$$

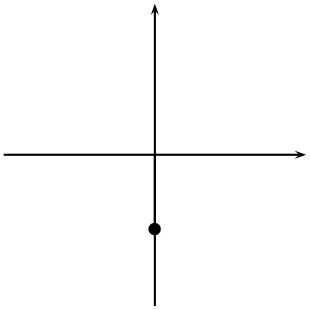
$$\begin{aligned} z &= (2-\sqrt{3}+i)\cdot\left(\frac{1}{4}+\frac{\sqrt{3}}{4}i\right) \\ z &= \frac{1}{2}+\frac{\sqrt{3}}{2}i-\frac{\sqrt{3}}{4}-\frac{3}{4}+\frac{1}{4}i-\frac{\sqrt{3}}{4}i \\ z &= \frac{1}{2}-\frac{\sqrt{3}}{2}-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)i \end{aligned}$$

Por lo tanto $z \in \left\{\frac{1}{2}-\frac{1}{2}i, \quad \frac{1}{2}+\frac{\sqrt{3}}{2}-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)i, \quad \frac{1}{2}-\frac{\sqrt{3}}{2}-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}\right)i\right\}$ ♡

Solución 47.

a) Las raíces cúbicas de $-i$. Si $z=-i$, entonces la forma polar es:

$$\begin{aligned} Arg(z) &= \frac{3\pi}{2} \\ |z| &= \sqrt{1} \\ z &= 1cis\left(\frac{3\pi}{2}\right) \end{aligned}$$



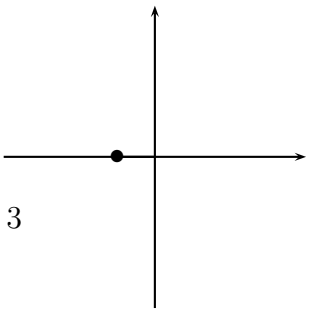
Las raíces cúbicas son

$$z_k = 1\cdot cis\left(\frac{\frac{3\pi}{2}+2k\pi}{3}\right); \quad k=0,1,2$$

- $k=0 \quad 1\cdot cis\left(\frac{\pi}{2}\right)=i$
- $k=1 \quad 1\cdot cis\left(\frac{7\pi}{6}\right)=1\cdot\left(-\frac{\sqrt{3}}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=-\frac{\sqrt{3}}{2}-\frac{1}{2}i$
- $k=2 \quad 1\cdot cis\left(\frac{11\pi}{6}\right)=1\cdot\left(\frac{\sqrt{3}}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=\frac{\sqrt{3}}{2}-\frac{1}{2}i$

b) Las raíces cuárticas de -1. Si $z=-1$, entonces la forma polar:

$$\begin{aligned} Arg(z) &= \pi \\ |z| &= \sqrt{1} \\ z &= 1cis(\pi) \end{aligned}$$



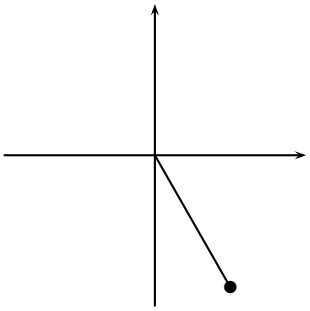
$$z_k = 1\cdot cis\left(\frac{\pi+2k\pi}{4}\right); \quad k=0,1,2,3$$

- $k=0 \quad 1\cdot cis\left(\frac{\pi}{4}\right)=1\cdot\left(\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right)=\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i$
- $k=1 \quad 1\cdot cis\left(\frac{3\pi}{4}\right)=1\cdot\left(-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i\right)=-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i$
- $k=2 \quad 1\cdot cis\left(\frac{5\pi}{4}\right)=1\cdot\left(-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i$

- $k=3 \quad 1\cdot cis\left(\frac{7\pi}{4}\right)=1\cdot\left(\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)=\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i$

c) Las raíces cuadradas de $2-2\sqrt{3}i$, si $z=2-2\sqrt{3}i$, entonces la forma polar

$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{-2\sqrt{3}}{2}\right) \\ Arg(z) &= -60 \\ Arg(z) &= \frac{-\pi}{3}+2\pi=\frac{5\pi}{3} \\ |z| &= \sqrt{4+4\cdot 3}=2 \\ z &= 2cis\left(\frac{5\pi}{3}\right) \end{aligned}$$

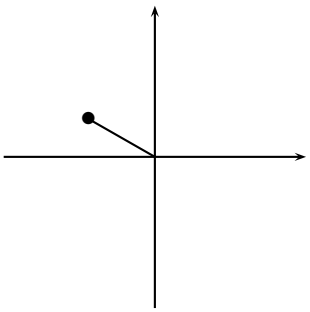


$$z_k=2\cdot cis\left(\frac{\frac{5\pi}{3}+2k\pi}{2}\right);\quad k=0,1$$

- $k=0 \quad 2\cdot cis\left(\frac{5\pi}{6}\right)=2\cdot\left(-\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)=-\sqrt{3}+i$
- $k=1 \quad 2\cdot cis\left(\frac{11\pi}{6}\right)=2\cdot\left(\frac{\sqrt{3}}{2}-\frac{1}{2}i\right)=-\sqrt{3}-i$

d) Las raíces cúbicas de $-\frac{\sqrt{3}}{2}+\frac{1}{2}i$, si $z=-\frac{\sqrt{3}}{2}+\frac{1}{2}i$ entonces la forma polar es:

$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{\frac{1}{2}}{-\frac{\sqrt{3}}{2}}\right) \\ Arg(z) &= -30 \\ Arg(z) &= -\frac{\pi}{6}+\pi=\frac{5\pi}{6} \\ |z| &= \sqrt{\frac{3}{4}+\frac{1}{4}}=1 \\ |z|^{\frac{1}{3}} &= 1cis\left(\frac{5\pi}{6}\right) \end{aligned}$$



Luego

$$z_k=1\cdot cis\left(\frac{\frac{5\pi}{6}+2k\pi}{3}\right);\quad k=0,1,2$$

- $k=0 \quad 1\cdot cis\left(\frac{5\pi}{18}\right)$
- $k=1 \quad 1\cdot cis\left(\frac{17\pi}{18}\right)$
- $k=2 \quad 1\cdot cis\left(\frac{29\pi}{18}\right)$ ♡

Solución 48.

