UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE MATEMÁTICAS

"TEOREMA DE LAGRANGE PARA DETERMINAR EL NÚMERO DE RAÍCES DE UNA ECUACIÓN POLINÓMICA MÓDULO p (primo) DE GRADO n"

TESIS GUIADA

PARA OPTAR EL TÍTULO DE

LICENCIADO EN MATEMÁTICAS

AUTOR:

Bach. Saul Felipe, RAMIREZ HUARAC

ASESOR:

Msc. Mario NINAQUISPE CASTILLO

HUARAZ – PERÚ

2018

PROGRAMA DE TITULACIÓN PROFESIONAL

MODALIDAD TESIS GUIADA – 2018

N° Registro: T003

HOJA DE VISTO BUENO

_____

M. Sc. Perpetua María Alayo Meregildo
Presidenta
Reg. COMAP Nº 1532

_____

Dr. Bibiano Martin Cerna Maguiña
Secretario
Reg. COMAP Nº 1014

_____

M. Sc. Rodríguez Sabino Vladimir Giovanni
Vocal
Reg. COMAP Nº 807

Dedicado a:

A mi familia, amigos y todas aquellas personas que, directa e indirectamente, me apoyaron en la realización de este trabajo

AGRADECIMIENTO

A nuestro Padre Celestial, Dios, por los dones y talentos que regala a cada uno de sus hijos y por siempre acompañarme con su espíritu.

A mi madre, Nila Huarac Sanchez, por su apoyo incondicional, palabras y actos alentadores que me hacen reflexionar, motivar y desear seguir adelante, por su confianza en mí y por sus sacrificios para darme la oportunidad de estudiar y ser una persona de provecho para la sociedad.

A mi asesor, quien con su magnífica paciencia, empeño, apoyo moral y sapiencia supo encaminarme en el inicio, realización y conclusión de esta tesis.

RESUMEN

En este trabajo de investigación se realizó el estudio de las ecuaciones en congruencias polinómicas, en primera instancia de las lineales, determinándose las soluciones y condiciones para conocer sus raíces, sin embargo, para las de mayor grado, estas son complicadas y en algunos casos imposible de conocerlas, motivo por el cual se abordó el estudio del cálculo del número de raíces que presenta una ecuación polinómica modulo p (primo) de grado n analizado por el teorema de Lagrange.

Para ello se empezó definiendo los conceptos de polinomios, tipos y operaciones en estos, el teorema fundamental del algebra (que establece que para cada polinomio de grado n este presenta n raíces) y al final, las congruencias en cuerpos y anillos, fueron el ámbito donde se desarrolló y se percibió el campo o conjunto al que pertenecen las raíces.

Como parte adicional, esta investigación pretende, obtener como resultados secundarios, el identificar las características de la teoría de congruencias que determinen el número de raíces de una ecuación polinómica de grado n, además de identificar ciertas particularidades que tienen las raíces de una ecuación polinómica de grado n y poder establecer, si es que se da el caso, ciertas condiciones para especificar el número de "raíces múltiples" de una ecuación polinómica de grado n.

Palabras clave: Congruencias, polinomios, número de raíces, teorema de Lagrange, campo, anillos.

ABSTRACT

In this research of the study, the study of performed in polynomial congruences, first of linear, determining solutions and conditions to know their roots, however, for higher grade, these are complicated and in some cases impossible of knowing, why the study of calculating the number of roots having a polynomial equation modulo p (prime) of degree n analyzed by Lagrange's theorem addressed.

To do this, we began by defining the concepts of polynomials, types and operations in these, the fundamental theorem of algebra (which states that for each polynomial of degree n this presents n roots) and in the end, the congruences in bodies and rings, were the scope where the field or group to which the roots belong was developed and perceived.

As an additional part, this research aims to obtain as secondary results, identify the characteristics of the congruence theory that determine the number of roots of a polynomial equation of degree n, as well as identify certain features that have the roots of a polynomial equation of grade n and be able to establish, if that is the case, certain conditions to specify the number of "multiple roots" of a polynomial equation of degree n.

Keywords: Congruences, polynomials, number of roots, Lagrange theorem, field, rings.

ÍNDICE GENERAL

AGRADECIMIENTO i

RESUMEN ii

ABSTRACT iii

INTRODUCCIÓN 1

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 2

1.1. FORMULACIÓN DEL PROBLEMA 2

1.2. OBJETIVOS DE LA INVESTIGACIÓN 2

1.2.1. Objetivo general 2

1.2.2. Objetivo específicos 2

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN 2

CAPITULO II: PRELIMINARES GENERALES 4

2.1. ESTRUCTURAS ALGEBRAICAS 4

2.1.1. CONJUNTO 4

2.1.1.1. Operaciones con Conjuntos 5

2.1.2. RELACIONES BINARIAS: 9

2.1.2.1. Producto cartesiano 9

2.1.2.2. Relación Binaria 9

2.1.2.3. Dominio e Imagen de una Relación 9

2.1.2.4. Propiedades de una Relación Binaria 9

2.1.3. RELACIONES DE EQUIVALENCIA 10

2.1.3.1. Particiones de un conjunto 10

2.1.3.2. Clases de Equivalencia 11

2.1.3.3. Conjunto Cociente 11

2.1.4. FUNCIONES 11

2.1.4.1. Tipos de funciones especiales 12

2.2. OPERACIONES BINARIAS 13

2.2.1. Ley de Composición Interna 15

2.2.2. Ley de Composición Externa 15

2.3. SEMIGRUPOS 15

2.4. MONOIDES 15

2.5. GRUPOS 16

2.6. HOMOMORFISMO 17

2.7. ANILLOS 17

2.8. CUERPOS 18

2.9. DIVISIBILIDAD 18

2.10. MÁXICO COMÚN DIVISOR 20

2.10.1. Divisor Común 20

2.10.2. Máximo Común Divisor 21

2.10.3. Máximo Común Divisor de Varios Números 23

2.10.4. Existencia y Unicidad del m.c.d. 23

CAPÍTULO III: MARCO TEÓRICO 29

3.1. DEFINICIÓN DE POLINOMIOS 29

3.2. OPERACIONES CON POLINOMIOS 30

3.3. RAÍCES DE UN POLINOMIO 32

3.4. DIVISIBILIDAD DE POLINOMIOS 35

3.5. EL ALGORITMO DE DIVISIÓN PARA POLINOMIOS 35

3.6. EL TEOREMA DEL RESTO 38

3.7. RAÍCES RACIONALES 40

3.7.1. Criterio de Gauss 40

3.8. MULTIPLICIDAD DE RAÍCES 41

3.9. TEOREMA FUNDAMENTAL DEL ALGEBRA 43

3.10. RAÍCES COMPLEJAS DE POLINOMIOS REALES 44

3.11. DEFINICIÓN DE CONGRUENCIA 48

3.12. ENTEROS MÓDULO m 51

3.12.1. Operaciones en $\mathbb{Z}\boldsymbol{m}$ 52

3.13. ECUACIONES LINEALES DE CONGRUENCIA 53

CAPITULO IV: METODOLOGÍA 59

4.1. TIPO DE INVESTIGACIÓN 59

4.2. MÉTODO DE LA INVESTIGACIÓN 59

4.3. DISEÑO DE LA INVESTIGACIÓN 59

CAPÍTULO V: RESULTADOS 60

5.1. GRADO DE CONGRUENCIA DE UN POLINOMIO 62

5.2. CONGRUENCIAS LINEALES 62

5.3. CONGRUENCIAS POLINÓMICAS - TEOREMA DE LAGRANGE 65

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 68

6.1. CONCLUSIONES 68

6.2. RECOMENDACIONES 69

BIBLIOGRAFÍA 70

INTRODUCCIÓN

El problema de investigación surge por el interés de resolver ecuaciones polinómicas, así como en el estudio de los temas del curso de teoría de números del nivel de pregrado de la Carrera profesional de Matemáticas en la Facultad de Ciencias de la UNASAM.

Como bien es sabido, las resoluciones de ecuaciones de primer y segundo grado, no presentan mayores dificultades en su resolución; más, la situación es completamente diferente para las ecuaciones de grado mayor a dos.