Supongamos que $2+3i$ divide $4+8i$, entonces existen $a, b \in \mathbb{Z}$ tal que:

$$4+8i = (2+3i)\cdot(a+bi)$$

Calculando norma tenemos

$$80 = 13t$$

Lo cual es una contradicción

Por lo tanto $2+3i$ no divide a $4+8i \quad \in \mathbb{Z}[i]$. ♡

Solución: 49 Supongamos que $7+5i$, no es primo, luego existen $z_1 = a_1+b_1i, \quad z_2 = a_2+b_2i$, no invertibles en $\mathbb{Z}[i]$ tales que

$$\begin{aligned} z_1 \cdot z_2 &= 7+5i \quad /\|\ \| \\ \|z_1\| \cdot \|z_2\| &= \|7+5i\| \\ \|z_1\| \cdot \|z_2\| &= 74 \\ \|z_1\| \cdot \|z_2\| &= 2 \cdot 37 \end{aligned}$$

Una posible solución es:

$$\begin{aligned} \|z_1\| = 2 \quad \wedge \quad \|z_2\| &= 37 \\ \|z_1\| &= a_1^2 + b_1^2 = 2 \\ \|z_2\| &= a_2^2 + b_2^2 = 37 \end{aligned}$$

De la cual se obtiene

$$7+5i = (1-i)\cdot(1+6i)$$

Por lo tanto $7+5i$ no es primo en $\mathbb{Z}[i]$

Solución: 50 Supongamos que 7, no es primo, luego existen $z_1 = a_1+b_1i, \quad z_2 = a_2+b_2i$, no invertibles en $\mathbb{Z}[i]$ tales que

$$\begin{aligned} z_1 \cdot z_2 &= 7 \quad /\|\ \| \\ \|z_1\| \cdot \|z_2\| &= \|7\| \\ \|z_1\| \cdot \|z_2\| &= 7^2 \\ \|z_1\| = 7 \quad \wedge \quad \|z_2\| &= 7 \end{aligned}$$

Veremos si es posible que un elemento tenga norma 7, primero notemos que a_1, b_1, no pueden ser múltiplo de 7.

$$\begin{aligned} \|z_1\| = a_1^2 + b_1^2 &= 7 \\ a_1^2 + b_1^2 &\equiv 0 (\texttt{mod } 7) \\ a_1^2 &\equiv -b_1^2 (\texttt{mod } 7) \quad / \cdot b_1^{-2}, b_1 \neq 0 \\ a_1^2 \cdot b_1^{-2} &\equiv -1 (\texttt{mod } 7) \\ (a_1 \cdot b_1^{-1})^2 &\equiv -1 (\texttt{mod } 7) \\ \left(\frac{-1}{7}\right) &= (-1)^{\frac{7-1}{2}} = -1 \end{aligned}$$

Por lo tanto $-1 \not\square_7$, de lo cual se obtiene que 7 es primo en $\mathbb{Z}[i]$. ♡

A.2.4. Polinomios

Solución 51. Si $p(x) = x^4+ax^2+bx+5$, como 1 es raíz de $p(x)$, luego $p(1) = 0$, análogamente $p(-2) = 0$.

$$\begin{aligned} p(1) = 0 \quad &\Leftrightarrow \quad 1 + a + b + 5 = 0 \\ p(-2) = 0 \quad &\Leftrightarrow \quad 16 + 4a - 2b + 5 = 0 \end{aligned}$$

Luego tenemos el sistema

$$\begin{array}{rcl} a+b & = & -6 \\ 4a-2b & = & 21 \end{array}$$

Amplificando por 2 y sumando obtenemos

$$\begin{aligned} 6a &= 9 \\ a &= \frac{9}{6} = \frac{3}{2} \end{aligned}$$

Reemplazando

$$b = -6 - a = -6 - \frac{3}{2} = -\frac{15}{2}$$

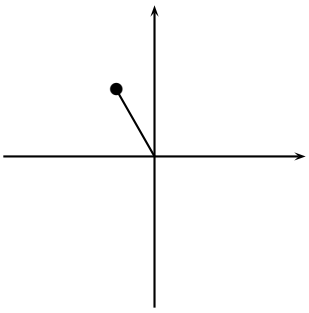
Luego tenemos que $p(x) == x^4 + \frac{3}{2}x^2 - \frac{15}{2}x + 5$. ♡

Solución 52. Determinar todas las raíces de $x^8 + x^4 + 1$. Sea $u = x^4$, luego $u^2 = x^8$ reemplazando obtenemos

$$\begin{aligned} u^2 + u + 1 &= 0 \\ u &= \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{3}i}{2} \\ x^4 &= \frac{-1 \pm \sqrt{3}i}{2} \end{aligned}$$