Frente a todo esto, se presentan en el primer capítulo, el planteamiento del problema donde se exponen los objetivos y la justificación del desarrollo de la investigación; en el segundo capítulo se muestran las nociones básicas de estructuras algebraicas que incluye conjuntos, relaciones binarias, funciones, operaciones binarias, criterios de divisibilidad remarcando la definición de máximo común divisor de dos números, que sirven de sustento formal para poder presentar a los polinomios, de este capítulo, como un elemento de los anillos.

En el capítulo tres, se expone el marco teórico compuesto por el estudio de las congruencias desde el enfoque de la teoría de números, tratando definiciones y teoremas orientados a las ecuaciones polinómicas congruentes, presentando las demostraciones formales de varios de estos resultados, en el capítulo cuarto se expone la metodología de la investigación, para que finalmente en el capítulo quinto, capitulo central, se estudia el teorema de Lagrange para las ecuaciones polinómicas congruentes, en la cual se dan condiciones que garantizan la existencia de las raíces de la ecuación en estudio.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. FORMULACIÓN DEL PROBLEMA

¿Cómo influye el uso del teorema de Lagrange en la determinación del número de raíces de una ecuación polinómica módulo p (primo) de grado n?

1.2. OBJETIVOS DE LA INVESTIGACIÓN

1.2.1. Objetivo general

Determinar el número de raíces que presenta una ecuación polinómica módulo p (primo) de grado n.

1.2.2. Objetivo específicos

- Comprobar que, las ecuaciones polinómicas modulo n, satisfacen el teorema fundamental del algebra que establece que para cada polinomio de grado n este presenta n raíces.
- Comprobar si una ecuación polinómica modulo p (primo) de grado n tendrán más de n soluciones, si los coeficientes del polinomio son múltiplos de este número p.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

La pertinencia de la investigación radica en comprender los pasos que permitan determinar el número de raíces de una ecuación polinómica de grado n tomando de apoyo la teoría de congruencias, específicamente, congruencias modulo primo del Teorema de Lagrange.

Si bien el Teorema fundamental del Algebra establece que, para cada polinomio f de grado $n \geq 1$, la ecuación $f(x) = 0$ tiene n soluciones en el cuerpo de los números complejos.

No existe un resultado directamente similar a este teorema para las ecuaciones polinómicas de congruencias. Así, se sabe que ciertas ecuaciones polinómicas de congruencia lineales carecen de soluciones (número de raíces ϵ ø), algunas tienen exactamente una solución (el número de raíces pertenece a un conjunto unitario) y otras en cambio tienen más de una solución (número de raíces pertenece a un conjunto finito).

Tomando este último caso como referencia, no parece que existe relación simple entre el número de soluciones con el grado del polinomio. Sin embargo, para las ecuaciones polinómicas de congruencias modulo primo, el teorema de Lagrange manifiesta que para todo polinomio de grado n, la ecuación polinómica de congruencia presenta a lo más n raíces.

CAPITULO II

PRELIMINARES GENERALES

Para este primer capítulo se ha considerado como referencia Sánchez, C. (2014), Hernández, (2007). Se presentan las definiciones, teoremas, lemas, corolarios y notaciones que usaremos a lo largo del trabajo, tales como monoides, cuerpo, grupo, anillos, divisibilidad, todos ellos relacionados con las estructuras algebraicas.

2.1. ESTRUCTURAS ALGEBRAICAS

2.1.1. CONJUNTO

Un conjunto es una colección de objetos que llamaremos "elementos". Un elemento a que está en el conjunto U se dice que pertenece a U y se escribe $a \in U$.Si a no está o no pertenece a U se escribe $a \notin U$. Usualmente, designaremos los conjuntos mediante letras mayúsculas del tipo A; B; etc, y a sus elementos con letras minúsculas. Utilizaremos algunos símbolos especiales para representar a algunos conjuntos numéricos, tales como: $\mathbb{N}$; $\mathbb{Z}$; $\mathbb{Q}$ y $\mathbb{R}$ que denotan los conjuntos de números naturales, enteros, racionales y reales, respectivamente; $\mathbb{Z}$ se debe a *zhalen* (número, en alemán) y $\mathbb{Q}$ se emplea por *quotient* (cociente).

Un conjunto puede definirse de las siguientes formas:

a) Por extensión, indicando todos los elementos del conjunto. En general, los elementos se representan entre llaves: $A = \{a_1, a_2, \dots, a_n\}$.

b) Por comprensión, dando una propiedad que caracterice a los elementos del conjunto:

$$B = \{x : p(x)\}$$

donde x toma valores en un cierto conjunto de referencia y *p(x)* es una forma proposicional que será verdadera si y sólo sí x se sustituye por un elemento de B.

Subconjunto o Inclusión

Un conjunto A es subconjunto de un conjunto B, $A \subseteq B$, si todo elemento de A pertenece a B, es decir, $\forall a \in A \Longrightarrow a \in B \; es \; verdadera$. También, se puede expresar que A esta incluido o contenido en *B*; o que B contiene o incluye a A, denota por $B \supseteq A$.

Conjunto Vacío

El conjunto vacío es un conjunto que no tiene elementos. Se simboliza por $\emptyset$ y satisface que $\emptyset \subseteq A$ cualquiera que sea el conjunto *A*.

Conjunto Universal o de Referencia

Un conjunto *U* se dice que es el universal de una serie de conjuntos con los que se está trabajando si cumple que, cualquiera de estos conjuntos es subconjunto de *U*.

2.1.1.1. Operaciones con Conjuntos

Presentaremos las operaciones que se realizan con los conjuntos, asi como algunas de las propiedades más usadas. Se considera que todos los conjuntos *A*, *B*, … están contenidos en un mismo conjunto U referencial.

Igualdad de Conjuntos

Dos conjuntos A y B son iguales, y se escribe $A = B$, si y sólo sí $A \subseteq B \quad y \quad B \supseteq A$. Escribiremos A = B. Simbólicamente, $A = B \iff (x \in A \iff x \in B)$ es verdadera para todo x. La igualdad de dos conjuntos se demuestra mediante la doble inclusión $A \subseteq B$ y $B \subseteq A$.

Conjunto Potencia

El conjunto **potencia de un conjunto** A es el conjunto de todos los subconjuntos posibles de A, se denotado por $P(A)$, es decir

$$P(A) = \{B \ / \ B \subseteq A\}$$

Llamaremos subconjunto propio de A a todo elemento B de P(A) distinto de A, puede emplearse la notación B ⊂ A.

Complemento

Dado un conjunto A de un conjunto referencial U, definimos su complemento, y se denota por $\bar{A}$ o A^C, en la forma: $A^C = \{x \in U / x \notin A\}$.

Intersección de Conjuntos

Es el conjunto formado por los elementos comunes de *A* y de *B*.

$$A \cap B = \{x \in U \ / \ x \in A \quad y \quad x \in B\}$$

Si $A \cap B = \emptyset$, los conjuntos se llaman disjuntos.

Unión de Conjuntos

La unión de los conjuntos A y B es el conjunto formado por todos los elementos de A y por todos los elementos de B:

$$A \cup B = \{x \in U \ / \ x \in A \ \ o \ \ x \in B\}$$

Diferencia de Conjuntos

La diferencia de los conjuntos A y B se le define como el conjunto:

$$A - B = \{x \in U \,/\, x \in A \,, x \notin B\} = A \cap B^C$$

Diferencia Simétrica

La diferencia simétrica de los conjuntos A y B es el conjunto:

$$A\Delta B = (A - B) \cup (B - A)$$

También se puede expresar:

$$A\Delta B = (A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)^C$$

Teorema 1.-

La unión, intersección, el complemento, diferencia y diferencia simétrica cumplen las siguientes propiedades.

Asociativa	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
	$(A \triangle B) \triangle C = A \triangle (B \triangle C)$	
Distributiva	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
Conmutativa	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Idempotente	$A \cup A = A$	$A \cap A = A$
	$A \triangle A = \emptyset$	
Simplificación	$A \cup (B \cap A) = A$	$A \cap (B \cup A) = A$

Absorción	$A \cup U = U, \quad A \cup \emptyset = A$		$A \cap U = A, \quad A \cap \emptyset = \emptyset$
	$A \triangle \emptyset = A$	$A \triangle U = A^C$	
Complementario	$(A^C)^C = A$	$A \subseteq B \Leftrightarrow B^C \subseteq A^C$	$U^C = \emptyset \quad \emptyset^C = U$
Leyes de Morgan	$(A \cup B)^C = A^C \cap B^C$		$(A \cap B)^C = A^C \cup B^C$

Observación. Las definiciones de intersección y unión de dos conjuntos se extienden a familias arbitrarias de conjuntos, consideremos para cada *i* perteneciente a una cierta familia *I* de índices, un subconjunto A_i de *U*.

Sabiendo que:

$$I = \{i \; i \; \epsilon \; \mathbb{Z}^+\}$$

Se pueden definir las operaciones unión e intersección de un número arbitrario de conjuntos:

$$A = \bigcap_{i \in I} A_i = \{x \in U : \; x \in A_i \; \forall \; i \in I\}$$

$$A = \bigcup_{i \in I} A_i = \{x \in U : \; x \in A_i, \text{para algun } i \in I\}$$

Cardinal de un conjunto finito A

Es el número de elementos que tiene dicho conjunto. Se representa por $Car(A)$ o $n(A)$ o $\#\,(A)$

Las siguientes fórmulas relacionan los cardinales y las operaciones entre conjuntos:

$n(A \cup B) = n(A) + n(B) - n(A \cap B)$

$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap B)$

$n(A^C) = n(U) - n(A)$

2.1.2. RELACIONES BINARIAS:

2.1.2.1. Producto cartesiano

Dados dos conjuntos A y B de un conjunto universal *U*, definimos el producto cartesiano de A y B al conjunto:

$$AxB = \{(a, b)/\ a \in A\ y\ b \in B\}$$

Los elementos (a, b) se les conoce como pares ordenados, "*a*" es la primera componente y "*b*" segunda componente; dos elementos de AxB son iguales si y sólo sí las componentes correspondientes son iguales, es decir

$$(a, b) = (a', b') \Leftrightarrow a = a',\ \ b = b'$$

Entre algunos resultados se tiene $AxB = BxA$ sí y sólo si A = B, si esto ocurre denotaremos $AxA = A^2$.

2.1.2.2. Relación Binaria

Dado los conjuntos *A* y *B*, cualquier subconjunto $\mathcal{R}$ de AxB, es una relación binaria de A en B, si $(a; b) \in \mathcal{R}$ diremos que a está relacionado con b, y se le denota $a\mathcal{R}b$. Si A = B entonces se tiene una relación $\mathcal{R}$ en A.

2.1.2.3. Dominio e Imagen de una Relación

Consideremos una relación $\mathcal{R}$ de $A\ en\ B$, definimos el dominio y la imagen de $\mathcal{R}$ como

$$Dom(\mathcal{R}) = \{x \in A:\ \ x\mathcal{R}y\ \ para\ algun\ y \in B\}$$

$$Im(\mathcal{R}) = \{y \in B:\ \ x\mathcal{R}y\ \ para\ algun\ x \in A\}$$

2.1.2.4. Propiedades de una Relación Binaria

Consideremos que $\mathcal{R}$ es una relación en *A*, se tiene las propiedades que puede cumplir:

Reflexiva. - Diremos que $\mathcal{R}$ es una relación reflexiva si y solo si $a\mathcal{R}a\ ,\ \forall a \in A$

Simétrica. - $\mathcal{R}$ se dice que es una relación simétrica si y solo $a\mathcal{R}b \implies b\mathcal{R}a$ es verdadera para cualesquiera sean $a, b \in A$

Antisimétrica. - Una relación $\mathcal{R}$ se dice que es una relación Antisimétrica si y solo $a\mathcal{R}b \wedge b\mathcal{R}a \implies a = b$ es verdadera para cualesquiera sean $a, b \in A$

Transitiva. - $\mathcal{R}$ se dice que es una relación transitiva si y solo $a\mathcal{R}b \wedge b\mathcal{R}c \implies a\mathcal{R}c$ es verdadera para cualesquiera sean $a, b, c \in A$

Orden. - $\mathcal{R}$ se dice que es una relación de orden en A si es reflexiva, antisimétrica y transitiva

2.1.3. RELACIONES DE EQUIVALENCIA

Una relación binaria $\mathcal{R}$ definida en un conjunto A es una relación de equivalencia si es reflexiva, simétrica y transitiva. Generalmente se usan los símbolos "$\sim$", "$\approx$", "$\equiv$", etc para indicar que se tiene una relación de equivalencia, dos elementos $x, y \in \mathcal{R}$ que son equivalente lo denotaremos $x \sim$y.

2.1.3.1. Particiones de un conjunto

Sabiendo que:

$$I = \{i / i \in \mathbb{Z}^+\}$$

y sea A un conjunto no vacío con $\{A_i\}_{i \in I}$ una familia de subconjuntos de A. Diremos que $\mathcal{P} = \{A_i\}_{i \in I}$ es una partición de A sí y sólo sí cumplen las siguientes condiciones:

$P_1)$ $\bigcup_{i \in I} A_i = A$

$P_2)$ $A_i \cap A_j = \emptyset_i \ si \ i \neq j$

Una partición de un conjunto *A* es una familia de subconjuntos no vacíos de A tal que todo elemento de *A* pertenece a uno y solo a uno de dichos subconjuntos.

2.1.3.2. Clases de Equivalencia

Sea ~ una relación de equivalencia en un conjunto A, y $a \in A$ definimos la clase de equivalencia de a como el conjunto de todos los elementos relacionados o equivalentes con él. Se representa por $\bar{a}$ ó $[a]$ o $Cl(a)$, es decir: $[a] = \{x \in A \,/\, x\Re a\} = \{x \in A \,/\, x{\sim}a\}$.

2.1.3.3. Conjunto Cociente

Sea $\Re$ una relación de equivalencia en un conjunto A. El conjunto de las clases de equivalencia se llama *Conjunto Cociente de A*. Y se representa por:

$$A \,/\, \Re = \{[a] \;/\, a \in A\}$$

2.1.4. FUNCIONES

Definición 1. - Sea $\mathcal{R}$ una relación del conjunto *A* en el conjunto *B*, diremos $\mathcal{R}$ es una función o aplicación de *A* en *B* si y sólo si para cada $a \in A$ existe un único $b \in B$ tal que $(a, b) \in \mathcal{R}$. Denotaremos las funciones con letras minúsculas de nuestro alfabeto f, g, h, … , y usaremos notaciones especiales para las relaciones funcionales (funciones); así , si f es una función de A en B escribiremos $f: A \longrightarrow B$ ó $A \xrightarrow{f} B$, el conjunto A es el conjunto de partida de f y el conjunto B es el conjunto de llegada de la función f.

Dado $a \in A$, la expresión *f(a)* (léase "f de *a*") indica el único elemento "*b*" de *B*, tal que $(a, b) \in f$, al valor de "*b*" es llamado la imagen de "*a*", equivalentemente que "*a*" es

una preimagen de "b"; luego a los conjuntos A y B se les conoce como el dominio y el codominio de f, respectivamente, se puede escribir como

$$Dom(f) = \{a \in A \,/\, \exists!\, b \in B, (a,b) \in f\} = A$$

$$Codom(f) = Im(f) = \{b \in B \,/\, \exists a \in A, (a,b) \in f\}$$

Dado un subconjunto X de A, la imagen de X mediante la aplicación f, denotada como $f(X)$ al subconjunto de B definido de la forma:

$$f(X) = Im(f) = \{b \in B \,/\, \exists x \in X, f(x) = b\}$$

Equivalentemente, dado un subconjunto Y de B la antiimagen de Y mediante f es el subconjunto de A, denotada como $f^{-1}(Y)$ y definido por:

$$f^{-1}(Y) = \{a \in A \,/\, f(a) \in Y\}$$

2.1.4.1. Tipos de funciones especiales

Una función $f: A \to B$ se denomina:

i) **Inyectiva**, si dado dos elementos cualesquiera $a_1, a_2 \in Dom(f)$ se cumple que

$$f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$$

En forma equivalente, una función es inyectiva si y sólo si a elementos diferentes del dominio corresponden elementos distintos del conjunto imagen; debido a ello, se dice también que una función es inyectiva si es una función uno a uno (1 -1)

ii) **Sobreyectiva**, la función f es sobreyectiva si $Im(f) = B$, equivale a decir que $\forall b \in B, \exists a \in A \,/\, f(a) = b$. También se le conoce como una función suryectiva, o simplemente diremos que f es una función de A sobre B.

iii) **Biyectiva**, diremos que f es una función biyectiva, o que f es una biyección de A en B, sí y solo si f es inyectiva y suryectiva.