Sea $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, su forma polar

$$\begin{aligned} Arg(z) &= \text{tg}^{-1}\left(\frac{\frac{\sqrt{3}}{2}}{-\frac{\sqrt{1}}{2}}\right) = -60 \\ Arg(z) &= -\frac{\pi}{3} + \pi = \frac{2\pi}{3} \\ |z| &= \sqrt{\frac{1}{4} + \frac{3}{4}} = 1 \end{aligned}$$



Por lo tanto

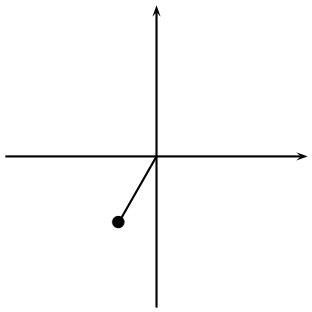
$$z_k = 1 \cdot cis\left(\frac{\frac{2\pi}{3} + 2k\pi}{4}\right); \quad k = 0, 1, 2, 3$$

- $k = 0 \quad z_0 = cis\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{1}{2}i$
- $k = 1 \quad z_1 = cis\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

- $k=2 \quad z_2 = cis\left(\frac{7\pi}{6}\right) = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$
- $k=3 \quad z_3 = cis\left(\frac{5\pi}{3}\right) = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

Ahora sea $w = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, su forma polar

$$\begin{aligned} Arg(w) &= \text{tg}^{-1}\left(\frac{\frac{-\sqrt{3}}{2}}{\frac{-\sqrt{1}}{2}}\right) = 60 \\ Arg(w) &= \frac{\pi}{3} + \pi = \frac{4\pi}{3} \\ |w| &= \sqrt{\frac{1}{4} + \frac{3}{4}} = 1 \end{aligned}$$



Luego

$$w = 1 \cdot cis\left(\frac{\frac{4\pi}{3} + 2k\pi}{4}\right); \quad k = 0, 1, 2, 3$$

- $k=0 \quad z_0 = cis\left(\frac{\pi}{3}\right) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
- $k=1 \quad z_1 = cis\left(\frac{5\pi}{6}\right) = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$
- $k=2 \quad z_2 = cis\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$
- $k=3 \quad z_3 = cis\left(\frac{11\pi}{6}\right) = \frac{\sqrt{3}}{2} - \frac{1}{2}i$

Por lo tanto las raíces de $x^8 + x^4 + 1$ son:

$$\left\{\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \frac{\sqrt{3}}{2} - \frac{1}{2}i, \frac{\sqrt{3}}{2} + \frac{1}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{\sqrt{3}}{2} - \frac{1}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i\right\}$$

♡

Solución 53. Sea $p(x) = 3x^3 + 2x^2 + cx - k$.

$$\begin{array}{|rcl} p(-2) &=& 37 \\ p(1) &=& -2 \\ \hline \end{array}; \qquad \begin{array}{|rcl} -24 + 8 - 2c - k &=& 37 \\ 3 + 2 + c - k &=& -2 \\ \hline \end{array}$$

$$\begin{array}{|rcl} 2c + k &=& -53 \\ c - k &=& -7 \\ \hline \end{array}$$

Sumando obtenemos

$$\begin{aligned} 3c &= -60; \qquad c = -20. \\ k &= c + 7; \qquad k = -20 + 7 = -13. \end{aligned}$$

por lo tanto, Sea $p(x) = 3x^3 + 2x^2 - 20x + 13$. ♡

Solución 54. Sea $p(x) = 2x^3 + bx^2 + cx + d$, tal que

- El resto al dividir $p(x)$ por x es $2+b$, es decir, $p(0) = 2+b$
- El resto al dividir $p(x)$ por $x+1$ es $b+d$, de otro modo, $p(-1) = b+d$
- 1 es raíz de $p(x)$, por lo tanto $p(1) = 0$

$$\left.\begin{array}{rrl} 2+b= & p(0) & =d \\ b+d= & p(-1) & =-2+b-c+d \\ 0= & p(0) & =2+b+c+d \end{array}\right|; \qquad \text{simplificando} \qquad \left.\begin{array}{rcr} -b+d & = & 2 \\ c & = & -2 \\ b+d & = & 0 \end{array}\right|$$

De lo cual

$$b=-1 \quad c=-2 \quad d=1$$

Por lo tanto $p(x) = 2x^3 - x^2 - 2x + 1$. ♡

Solución 55. Como se tiene que $gr((x-2)(x-3)(x-4)) = 3$, luego el resto debe ser $r(x) = ax^2 + bx + c$, sea $p(x)$ tal que,

$$\left.\begin{array}{rcl} p(x) & = & q_1(x)\cdot(x-3)+2 \\ p(x) & = & q_2(x)\cdot(x-2)+0 \\ p(x) & = & q_3(x)\cdot(x-4)+6 \\ p(x) & = & q(x)\cdot(x-3)\cdot(x-2)\cdot(x-4)+ax^2+bx+c \end{array}\right|;$$

Evaluando en 3,2 4, obtenemos

$$\left.\begin{array}{rrl} 2= & p(3) & =9a+2b+c \\ 0= & p(2) & =4a+2b+c \\ 6= & p(4) & =16a+4b+c \end{array}\right|; \quad \text{simplificando} \quad \left.\begin{array}{rcr} 9a+2b+c & = & 2 \\ 4a+2b+c & = & 0 \\ 16a+4b+c & = & 6 \end{array}\right|;$$