Una función f es biyectiva si y sólo si para cada $b \in B$ existe un único $a \in A$ tal que b = f(a); también se puede expresar: que f establece una correspondencia biunívoca entre los elementos de A y B. Una biyección de un conjunto X en sí mismo se dirá simplemente una biyección de X. Dos conjuntos se dice que son coordinables si y sólo si existe una biyección entre ellos.

2.2. OPERACIONES BINARIAS

Definición 2. - Si A es un conjunto, cualquier función $\varpi: AxA \rightarrow A$ será una operación binaria en A, es decir que una operación binaria hace corresponder a cada par ordenado (a; b) de AxA un único elemento $\varpi(a; b)$ de A, Dom(f) = AxA.

Si el conjunto A tiene cardinalidad finita, se puede presentar la operación binaria mediante una tabla de doble entrada, con una fila y una columna para cada elemento de A, en dicha tabla se escribe, en el lugar correspondiente a la fila "a" y columna "b", el resultado $\varpi(a; b)$.

Generalmente se usa otros tipos de símbolos para denotar tal resultado, como a + b, a.b, axb, $a \otimes b$, … . ó cualquier otra forma.

Una operación binaria definida en un conjunto A, debe ser cerrada en A, esto quiere decir $\forall a, b \in A$ entonces que $\varpi(a; b) \in A$.

En general, a un conjunto A que tiene una operación binaria se le conoce como una Estructura Algebraica (E.A.) que denotaremos como $[A, *]$, se presenta las estructuras más habituales y las necesarias para llega r al objetivo.

Definición 3. - Sea * una operación binaria definida en A.

1. Asociativa. - La operación * es asociativa si y sólo si

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$$

2. Conmutativa. - La operación * es conmutativa si y sólo si

$$a * b = b * a \quad \forall a, b \in A$$

3. Existencia de elemento neutro. - Si $e \in A$ diremos que e es elemento neutro respecto a la operación * si y sólo si

$$e * a = a * e = a \quad \forall a \in A.$$

4. Existencia de elemento neutro. - Si $e \in A$ diremos que e es elemento neutro respecto a la operación * si y sólo si $e * a = a * e = a \quad \forall a \in A$.

5. Existencia de elemento inverso. - Si la operación * tiene elemento neutro e, un elemento $a \in A$ se dice inversible si y sólo si existe $b \in A$ tal que $a * b = b * a = e$, entonces al elemento $b \in A$ se le llama el inverso de $a \in A$.

6. Cancelativa.- La operación * es cancelativa a derecha (respectivamente a izquierda) si y sólo si $a * b = c * b \Longrightarrow a = c \quad (b * a = b * c \Longrightarrow a = c) \quad \forall a, b, c \in A$.

Diremos que * es cancelativa si y sólo si lo es a derecha y a izquierda.

7. Idempotencia.- Un elemento $a \in A$ se dice que es Idempotente si a*a = a

8. Relación de congruencia. - Sea R una relación de equivalencia definida en A, diremos que R es una congruencia si

$$\div \forall a, b, c, d \in A : (aRb) \wedge (cRd) \Longrightarrow (a; c)R(bRd)$$

2.2.1. Ley de Composición Interna

Sea A un conjunto cualquiera, y sea * una operación binaria bien definida $*: AxA \to A$ entonces a esta operación se le llama Ley de Composición Interna (L.C.I).

Teorema 2.- Sea $[A,*]$ una ley de Composición Interna, entonces existe a lo más un elemento neutro $e \in A$ respecto a la operación *

Demostración:

Por reducción al absurdo, supongamos que existen dos elementos neutros

$e_1 \in A \ y \ e_2 \in A$, $e_1 \neq e_2$, entonces $e_1 * e_2 = e_2$ por ser e_1 elemento neutro por la izquierda, de manera semejante se tiene que $e_1 * e_2 = e_1$ por ser e_2 elemento neutro por la derecha, luego

$$e_1 * e_2 = e_1 = e_2$$

Lo que contradice a la suposición inicial $e_1 \neq e_2$, y por tanto el elemento neutro es único

2.2.2. Ley de Composición Externa

Dados dos conjuntos $A \ y \ B$, una ley de composición externa es una función $\doteq: AxB \to A$, tal que, a un elemento de A y a otro elemento de B les hace corresponder uno de A.

2.3. SEMIGRUPOS

Definición 4. - Sea A un conjunto cualquiera, y $*: AxA \to A$ una ley de Composición Interna diremos que $[A,*]$ es un Semigrupo si, * es asociativa.

2.4. MONOIDES

Definición 5. - Sea $[A,*]$ un Semigrupo, si existe un elemento neutro $e \in A$, diremos que $[A,*,e]$ es un Monoide.

Teorema 3. En un Monoide $[A,*,e]$, cada elemento $a \in A$ tiene un único elemento inverso a^{-1}.

Demostración

Supongamos que para $a \in A$ existen dos elementos inversos $a_1^{-1}\ y\ a_2^{-1}$ tal que $a_1^{-1} \neq a_2^{-1}$.

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}$$

El cual contradice la hipótesis $a_1^{-1} \neq a_2^{-1}$ por tanto el inverso de a es único.

2.5. GRUPOS

Definición 6. - Sea $[A,*]$ un Monoide, se llamará un Grupo si sus elementos tienen inverso.

Demostración:

Supongamos que e y e' son dos elementos neutros que pertenecen a A. Entonces

$e * e' = e'$ pero también $e * e' = e$

Por lo tanto $e = e'$.

Si a_1 y a_2 son dos inversos de $a \in A$, entonces

$a_1 * (a * a_2) = a_1 * e = a_1$

$(a_1 * a) * a_2 = e * a_2 = a_2$

Ahora, por la propiedad asociativa, deducimos que $a_1 = a_2$ ■

Definición 7. - Sea $[A,*]$ un Grupo, si sus elementos satisfacen que es Conmutativo, entonces se le conoce como Grupo Conmutativo o Abeliano.

$$a * b = b * a\ , \forall a, b \in A$$

Demostración:

Cuando se usa notación aditiva $(* = +)$, se supone que la operación es conmutativa y que, por tanto:

$$a + b = b + a \,, \forall a, b \in A$$

$$a * b = a * b \quad \blacksquare$$

Se concluye que $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ y $(\mathbb{C}, +)$ forman cuatro grupos abelianos.

2.6. HOMOMORFISMO

Definición 8. - Sean $[A,*]$ y $[B, o]$ leyes de composición interna. Entonces una función

$f: A \to B$ se dice que es un Homomorfismo de $[A,*]$ a $[B, o]$ si verifica que:

$$f(a * b) = f(a)\, o\, f(b) \in B \,, \quad \forall a, b \in A$$

Definición 9. - Sea f un Homomorfismo de $[A,*]$ a $[B, o]$, diremos que f es un Isomorfismo si f es biyectiva.

2.7. ANILLOS

Definición 10. - Se llama anillo, y se denota por $[A,*,\otimes]$, a un conjunto A dotado de dos operaciones " * " y "$\otimes$" que verifica las siguientes:

1. $[A, *]$ es un grupo abeliano, su elemento neutro lo denotaremos como 0.
2. $(a \otimes b) \otimes c = a \otimes (b \otimes c) \quad \forall a, b \in A \quad (propiedad\ asociativa)$
3. $\begin{cases} a \otimes (b * c) = (a \otimes b) * (a \otimes c) \\ (a \otimes b) * c = (a * c) \otimes (b * c) \end{cases} \quad \forall a, b \in A$ (propiedad distributiva)

Definición 11. - Un anillo $[A,*,\otimes]$, se llamará anillo unitario si verifica:

$$\exists\, e \in A \,/\, a \otimes e = e \otimes a \,, \qquad \forall a \in A$$

Definición 12. - Un anillo $[A,*,\otimes]$, se llamará anillo conmutativo si verifica:

$$a \otimes b = b \otimes a \, , \forall a, b \in A$$

Definición 13. - En un anillo $[A,*,\otimes]$, se dice que un elemento $a \in A$ no nulo es un divisor de cero si existe otro elemento no nulo $b \in A$ tal que:

$$a \otimes b = 0$$

Definición 14. - Un anillo conmutativo $[A,*]$, se dice que es un Dominio Integro si

$$a * b = 0 \iff a = 0 \quad o \quad b = 0$$

2.8. CUERPOS

Definición 15. - Se llama cuerpo a un anillo unitario $[A,*,\otimes]$, tal que $[A - \{0\},\otimes]$ es un grupo, es decir todo elemento $a \in A$ distinto de 0 es inversible respecto de $\otimes$. Si el anillo $[A,*,\otimes]$ es conmutativo, se dice que el cuerpo A es conmutativo.

2.9. DIVISIBILIDAD

Sean a y b dos números enteros tales que $a \neq 0$. Diremos que a divide a b si existe un numero entero q tal que $b = a.q$. Suele notarse $a|b$, es decir,

$$a|b \Leftrightarrow \exists \, q \in \mathbb{Z}: b = aq$$

Expresiones equivalentes a "a divide a b" son "a es un divisor de b" o "b es multiplo de a" o "b es divisible por a".

Nota. – Es importante recalcar que la suma y el producto de números enteros son operaciones asociativas y conmutativas, que $\{\mathbb{Z},+\}$ es grupo abeliano y que se satisface la propiedad distributiva del producto respecto a la suma, por lo que $\{\mathbb{Z},+,\cdot\}$ es un anillo conmutativo con elemento unidad (el 1) y sin divisores de cero.

Propiedades

Sean a, b y c tres números enteros, siendo a y b distintos de cero. Se verifica:

(i) 1 divide a "a" y "a" divide a cero (0).

(ii) Si "a" divide a "b" y "b" divide a "a" , entonces $a = \pm b$.

(iii) Si "a" divide a "b" y "b" divide a "c", entonces "a" divide a "c".

(iv) Si "a" divide a "b" y "a" divide a "c", entonces "a" divide a $pb + qc$, cualesquiera que sean p y q, enteros. (A la expresión $pb + qc$ se le llama combinación lineal de b y c con coeficientes enteros).

<u>Demostración:</u>

(i) $1|a$ y $a|0$, en efecto:

$$a = 1.a\,, \quad \text{con } a \in \mathbb{Z}\,, \quad \text{luego } 1|a$$

$$0 = a.0\,, \quad \text{con } 0 \in \mathbb{Z}\,, \quad \text{luego } a|0$$

(ii) $a|b$ y $b|a \;\Rightarrow a = \pm b, \forall\, a, b \in \mathbb{Z}\backslash\{0\}$, en efecto:

$$\left.\begin{array}{l} a|b \Leftrightarrow \exists p \in \mathbb{Z}: b = ap \\ \qquad\qquad \wedge \\ b|a \Leftrightarrow \exists q \in \mathbb{Z}: a = bq \end{array}\right\} \Rightarrow b = bqp \Rightarrow b(1 - qp) = 0$$

y al ser $b \neq 0$ y no tener $\mathbb{Z}$ divisores de cero, se sigue que:

$$1 - pq = 0 \Rightarrow pq = 1 \Rightarrow \begin{cases} p = q = 1 \\ \quad \vee \\ p = q = -1 \end{cases}$$

luego,

$$\left.\begin{array}{l}\left.\begin{array}{l} b = ap \\ a = bq \\ p = q = 1 \end{array}\right\} \Rightarrow a = b \\ \vee \\ \left.\begin{array}{l} b = ap \\ a = bq \\ p = q = -1 \end{array}\right\} \Rightarrow a = -b \end{array}\right\} \Rightarrow a = \pm b$$

(iii) $a|b$ y $b|c \Rightarrow a|c$, en efecto,

$$\left.\begin{array}{l} a|b \Leftrightarrow \exists p \in \mathbb{Z}: b = ap \\ \wedge \\ b|c \Leftrightarrow \exists q \in \mathbb{Z}: c = bq \end{array}\right\} \Rightarrow c = apq$$

con $pq \in \mathbb{Z}$, luego

$$a|c$$

(iv) $a|b$ y $a|c \Rightarrow a|pb + qc, \forall\, p, q \in \mathbb{Z}$

En efecto,

$$\left.\begin{array}{l} a|b \Leftrightarrow \exists s \in \mathbb{Z}: b = as \Rightarrow pb = pas \\ \wedge \\ a|c \Leftrightarrow \exists t \in \mathbb{Z}: c = at \Rightarrow qc = qat \end{array}\right\} \Rightarrow pb + qc = a(ps + qt)$$

siendo $ps + qt \in \mathbb{Z}$, luego

$$a|pb + qc$$

2.10. MÁXICO COMÚN DIVISOR

En esta parte se centrará la atención en los divisores comunes de un par de números enteros.

2.10.1. Divisor Común

Dados dos números enteros a y b, diremos que el entero $d \neq 0$, es un divisor común de ambos, si divide a "a" y divide a "b", es decir,

$d \neq 0$, es divisor común de a y $b \Leftrightarrow d|a$ y $d|b$

Obsérvese que es lo mismo que decir que a y b son divisibles por d o que a y b son multiplos de d.

2.10.2. Máximo Común Divisor

Sean a y b dos números enteros. Diremos que d es el máximo común divisor de a y b, si d es el máximo del conjunto de os divisores positivos comunes de ambos, ordenado por la relación de divisibilidad. A partir de aquí lo denotaremos como $(a, b) = d$ y se leerá: El máximo común divisor de "a" y "b" es "d".

Teniendo en cuenta la definición de máximo de un conjunto ordenado, si llamamos D al conjunto de todos los divisores positivos comunes a "a" y a "b", tendremos:

$$d = (a, b) \Leftrightarrow \begin{cases} i)\ d|a \wedge d|b \\ \wedge \\ ii)\ d = máx(D) \end{cases}$$

$$\Leftrightarrow \begin{cases} i)\ d|a \wedge d|b \\ \wedge \\ ii)\ \forall c, c \in D \Rightarrow c|d \end{cases}$$

$$\Leftrightarrow \begin{cases} i)\ d|a \wedge d|b \\ \wedge \\ ii)\ c|a \wedge c|b \ \Rightarrow\ c|d \end{cases}$$

Si $a = b = 0$, entonces $(a, b) = 0$.

Propiedades

Sean a y b dos números enteros distintos de cero. Se verifica:

I. $(a, 0) = |a|$

II. $(a, b) = (|a|, |b|)$

Demostración:

I. $(a,0) = |a|, \forall a \in \mathbb{Z}\backslash\{0\}$.

En efecto, el máximo común divisor de a y 0 es, por definición, el máximo del conjunto de divisores comunes a a y a 0 ordenado por la relación de divisibilidad. Ahora bien, como todos los números enteros son divisores de cero, el citado conjunto estará formado, únicamente, por los divisores de a y el mayor divisor de a es el propio a, luego

$$(a,0) = a$$

y al ser el máximo común divisor mayor que cero, tomamos

$(a,0) = a$, si $a > 0 \ \wedge \ (a,0) = -a$, si $a < 0$

es decir, $(a,0) = |a|$

II. $(a,b) = (|a|,|b|)$.

En efecto, sea d un divisor de a y de b. Como a y b son distintos de cero, pueden ocurrir cuatro casos

1) $a < 0$ y $b > 0$. Entonces,

$$d|a \wedge d|b \Rightarrow d|-a \wedge d|b \Rightarrow d||a| \wedge d||b|$$

2) $a > 0$ y $b < 0$. Entonces,

$$d|a \wedge d|b \Rightarrow d|a \wedge d|-b \Rightarrow d||a| \wedge d||b|$$

3) $a < 0$ y $b < 0$. Entonces,

$$d|a \wedge d|b \Rightarrow d|-a \wedge d|-b \Rightarrow d||a| \wedge d||b|$$

4) $a > 0$ y $b > 0$. Entonces,

$$d|a \wedge d|b \Rightarrow d||a| \wedge d||b|$$

Luego, en cualquier caso, el conjunto de los divisores comunes a "a" y a "b" coincide con el de los divisores comunes a $|a|$ y a $|b|$, por lo tanto, el máximo común divisor será el mismo, es decir,

$$(a, b) = (|a|, |b|)$$

Obsérvese que si a y b son enteros positivos, esto es lo mismo que decir que

$$(-a, b) = (a, -b) = (-a, -b) = (a, b)$$

2.10.3. Máximo Común Divisor de Varios Números

Sean $a_1, a_2, \dots, a_n$ números enteros. Se llamará máximo común divisor de $a_1, a_2, \dots, a_n$ al divisor común $d > 0$ tal que cualquier otro divisor común de $a_1, a_2, \dots, a_n$ divide también a d. Se designará mediante $d = (a_1, a_2, \dots, a_n)$.