Despejemos c de la primera ecuación, $c = 2-3b-9a$ y lo reemplazamos en la segunda ecuación

$$\begin{array}{rcl} 4a+2b+2-3b-9a & = & 0 \\ b & = & -5a+2 \end{array}$$

Reemplazando en el valor de b obtenemos

$$\begin{array}{rcl} c & = & 2-3\cdot(-5a+2)-9a \\ c & = & 6a-4 \end{array}$$

de este modo tenemos $b = -5a+2;\ c = 6a-4$, reemplacemos en la tercera ecuación del sistema

$$\begin{array}{rcl} 16a+4\cdot(-5a+2)+6a-4 & = & 6 \\ 16a-20a+8+6a-7 & = & 6 \\ a & = & 1 \end{array}$$

$$\begin{aligned} b &= -5a + 2 = -5 + 2 = -3 \\ c &= 6a - 4 = 6 - 4 = 2 \end{aligned}$$

Por lo tanto $r(x) = x^2 - 3x + 2$. ♡

Solución 56. Apliquemos división sintética en $p(x) = x^4 + ax^3 + (a-b)x^2 + bx + 1$

-1	1	a	$a-b$	b	1
		-1	$-a+1$	$-1+b$	$1-2b$
-1	1	$a-1$	$1-b$	$-1+2b$	$2-2b=0$
		-1	$2-a$	$-3+a+b$	
	1	$a-2$	$3-a-b$	$-4+a+3b=0$	

De lo cual obtenemos el siguientes sistema

$$\left.\begin{aligned} 2-2b &= 0 \\ -4+a+3b &= 0 \end{aligned}\right|$$

Resolviendo el sistema obtenemos

$$b = 1; \quad a = 1$$

Luego $p(x) = x^4 + x^3 + x + 1$. ♡

Solución 57. Sea $p(x) = 6x^3 + tx^2 + kx - 3t$, el enunciados se traduce en el siguiente sistema

$$\left.\begin{aligned} p(2) &= 21 \\ p(1) &= 0 \end{aligned}\right|$$

Reemplazando obtenemos

$$\left.\begin{aligned} 48 + 4t + 2k - 3t &= 21 \\ 6 + t + k - 3t &= 0 \end{aligned}\right|; \quad \text{Simplificando} \quad \left.\begin{aligned} t + 2k &= -27 \\ -2t + k &= -6 \end{aligned}\right|$$

Amplificando por 2 y sumando las ecuaciones

$$\begin{aligned} 5k = -60; &\qquad k = -12 \\ t = -27 - 2k; &\qquad t = -27 + 24 = -3 \end{aligned}$$

Por lo tanto $k = -12$ y $t = -3$ y $p(x) = 6x^3 - 3x^2 - 12x + 9$. ♡

Solución 58. Sea $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$, tal que

$$\left.\begin{aligned} p(1) &= 0 \\ p(\tfrac{1}{2}) &= 0 \end{aligned}\right|; \quad \text{Evaluando} \quad \left.\begin{aligned} 2 + a + 28 + b + 6 &= 0 \\ \tfrac{1}{8} + \tfrac{a}{8} + 7 + \tfrac{b}{2} + 6 &= 0 \end{aligned}\right|$$

Simplificando

$$\left.\begin{aligned} a + b &= -36 \\ -a - 4b &= 105 \end{aligned}\right|;$$

Sumando obtenemos

$$\begin{aligned} -3b = 69; \qquad & b = -23 \\ a = -36 - b; \qquad & a = -36 + 23 = -13 \end{aligned}$$

Luego Sea $p(x) = 2x^4 - 13x^3 + 28x^2 - 23x + 6$. ♡

Solución 59. Ya que el $gr((x+1)\cdot(x-1)) = 2$, luego el resto debe ser $r(x) = ax + b$. Sea $p(x) \in \mathbb{R}[x]$ tal que

$$\left.\begin{array}{rcl} p(x) & = & q_1(x)\cdot(x+1)+2 \\ p(x) & = & q_2(x)\cdot(x-1)+3 \\ p(x) & = & q(x)\cdot(x+1)\cdot(x-1)+ax+b \end{array}\right|;$$

Evaluando y simplificando obtenemos

$$\left.\begin{array}{rcl} 3 & = & a+b \\ 2 & = & -a+b \end{array}\right|;$$

Luego

$$\begin{aligned} 5 = 2b; \qquad & b = \frac{5}{2} \\ a = -b + 3; \qquad & a = 3 - \frac{5}{2} = \frac{1}{2} \end{aligned}$$

Por lo tanto $r(x) = \frac{1}{2}x + \frac{5}{2}$. ♡

Solución 60. La factorización esta dada por

a) En $\mathbb{Q}[x]$:

$$x^6 - 1 = (x^3-1)\cdot(x^3+1) = (x-1)\cdot(x^2+x+1)\cdot(x+1)\cdot(x^2-x+1)$$

b) En $\mathbb{R}[x]$:

$$x^6 - 1 = (x-1)\cdot(x^2+x+1)\cdot(x+1)\cdot(x^2-x+1)$$

c) En $\mathbb{C}[x]$:

$$x^6-1 = (x-1)\left(x - \frac{-1+\sqrt{3}i}{2}\right)\left(x - \frac{-1-\sqrt{3}i}{2}\right)(x+1)\left(x - \frac{1+\sqrt{3}i}{2}\right)\left(x - \frac{1-\sqrt{3}i}{2}\right)$$

♡

Solución 61. Sea $p(x) = 2x^4 + ax^3 + 28x^2 + bx + 6$, apliquemos división sintética

1	2	a	28	b	6
		2	$2+a$	$30+a$	$30+a+b$
$\frac{1}{2}$	2	$2+a$	$30+a$	$30+a+b$	$36+a+b=0$
		1	$\frac{3+a}{2}$	$\frac{63+3a}{4}$	
	2	$3+a$	$\frac{63+3a}{2}$	$\frac{183+7a+4b}{4}=0$	

$$\left.\begin{array}{rcll} a+b & = & -36 & /\cdot -4 \\ 7a+4b & = & -183 & \end{array}\right|; \quad \text{Amplificando} \quad \left.\begin{array}{rcl} -4a-4b & = & 144 \\ 7a+4b & = & -183 \end{array}\right|;$$

Sumando obtenemos

$$\begin{aligned} 3a = -39; \qquad & a = -13 \\ b = -36 - a; \qquad & b = -36 + 13 = -23 \end{aligned}$$

Luego el polinomio es $p(x) = 2x^4 + -13x^3 + 28x^2 - 23x + 6$, y se factoriza $p(x) = (x-1)(x-\frac{1}{2})(2x^2 - 10x + 12)$. Veamos ahora el factor cuadrático $2x^2 - 10x + 12$, cuyo discriminante es $\Delta = 10^2 - 4 \cdot 2 \cdot 12 = 4$, luego las raíces son

$$x_1 = \frac{10+2}{4} = 3; \qquad x_2 = \frac{10-2}{4} = 2$$

Luego el polinomio es

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

♡

Solución 62. Sea $p(x) = x^6 - x^5 - 5x^4 + 5x^3 - 36x^2 + 36x$

a) Determine las raíces racionales de $p(x)$

$p(x) = x \cdot (x^5 - x^4 - 5x^3 + 5x^2 - 36x + 36)$

1	1	−1	−5	5	−36	36
		1	0	−5	0	−36
	1	0	−5	0	−36	0

$$\begin{aligned} p(x) &= x \cdot (x-1) \cdot (x^4 - 5x - 36) \\ p(x) &= x \cdot (x-1) \cdot (x^2 - 9) \cdot (x^2 + 4) \\ p(x) &= x \cdot (x-1) \cdot (x+3) \cdot (x-3) \cdot (x^2 + 4) \end{aligned}$$

Raíces racionales $0, 1, \pm 3$

b) La factorización de $p(x)$ como producto de polinomios irreducibles en $\mathbb{R}[x]$ es

$$p(x) = x \cdot (x-1) \cdot (x+3) \cdot (x-3) \cdot (x^2 + 4)$$

c) La factorización de $p(x)$ como producto de polinomios irreducibles en $\mathbb{C}[x]$

$$p(x) = x \cdot (x-1) \cdot (x+3) \cdot (x-3) \cdot (x+2i) \cdot (x-2i)$$

♡

Solución 63. Para factorizar $x^8 + x^4 + \overline{1} \in \mathbb{Z}_7[x]$, note que 0 no es raíz de $p(x)$, además

$$\begin{aligned} x^7 &\equiv x(\texttt{mod } 7) \quad / \cdot x \\ x^8 &\equiv x^2(\texttt{mod } 7) \end{aligned}$$

Luego

$$x^4 + x^2 + \overline{1} = 0$$

Realizando el cambio de variable $u = x^2,\ u^2 = x^4$ tenemos

$$\begin{aligned} u^2 + u + \overline{1} &= 0 \quad 1 \equiv -6(\texttt{mod } 7) \\ u^2 + u - \overline{6} &= 0 \\ (u + \overline{3}) \cdot (u - \overline{2}) &= 0 \\ (x^2 + \overline{3}) \cdot (x^2 - \overline{2}) &= 0 \quad 3 \equiv -4(\texttt{mod } 7), \quad -2 \equiv -9(\texttt{mod } 7) \\ (x^2 - \overline{4}) \cdot (x^2 - \overline{9}) &= 0 \\ (x - \overline{2}) \cdot (x + \overline{2}) \cdot (x + \overline{3}) \cdot (x - \overline{3}) &= 0 \end{aligned}$$

Por lo tanto

$$x^8 + x^4 + \overline{1} = (x - \overline{2}) \cdot (x + \overline{2}) \cdot (x + \overline{3}) \cdot (x - \overline{3})$$

♡

Solución 64. Factorizar $x^4 + \overline{4} \in \mathbb{Z}_5[x]$.

$$\begin{aligned} x^4 + \overline{4} &= x^4 - \overline{1} \quad 4 \equiv -1(\texttt{mod } 5) \\ x^4 + \overline{4} &= (x^2 - \overline{1}) \cdot (x^2 + \overline{1}) \quad 1 \equiv -4(\texttt{mod } 5) \\ x^4 + \overline{4} &= (x - \overline{1}) \cdot (x + \overline{1}) \cdot (x^2 - \overline{4}) \\ x^4 + \overline{4} &= (x - \overline{1}) \cdot (x + \overline{1}) \cdot (x + \overline{2}) \cdot (x - \overline{2}) \end{aligned}$$

♡

Solución 65 Descomponer $p(x) = x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$ en factores irreducibles.