Nota. – Nos planteamos ahora las siguientes cuestiones:

1. Dados dos números enteros a y b, ¿existe siempre su máximo común divisor? Caso de que la respuesta sea afirmativa, ¿Cómo se hallara dicho número?

2. ¿Cuántos máximo común divisor pueden tener un par de números enteros?

El siguiente teorema responde a ambas preguntas demostrando la existencia y unicidad del máximo común divisor de dos números enteros.

2.10.4. Existencia y Unicidad del m.c.d.

Dados dos números enteros a y b distintos de cero, existe un único d, que es el máximo común divisor de ambos.

Demostración:

Supondremos que a y $b \in \mathbb{Z}^+$, ya que según hemos visto en la **Propiedad (II)**, si uno de los dos o ambos fuera negativo, el máximo común divisor seria el mismo.

Existencia.

Sea C el conjunto de todas las combinaciones lineales positivas con coeficientes enteros que puedan formarse con a y b, es decir,

$$C = \{ma + nb \in \mathbb{Z}^+ : m, n \in \mathbb{Z}\}$$

C es no vacío. En efecto, como a es positivo, podemos escribirlo en la forma:

$$a = 1.a + 0.b$$

y, al menos, a estaría en C.

Así pues, C es un subconjunto no vacío de $\mathbb{Z}^+$y sabiendo que $\mathbb{Z}^+$, con la relación de orden "menor o igual" (relación de orden total) se afirma que $\mathbb{Z}^+$ está bien ordenado con la relación mencionada. Y además toda parte no vacía de $\mathbb{Z}^+$ tiene elemento mínimo o primer elemento. Entonces C ha de tener primer elemento o elemento mínimo llamado d.

Veamos que d es el máximo común divisor de a y b. En efecto,

$$d \in C \Rightarrow d = sa + tb, \text{ con } s \text{ y } t \text{ enteros}$$

Pues bien,

1. d es un divisor común de a y b.

Supongamos lo contrario, es decir d no es divisor de a ó d no es divisor de b. Entonces, si d no divide a a, por el teorema de existencia y unicidad del cociente y resto, podremos encontrar dos enteros q y r tales que:

$$a = dq + r, \text{ con } 0 < r < d$$

de aquí que

$$r = a - dq \Rightarrow r = a - (sa + tb)q \Rightarrow r = (1 - sq)a + (-tq)b > 0$$

con $1 - sq$ y $-tq$ enteros, luego r está en C.

Así pues, tenemos que:

$$r \in C \text{ y } r < d$$

lo cual contradice el que d sea el mínimo de C. Consecuentemente, la supocicion hecha es falsa y $d|a$.

Con un razonamiento idéntico, se prueba que $d|b$.

2. Veamos ahora que d es el máximo de los divisores comunes a a y b.

En efecto, si $c \in \mathbb{Z}$ es otro divisor común de a y de b, entonces

$$\left.\begin{matrix} c|a \\ \wedge \\ c|b \end{matrix}\right\} \xRightarrow{Propiedad\ (iv)} c|ma + nb$$

cualesquiera que sean m y n enteros. En particular,

$$c|sa + tb$$

luego

$$c|d$$

De 1. Y 2. Se sigue que $d = (a, b)$.

Unicidad.

En efecto, supongamos que hubiese dos máximo común divisor de a y b, digamos d_1 y d_2.

Entonces,

$$\left.\begin{matrix} \left.\begin{matrix} d_1 = (a,b) \\ d_2\ es\ divisor\ común\ de\ a\ y\ b \end{matrix}\right\} \Rightarrow d_2|d_1 \\ \left.\begin{matrix} d_2 = (a,b) \\ d_1\ es\ divisor\ común\ de\ a\ y\ b \end{matrix}\right\} \Rightarrow d_1|d_2 \end{matrix}\right\} \xRightarrow{Propiedad\ (ii)} d_1 = d_2$$

ya que por definición d_1 y d_2 son mayores que cero.

Proposición

Si d es el menor entero positivo que puede escribirse como combinación lineal con coeficientes enteros de dos enteros dados a y b y es divisor común de ambos, entonces d es el máximo común divisor de a y de b,

Demostración

En efecto, supongamos que

$$d = pa + qb, \text{ con } p, q \in \mathbb{Z}$$

$$\wedge$$

$$d|a \text{ y } d|b$$

entonces,

1. d es divisor de a y de b. Directamente de la hipótesis.

2. d es el máximo. En efecto, sea c otro de los divisores comunes de a y b. Entonces,

$$\left.\begin{matrix} c|a \\ \wedge \\ c|b \end{matrix}\right\} \Rightarrow c|pa + qb, \text{con } p \text{ y } q \text{ enteros } \Rightarrow c|d$$

Por lo tanto $d = (a, b)$

Se muestra a continuación un corolario a la proposición anterior que en ele caso de que el máximo común divisor de a y b sea 1, se verifica el reciproco sin necesidad de añadirle ninguna hipótesis al numero d.

Corolario 1.-

Si a y b son dos enteros distintos de cero, entonces $1 = (a, b)$ si, y solo si existen dos números enteros p y q tales $pa + qb = 1$.

Demostración

($\Rightarrow$) Si $1 = (a, b)$, entonces, por teoría, si pueden encontrarse dos números enteros p y q tales que $pa + qb = 1$.

($\Leftarrow$) Sean p y q dos números enteros tales que $pa + qb = 1$. Como 1 s divisor de cualquier número entero, $1|a$ y $1|b$. Decimos $1 = (a, b)$

Otras Propiedades

Sean a y b dos números enteros. Se verifica:

(i) Si $d = (a, b)$, entonces $1 = (\frac{a}{d}, \frac{b}{d})$

(ii) $(ka, kb) = k.(a, b), \forall k \in \mathbb{Z}^+$

Demostración

(i) Si $d = (a, b)$, entonces $1 = (\frac{a}{d}, \frac{b}{d})$

En efecto,

$$d = (a, b) \Rightarrow \exists\, p, q \in \mathbb{Z}: pa + qb = d$$

$$\Rightarrow \exists\, p, q \in \mathbb{Z}: p\frac{a}{d} + q\frac{b}{d} = 1$$

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

(ii) $(ka, kb) = k.(a, b), \forall k \in \mathbb{Z}^+$

En efecto, supongamos que $d = (a, b)$. Entonces,

$$d = (a, b) \Rightarrow \exists\, p, q \in \mathbb{Z}: pa + qb = d$$

$$\Rightarrow \exists\, p, q \in \mathbb{Z}: pka + qkb = kd$$

Veamos que kd es el máximo común divisor de ka y kb.

1. kd es divisor de ka y kb.

En efecto,

$$\left.\begin{array}{l} c|ka \\ \wedge \\ c|kb \end{array}\right\} \Rightarrow c|pka + qkb \text{ con } p, q \in \mathbb{Z} \Rightarrow c|kd$$

Luego,

$$(ka, kb) = k.d = k.(a, b)$$

(González Gutiérrez, 2004)

CAPÍTULO III

MARCO TEÓRICO

Presentamos, en este capítulo, las definiciones, teoremas necesarias y básicas relacionadas con los polinomios de manera formal, así como resultados de congruencias con polinomio, para lo cual se ha considerado como referencias De Nápoli, P. (2014), Moreno, H. (2013), Sánchez, C. M. (2014), Rivero, (s/f), Mateos, (s/f)

3.1. DEFINICIÓN DE POLINOMIOS

Sea A un anillo conmutativo. Un polinomio en una variable indeterminada "x" con coeficientes en el anillo A es una expresión formal de la forma:

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

donde los $a_i \in A$, llamados **coeficientes** del polinomio $P(x), n \in \mathbb{N}$

Si $a_n \neq 0$ diremos que a_n es el coeficiente principal de $P(x)$.

Si $a_n = 1$, entonces $P(x)$ es llamado **Polinomio Mónico.**

Denotamos $A[x]$ como el conjunto de todos los posibles polinomios en la variable "x" con coeficientes en el anillo A.

Se concluye: $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$.

Existen polinomios importantes como: el **Polinomio Nulo**, que tiene a todos sus coeficientes a_i igual a cero, la noción de grado para un polinomio nulo no está definida.