1	1	1	1	1	1
		1	2	3	4
1	1	2	3	4	$5 = 0$
		1	3	6	
1	1	3	6	$10 = 0$	
		1	4		
1	1	4	$10 = 0$		
		$5 = 0$			

Por lo tanto $x^4 + x^3 + x^2 + x + \overline{1} = (x - \overline{1})^4$ ♡

Solución 66. Dado el polinomio $x^3 + x^2 + x + 1 = (x - a) \cdot (x - b) \cdot (x - c)$

$$x^3 + x^2 + x + 1 = x^3 + x^2 \cdot (-a - b - c) + x \cdot (ab + bc + ac) - abc$$

de lo cual obtenemos el siguiente sistema

$$\begin{array}{rcl|} -a-b-c & = & 1 \\ ab+bc+ac & = & 1 \\ -abc & = & 1 \\ \hline \end{array}$$

Además, se tiene que

$$(x-a^2)\cdot(x-b^2)\cdot(x-c^2) = x^3 + x^2\cdot(-a^2-b^2-c^2) + x\cdot(a^2b^2+b^2c^2+a^2c^2) - a^2b^2c^2$$

Luego debemos calcular el valor de $a^2b^2c^2,\ (a^2b^2+b^2c^2+a^2c^2),\ (-a^2-b^2-c^2)$, veamos el primer valor, de la tercera ecuación tenemos

$$\begin{array}{rcll} -abc & = & 1 & /()^2 \\ a^2b^2c^2 & = & 1 & /\cdot -1 \\ -a^2b^2c^2 & = & -1 & \end{array}$$

De la segunda ecuación tenemos

$$\begin{array}{rcll} -a-b-c & = & 1 & /()^2 \\ a^2+b^2+c^2+2ab+2bc+2ac & = & 1 & \\ a^2+b^2+c^2+2\cdot(ab+bc+ac) & = & 1 & \end{array}$$

Reemplazando el valor de la segunda ecuación

$$\begin{array}{rcl} a^2+b^2+c^2+2 & = & 1 \\ a^2+b^2+c^2 & = & -1 \end{array}$$

El último coeficiente lo obtenemos de

$$\begin{array}{rcll} ab+bc+ac & = & 1 & /()^2 \\ a^2b^2+b^2c^2+a^2c^2+2aabc+2babc+2cabc & = & 1 & \\ a^2b^2+b^2c^2+a^2c^2+2abc\cdot(a+b+c) & = & 1 & \end{array}$$

Reemplazando tenemos

$$a^2b^2+b^2c^2+a^2c^2 = -1$$

Por lo tanto el polinomio pedido es $x^3+x^2-x-1 = (x-a^2)\cdot(x-b^2)\cdot(x-c^2)$. ♡

Solución 67. De forma similar obtenemos

$$x^3+2x^2+3x+1 = x^3+x^2\cdot(-a-b-c)+x\cdot(ab+bc+ac)-abc,$$

igualando coeficiente obtenemos

$$\begin{array}{rcl|} -a-b-c & = & 2 \\ ab+bc+ac & = & 3 \\ -abc & = & 1 \\ \hline \end{array}$$

Por otro lado necesitamos los valores de

$$(x-a^2)\cdot(x-b^2)\cdot(x-c^2) = x^3+x^2\cdot(-a^2-b^2-c^2)+x\cdot(a^2b^2+b^2c^2+a^2c^2)-a^2b^2c^2$$

$$-a^2b^2c^2=(abc)^2=-1$$

El segundo se obtiene de

$$a^2+b^2+c^2=(-a-b-c)^2-2\cdot(ab+bc+ac)=-2$$

Y el tercero

$$a^2b^2+b^2c^2+a^2c^2=(ab+bc+ac)^2-2abc\cdot(a+b+c)=5$$

Por lo tanto el polinomio pedido es $x^3+2x^2+5x-1=(x-a^2)\cdot(x-b^2)\cdot(x-c^2)$. ♡

Solución: 68 Sea $x^3-x^2-1=(x-a)\cdot(x-b)\cdot(x-c)$, luego

$$x^3-x^2-1 = x^3-x^2\cdot(a+b+c)+x\cdot(ab+bc+ac)-abc$$

De lo cual se obtiene

$$\begin{array}{|rcl|}\hline a+b+c &=& 1\\ ab+bc+ac &=& 0\\ abc &=& 1\\ \hline\end{array}$$

Por otro lado

$$\begin{aligned}
& (x-(a+b))\cdot(x-(a+c))\cdot(x-(b+c))\\
= \;& (x^2-(a+c)x-(a+b)x+(a+b)\cdot(a+c))\cdot(x-(b+c))\\
= \;& (x^2-x(2a+b+c)+(a+b)\cdot(a+c))\cdot(x-(b+c))\\
= \;& x^3-x^2(2a+b+c)+x(a+b)(a+c)-\\
& \quad x^2(b+c)+x(2a+b+c)(b+c)-(a+b)(a+c)(b+c)\\
= \;& x^3-x^2(2a+2b+2c)+x(a^2+b^2+c^2+3ab+3bc+3ac)-\\
& \quad (a^2b+a^2c+b^2c+b^2a+ac^2+bc^2+2abc)
\end{aligned}$$

Los coeficientes buscados

$$\begin{aligned}
2a+2b+2c &= 2(a+b+c)=2\\
a^2+b^2+c^2+3ab+3bc+3ac &= (a+b+c)^2+(ab+bc+ac)=1
\end{aligned}$$

Además

$$\begin{aligned}
& a^2b+a^2c+b^2c+b^2a+ac^2+bc^2+2abc\\
= \;& (a+b+c)(ac+ab+bc)-abc=-1
\end{aligned}$$

Por lo tanto el polinomio pedido es x^3-2x^2+x+1. ♡

Solución 69. Factorizar $x^8+\overline{4}\in\mathbb{Z}_5[x]$

$$\begin{aligned}
x^8+\overline{4} &= x^8-\overline{1} \quad 4\equiv -1(\texttt{mod } 5)\\
x^8+\overline{4} &= (x^4-\overline{1})\cdot(x^4+\overline{1}) \quad 1\equiv -4(\texttt{mod } 5)\\
x^8+\overline{4} &= (x^2-\overline{1})\cdot(x^2+\overline{1})\cdot(x^4-\overline{4})\\
x^8+\overline{4} &= (x-\overline{1})\cdot(x+\overline{1})\cdot(x^2-\overline{4})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})\\
x^8+\overline{4} &= (x-\overline{1})\cdot(x+\overline{1})\cdot(x-\overline{2})\cdot(x+\overline{2})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})
\end{aligned}$$

Veremos los polinomios cuadráticos

$$\begin{aligned}
x^2-\overline{2} &\equiv 0(\texttt{mod } 5)\\
x^2 &\equiv \overline{2}(\texttt{mod } 5)\\
\left(\frac{2}{5}\right) &= (-1)^{\frac{5^2-1}{8}}=-1
\end{aligned}$$

Por lo tanto $2\notin\mathbb{Z}_5$, es decir, $x^2-\overline{2}$ es irreducible en $\mathbb{Z}_5[x]$

$$\begin{aligned}
x^2+\overline{2} &\equiv 0(\texttt{mod } 5)\\
x^2 &\equiv -\overline{2}(\texttt{mod } 5)
\end{aligned}$$

Veamos si -2 es un cuadrado, para ello calculemos

$$\left(\frac{-2}{5}\right)=\left(\frac{-1}{5}\right)\cdot\left(\frac{2}{5}\right)=(-1)^{\frac{5-1}{2}}(-1)^{\frac{5^2-1}{8}}=1\cdot -1=-1$$

Por lo tanto $-2\notin\mathbb{Z}_5$, es decir, $x^2+\overline{2}$ es irreducible en $\mathbb{Z}_5[x]$, de este modo tenemos que

$$x^8+\overline{4}=(x-\overline{1})\cdot(x+\overline{1})\cdot(x-\overline{2})\cdot(x+\overline{2})\cdot(x^2-\overline{2})\cdot(x^2+\overline{2})$$

♡

Solución 70. El anillo

$$\begin{aligned}
\mathbb{Z}_3[x]/<x^2-\overline{1}> &= \{\overline{ax+b}\mid a,b\in\mathbb{Z}_2\wedge\overline{x^2-1}=\overline{0}\}\\
\mathbb{Z}_3[x]/<x^2-\overline{1}> &= \{\overline{0},\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}
\end{aligned}$$

La aditiva

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x++2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+2}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x}$	$\overline{2x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{0}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{1}$	$\overline{2}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{x}$	$\overline{1}$	$\overline{2}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2}$	$\overline{0}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{0}$	$\overline{1}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{x+1}$	$\overline{2}$	$\overline{0}$	$\overline{x+2}$	$\overline{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{x+2}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$

Ahora la multiplicativa

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+1}$
$\overline{x}$	$\overline{x}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{2x+1}$
$\overline{2x}$	$\overline{2x}$	$\overline{x}$	$\overline{2}$	$\overline{x}$	$\overline{2x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{x+1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x+2}$	$\overline{0}$	$\overline{0}$	$\overline{x+1}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{0}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{0}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x+1}$	$\overline{x+1}$	$\overline{0}$	$\overline{0}$	$\overline{2x+2}$

♡

Solución 71. Dado el cuerpo

$$\mathbb{F}_{27} = \mathbb{Z}_3[x]/ < x^3 + 2x + 1 >= \{\overline{ax^2 + bx + c} \quad | \quad a, b, c \in \mathbb{Z}_3 \wedge \overline{x^3 + 2x + 1} = \overline{0}\}$$

Ya que,

$$x^3 = -2x - 1; \quad x^3 = x + 2; \quad x^4 = x^2 + 2x; \quad x^4 + 1 = x^2 + 2x + 1$$

Ahora busquemos el inverso de $\overline{x^4 + \overline{1}}$

$$\begin{aligned}
1 &= (x^2 + 2x + 1) \cdot (ax^2 + bx + c) \\
1 &= ax^4 + bx^3 + cx^2 + 2ax^3 + 2bx^2 + 2cx + ax^2 + bx + c \\
1 &= ax^4 + (b + 2a) \cdot x^3 + (a + c + 2b) \cdot x^2 + (b + 2c) \cdot x + c \\
1 &= a \cdot (x^2 + 2x) + (b + 2a) \cdot (x + 2) + (a + c + 2b) \cdot x^2 + (b + 2c) \cdot x + c \\
1 &= x^2 \cdot (2a + 2b + c) + x \cdot (4a + 2b + 2c) + 4a + 2b + c
\end{aligned}$$

De lo cual tenemos, el siguiente sistema

$$\left|\begin{array}{rcl} 2a + 2b + c &=& 0 \\ a + 2b + 2c &=& 0 \\ a + 2b + c &=& 1 \end{array}\right.$$

Ahora resolveremos el sistema, los coeficiente esta módulo 3. Despejando de la primera ecuación obtenemos $c = -2a - 2b = a + b$, reemplazando el la segunda ecuación obtenemos $b = 0$, de lo cual $c = a$ reemplazando en la tercera ecuación $a+2b+c = 1$, obtenemos $2a = 1$, y finalmente $a = 2$. Por lo tanto

$$\overline{x^4 + \overline{1}}^{-1} = \overline{\overline{2}x^2 + \overline{2}}$$

♡

Solución 72.

$$\mathbb{F}_{25} \quad = \quad \{\overline{ax + b} \quad | \quad a, b \in \mathbb{Z}_5 \wedge \overline{x^2 + x + 1} = \overline{0}\}$$

Busquemos un representante de $x^7+x^5+x^4+4$, para ello

$$x^7+x^5+x^4+4=(x^2+x+1)(x^5-x^4+x^3+x^2-2x+1)+(x+3)$$

De este modo obtenemos $x^7+x^5+x^4+4=x+3$ en $\mathbb{F}_{25}$.