Otro polinomio importante, es el polinomio constante, de la forma $a_0 x^0$ donde $a_0 \in A$, es decir que $a_i = 0 \ \ si\ i > 0$, con grado igual a cero, si $a_0 \neq 0$.

Si identificamos $a_0 \in A$ con el polinomio constante $a_0x^0 \in A[x]$, pensamos que:

$$A \subset A[X]$$

Evaluación de polinomios

Consideremos un polinomio $P(x) \in A[x]$, , $y\ b \in A$ entonces el valor de $P(x)$ cuando $x = b$ se le define como

$$P(b) = \sum_{i=0}^{n} a_i . b^i$$

como el elemento de A que se obtiene al reemplazar el x por el valor b y efectuamos las operaciones necesarias del anillo, luego $P(b) \in A$.

3.2. OPERACIONES CON POLINOMIOS

Definición 16. - Sea $P(x) = \sum_{i=0}^{m} a_i x^i , Q(x) = \sum_{j=0}^{n} b_j x^j$ dos elementos de $A[x]$, y supongamos que $m \leq n$, se define la suma de los polinomios $P(x)\ y\ Q(x)$ como el polinomio

$$P(x) + Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_{m+1}x^{m+1} + (a_m + b_m)x^m + \cdots$$
$$+ (a_1 + b_1)x + (a_0 + b_0) \in A[x]$$

Definición 17. - Sea $k \in \mathbb{N}$, $P(x) = \sum_{i=0}^{m} a_i x^i , Q(x) = b_k x^k$ elementos de $A[x]$, se define el producto de $P(x)\ y\ Q(x)$ como el polinomio

$$P(x).Q(x) = a_n b_k x^{k+n} + \cdots + a_1 b_k x^{k+1} + a_0 b_k x^k \in A[x]$$

Si $P(x) = \sum_{i=0}^{m} a_i x^i$, $Q(x) = \sum_{j=0}^{n} b_j x^j$ definimos el producto de $P(x)\ y\ Q(x)$ como el polinomio

$$P(x).Q(x) = P(x).Q_k(x) + \cdots + P(x).Q_1(x) + P(x).Q_0(x) \in A[x]$$

donde $Q_k(x) = b_k x^k$

Teorema 4. - Las operaciones en las definiciones 16 y 17 satisfacen las siguientes propiedades:

- La suma de polinomios es asociativa, es decir

$$P(x) + \big(Q(x) + R(x)\big) = \big(P(x) + Q(x)\big) + R(x)$$

- La suma de polinomios es conmutativa, es decir

$$P(x) + Q(x) = Q(x) + P(x)$$

- La suma tiene un elemento neutro, denotado por $P(x) = 0$
- Dado $P(x) \in A[x]$ existe $Q(x) \in A[x]$ tal que $P(x) + Q(x) = 0$, denotaremos como $-P(x) \in A[x]$.
- El producto de polinomios es asociativa, es decir

$$P(x).\big(Q(x).R(x)\big) = \big(P(x).Q(x)\big).R(x)$$

- El producto de polinomios es conmutativa, es decir

$$P(x).Q(x) = Q(x).P(x)$$

- El producto tiene un elemento neutro, denotado por $P(x) = 1$
- El producto es distributivo con respecto a la suma, es decir

$$P(x).\big(Q(x) + R(x)\big) = P(x).Q(x) + P(x).R(x)$$

Estos resultados nos dicen que Si A es un anillo conmutativo, entonces $A[x]$ también es un anillo conmutativo; además, podemos identificar A como los elementos de $A[x]$ de la forma $P(x) = a$ en esta situación A es un subanillo de $A[x]$.

Definición 18. - Sea A un anillo y $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in A[x]$

i) Si $a_n \neq 0$ entonces diremos que el polinomio $P(x)$ tiene grado "n". Nótese que no se ha definido el grado del polinomio 0. En ocasiones, consideraremos que el grado del polinomio es -1.

ii) Al elemento $a_k \in A$ se le llama coeficiente de grado k, y a la expresión $a_k x^k$, término de grado k.

iii) La expresión $a_n x^n$ se le llama término principal y a "a_n" se le llama coeficiente principal.

iv) El coeficiente de grado 0 de un polinomio se le llama término independiente.

v) Un polinomio que, bien tiene grado 0, o bien es el polinomio 0 se dice que es un polinomio constante.

Teorema 5. - Sean $P(x), Q(x) \in A[x]$, entonces

$$gr\big(P(x) + Q(x)\big) \leq max\{gr\big(P(x), Q(x)\big)\}$$

$$gr\big(P(x).Q(x)\big) \leq gr\big(P(x)\big) + gr\big(Q(x)\big)$$

En particular, si el anillo A es un dominio íntegro, se tiene

$$P(x).Q(x) = 0 \; si \; y \; sólo \; si \; P(x) = 0 \quad o \quad Q(x) = 0$$

es decir que $A[X]$ resulta a su vez un dominio íntegro, además

$$gr\big(P(x).Q(x)\big) = gr\big(P(x)\big) + gr\big(Q(x)\big)$$

3.3. RAÍCES DE UN POLINOMIO

El anillo de coeficientes A es un cuerpo, y lo representaremos con K , tal como $K = \mathbb{Q}$, $K = \mathbb{R}$ ó $K = \mathbb{C}$, que son los cuerpos más usados

Definición 19. - Sea $P(x) \in K[x]$ un polinomio y $b \in K$, diremos que b es un **cero** o una **raíz** de $P(x) \; si \; P(b) = 0$.

Teorema 6. - Un polinomio de grado 1, $P(x) = ax + b$, siempre tiene una única raíz igual a

$$-\frac{b}{a}$$

Demostración.

$P(x) = ax + b \in K[x]$ tiene como raíz a $-\frac{b}{a}$, en efecto,

$$P\left(-\frac{b}{a}\right) = a\left(-\frac{b}{a}\right) + b = -a.\frac{b}{a} + b = -b + b = 0$$

A continuación, se presentará el teorema de Bolzano, que nos da un método para probar la existencia de soluciones de ecuaciones escalares en una variable.

Teorema 7. (Teorema de Bolzano) Sean $a, b \in K$ con $a < b$ y $P(x) \in K[x]$ un polinomio, que también es función continua, que satisface $P(a) < 0 < P(b)$. Entonces $\exists c \in]a; b[$ tal que $P(c) = 0$.

Demostración.

Consideremos el conjunto $C = \{x \in [a; b] \ / \ P(x) < 0\} \neq \emptyset$, pues $a \in C$, y es acotado, tomando $c = \sup C$, luego $c \in [a; b]$ y la demostración se concluirá probando que $P(c) = 0$, pues ello también implicará que $c \neq a \ \ y \ \ c \neq b$. Si determinamos que $P(c) < 0$ y $P(c) > 0$,se tendría contradicción.

Supongamos que $P(c) < 0$, como $P(x)$ es continua en el punto c, la propiedad de conservación del signo nos proporciona un $\delta > 0$ verificando que, para $x \in [a; b]$ con $|x - c| < \delta$ se tiene $P(x) < 0$. Utilizando esto es claro que $b \geq c + \delta$, pues en otro caso sería $|b - c| = b - c < \delta$ y entonces tendríamos $P(x) < 0$ contradicción a la hipótesis..

Luego $x \in]c, c+\delta[$ tenemos $x \in [a;b]$ y $|x-c| = x-c < \delta$ por tanto $P(x) < 0$ y $x \in C$, esto es una contradicción, ya que $x > c = \sup C$.

Supongamos entonces que $P(x) > 0$ por tanto $c \notin C$. Aplicando de nuevo la conservación del signo obtenemos $\delta > 0$, tal que $P(x) > 0$ siempre que $x \in [a;b]$ verifique $|x-c| < \delta$. Entonces, para $x \in C$ se deberá tener $\delta \leq |x-c| = c-x$ (porque sino, no se verificaría la propiedad de conservación del signo puesto que $x \in C$, de donde $x \leq c-\delta$. Obtenemos así que $c-\delta$ es mayor que C, lo cual es una contradicción, pues $c-\delta \leq c = \sup C$.

El *Teorema 7* es cierto si $P(a) > 0 > P(b)$, para esto basta tomar $-P(x)$ en lugar de $P(x)$, y aplicar el *Teorema 7*.

Teorema 8. - Si $P(x) \in \mathbb{R}[X]$ es un polinomio de grado impar, entonces $P(x)$ debe tener alguna raíz real.