Ahora busquemos el inverso

$$\begin{aligned}(x+3)\cdot(ax+b) &= 1\\ (2a+b)\cdot x-a+3b &= 0\cdot x+1\end{aligned}$$

de lo cual tenemos el siguiente sistema

$$\begin{array}{rcl}2a+b &=& 0\\ -a+3b &=& 1\end{array}$$

Amplificando por 2, y sumando las ecuaciones tenemos

$$\begin{aligned}7b=2; &\qquad b=1\\ 2a=-b; &\qquad a=2\end{aligned}$$

Por lo tanto $[x^7+x^5+x^4+4]^{-1}=[2x+1]$ ♡

Solución 73.

$$\begin{aligned}\mathbb{F}_8 &= \{\overline{ax^2+bx+c} \quad | \quad a,b,c\in\mathbb{Z}_2\wedge\overline{x^3+x+1}=\overline{0}\}\\ \mathbb{F}_8^* &= \{\overline{1},\overline{x},\overline{x^2},\overline{x+1},\overline{x^2+1},\overline{x^2+x},\overline{x^2+x+1}\}\end{aligned}$$

Veremos el generado por $\overline{x}$

$$<\overline{x}> \;=\; \{\overline{x},\overline{x^2},\overline{x+1},\overline{x^2+x},\overline{x^2+x+1},\overline{x^2+1},\overline{1}\}$$

Por lo tanto $\mathbb{F}_8^*$ es cíclico, pues $\overline{x}$ es un generador. ♡

Solución 74. Los elementos invertibles son;

$$\begin{aligned}\mathbb{F}_9 &= \{\overline{ax+b} \quad | \quad a,b\in\mathbb{Z}_3\wedge\overline{x^2+1}=\overline{0}\}\\ \mathbb{F}_9^* &= \{\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}\end{aligned}$$

Ahora veremos los ordenes, recuerde que debe ser un divisor de $9-1=8$

$$\begin{aligned}<\overline{1}> &= \{\overline{1}\}\\ <\overline{2}> &= \{\overline{2},\overline{1}\}\\ <\overline{x}> &= \{\overline{x},\overline{2},\overline{2x},\overline{1}\}\\ <\overline{2x}> &= \{\overline{2x},\overline{2},\overline{x},\overline{1}\}\\ <\overline{x+1}> &= \{\overline{x+1},\overline{2x},\overline{2x+1},\overline{2},\overline{2x+2},\overline{x},\overline{x+2},\overline{1}\}\\ <\overline{x+2}> &= \{\overline{x+2},\overline{x},\overline{2x+2},\overline{2},\overline{2x+1},\overline{2x},\overline{x+1},\overline{1}\}\\ <\overline{2x+1}> &= \{\overline{2x+1},\overline{x},\overline{x+1},\overline{2},\overline{x+2},\overline{2x},\overline{2x+2},\overline{1}\}\\ <\overline{2x+2}> &= \{\overline{2x+2},\overline{2x},\overline{x+2},\overline{2},\overline{x+1},\overline{x},\overline{2x+1},\overline{1}\}\end{aligned}$$

elemento	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$
orden	1	2	4	4	8	8	8	8

♡

Solución 75. Necesitamos saber si x^2-8 es irreducible en $\mathbb{Z}_{19}$, lo cual depende si 8 es un cuadrado

$$\left(\frac{8}{19}\right) = \left(\frac{2^2}{19}\right)\cdot\left(\frac{2}{19}\right) = 1(-1)^{\frac{19^2-1}{8}} = -1$$

Por lo tanto, $8 \notin \square_{19}$, es decir, x^2-8 es irreducible, luego $\mathbb{Z}_{19}[x]/ < x^2-8 >$ es un cuerpo. ♡

Solución 76. El polinomio x^2+1 irreducible en $\mathbb{Z}_3$, luego

$$\begin{aligned}\mathbb{F}_9 &= \{\overline{ax+b} \quad | \quad a,b \in \mathbb{Z}_3 \wedge \overline{x^2+1} = \overline{0}\}\\ \mathbb{F}_9 &= \{\overline{1},\overline{2},\overline{x},\overline{2x},\overline{x+1},\overline{x+2},\overline{2x+1},\overline{2x+2}\}\end{aligned}$$

$$\begin{aligned}\overline{-1}^2 = \overline{1}^2 &= \overline{1}\\ \overline{-x}^2 = \overline{x}^2 &= \overline{2}\\ \overline{2x+2}^2 = \overline{x+1}^2 &= \overline{x^2+2x+1} = \overline{-1+2x+1} = \overline{2x}\\ \overline{2x+1}^2 = \overline{x+2}^2 &= \overline{x^2+4x+4} = \overline{-1+x+1} = \overline{x}\end{aligned}$$

Luego los cuadrados son

$$\square_{\mathbb{F}_9} = \{\overline{1},\overline{2},\overline{x},\overline{2x}\}$$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{2x}$	$\overline{2}$	$\overline{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{x}$	$\overline{1}$	$\overline{2}$

♡

Solución 77. Para que no se un cuerpo es necesario que $x^2-\alpha$ sea reducible, luego la ecuación

$$\begin{aligned}x^2-\alpha &\equiv 0(\texttt{mod } 7)\\ x^2 &\equiv \alpha(\texttt{mod } 7)\end{aligned}$$

Debe tener solución, luego $\alpha = 0 \vee \alpha \in \square_7$

Pero

$$\square_7 = \{\overline{1},\overline{4},\overline{2}\}$$

Por lo tanto $\alpha \in \{\overline{0},\overline{1},\overline{2},\overline{4}\}$. ♡