Demostración:

Si $P(x)$ es de grado impar y su coeficiente principal a_n es positivo se tiene:

$$\lim_{x \to +\infty} P(x) = +\infty$$

$$\lim_{x \to -\infty} P(x) = -\infty$$

(Si $a_n < 0$, la situación es inversa). En consecuencia, P debe cambiar de signo (esto es: existen $a, b \in \mathbb{R}$ tales que $P(a) < 0\ y\ P(b) > 0$); y entonces, como $P(x)$ es una función continua de la variable real x, por el teorema de Bolzano debe existir algún $\alpha \in [a, b]$ tal que $P(\alpha) = 0$.

3.4. DIVISIBILIDAD DE POLINOMIOS

En el conjunto de polinomios $A[X]$ se ha definido las operaciones de adición y multiplicación, entonces se tiene la divisibilidad o factorización, tal como se realiza con los números enteros.

La factorización de polinomios, está en estrecha relación con el problema de encontrar las raíces o ceros de un polinomio.

Definición 20. - Sean $P(x), Q(x) \in K[x]$, diremos que $P(x)\ divide\ a\ Q(x)$, y lo escribiremos $P(x) \mid Q(x)$, si existe un polinomio $S(x)$ en K[x] tal que $Q(x) = P(x).S(x)$.

Definición 21. - Sea $P(x) \in K[x]$ un polinomio no constante, diremos que el polinomio $P(x)$ es irreducible en $K[x]$ si no es posible factorizarlo en la forma $P(x) = Q(x).S(x)$ donde $Q(x)\ y\ S(x)$ son polinomios en $K[x]$ no contantes.

3.5. EL ALGORITMO DE DIVISIÓN PARA POLINOMIOS

Teorema 9. - Sea $P(x),\ D(x) \in K[x]$ con $D(x) \neq 0$, existen únicos polinomios $Q(x)$: $cociente$, $y\ R(x)$: $resto$ de la división de polinomios de $P(x)$ por $D(x)$, tales que

$$P(x) = Q(x).D(x) + R(x)$$

y $R(x) = 0$ o $gr(R(x)) < gr(D(x))$.

<u>Demostración</u>

Existencia:

Si $P(x) = 0$ o si $gr\big(P(x)\big) = 0$: polinomios contantes, entonces basta considerar $Q(x) = 0$ y $R(x) = P(x)$.

Usando el método inductivo: Supongamos que $gr(P(x)) = n$ y que ya hemos demostrado el teorema cuando el grado del dividendo es menor que n.

Sean:

$$P(x) = \sum_{i=0}^{n} a_i x^i \qquad con\ \ a_n \neq 0\ \ , \qquad gr(P(x)) = n$$

$$D(x) = \sum_{j=0}^{m} b_j x^j \qquad con\ b_m \neq 0\ , \qquad gr(D(x)) = m$$

Si $n < m$, podemos tomar $Q(x) = 0\ \ y\ \ R(x) = P(x)$.

Supongamos que $n \geq m,$ entonces podemos determinar un primer cociente aproximado $Q_0(x)$, dividiendo el monomio principal de $P(x)$: $a_n x^n$, por el monomio principal $b_m x^m$ de $Q(x)$, obteniendo:

$$Q_0(x) = \frac{a_n}{b_m} x^{n-m}$$

Se ha usado el hecho de que en K podemos dividir, pues K es un cuerpo.

Entonces, definiendo $R_0(x) = P(x) - Q_0(x)D(x)$, obtenemos un primer resto aproximado.

Si fuera $R_0(x) = 0\ \ o\ \ gr(R_0(x)) < gr(D(x))$, hemos terminado: tomando

$Q(x) = Q_0(x)\ \ y\ \ R(x) = R_0(x)$.

Repitiendo el proceso, para lo cual se considera que $gr(R_0(x)) < gr(P(x))$, tal como se ha elegido $Q_0(x)$ los términos correspondientes a la potencia x^n se cancelan, entonces, por la hipótesis de inducción, existirán $Q_1(x)\ \ y\ \ R_1(x)$, cociente y resto respectivamente en la división de $R_0(x)$ por $D(x)$, de modo que:

$$R_0(x) = Q_1(x)D(x) + R_1(x)$$

donde $R_1(x) = 0 \;\; o \;\; gr(R_1(x)) < gr(D(x))$, entonces

$$\begin{aligned} P(x) &= Q_0(x)D(x) + R_0(x) \\ &= Q_0(x)D(x) + Q_1(x)D(x) + R_1(x) \\ &= \big(Q_0(x) + Q_1(x)\big)D(x) + R_1(x) \end{aligned}$$

haciendo $R(x) = R_1(x) \;\; y \;\; Q(x) = Q_0(x) + Q_1(x)$ lo que demuestra la existencia.

***Unicidad*:**

Supongamos que tenemos dos cocientes $Q(x) \;\; y \;\; \tilde{Q}(x)$, y dos restos $R(x) \;\; y \;\; \tilde{R}(x)$ tal que

$$P(x) = Q(x)D(x) + R(x) \quad y \quad R(x) = 0 \;\; o \;\; gr\big(R(x)\big) < gr(D(x))$$

$$P(x) = \tilde{Q}(x)D(x) + \tilde{R}(x) \quad y \quad \tilde{R}(x) = 0 \quad o \quad gr\left(\tilde{R}(x)\right) < gr(D(x))$$

Se tiene $Q(x)D(x) + R(x) = \tilde{Q}(x)D(x) + \tilde{R}(x) \Longrightarrow: \left(Q(x) - \tilde{Q}(x)\right)D(x) = \tilde{R}(x) - R(x)$

Si $R(x) = \tilde{R}(x)$ entonces $\left(Q(x) - \tilde{Q}(x)\right).D(x) = 0$, como $D(x) \neq 0, Q(x) = \tilde{Q}(x)$.

Probaremos que no puede suceder que $R(x) \neq \tilde{R}(x)$.

Pero si esto ocurriera, sería $R(x) - \tilde{R}(x) \neq 0, \;\; Q(x) - \tilde{Q}(x) \neq 0$ y comparando los grados obtenemos una contradicción pues:

$$gr\left[\left(Q(x) - \tilde{Q}(x)\right)D(x)\right] = gr(Q(x) - \tilde{Q}(x)) + gr(D(x)) \geq gr(D(x))$$

además

$$gr\big(\tilde{R}(x) - R(x)\big) \leq \max(gr\big(R(x)\big), gr\left(\tilde{R}(x)\right)) < gr(D(x))$$

esta contradicción se debió de haber supuesto que $R(x) \neq \tilde{R}(x)$, por tanto $R(x) = \tilde{R}(x)$, y $\;Q(x) = \tilde{Q}$(x).

3.6. EL TEOREMA DEL RESTO

Un caso importante de la división de polinomios, es la división de polinomios por polinomios de la forma x$-a$:

Teorema 10. (Teorema del Resto). El resto de la división de un polinomio $P(x) \in K[X]$ por $x - a,\ a \in K$, coincide con el valor $P(a)$.

Demostración:

Dividendo $P(x)$ por $x - a$ se tiene:

$$P(x) = Q(x).(x - a) + R(x)$$

donde el resto $R(x)$ debe ser un polinomio constante. Luego, evaluando en $x = a$, obtenemos que: $P(a) = R(a)$.

Corolario 2. - Sea $P(x) \in K[x]$ un polinomio, entonces $P(x)$ es divisible por $x - a,\ a \in K$ si y solo si a es raíz de $P(x)$.

Demostración:

Como $P(x)$ es divisible por $x - a$ entonces $\exists S(x) \in K[x]$ tal que $P(x) = (x - a).S(x)$ luego $P(a) = (a - a).S(a) = 0$, esto nos dice que $x = a$ es una raíz de $P(x)$.

Corolario 3. - Si un polinomio $P(x)$ es irreducible en $K[x]$, no puede tener raíces en K.

Corolario 4. - Si $P(x) \in K[x]$ es un polinomio de grado 2 o 3, entonces $P(x)$ es irreducible en $K[x]$ sí y solo si $P(x)$ no tiene raíces en K.

Demostración:

Por el *Corolario 3*, basta probar la afirmación recíproca, si $P(x)$ es irreducible, no puede tener raíces.

Pero si tuviéramos que $P(x) = R(x).S(x)$ con $R(x)$, $S(x)$ no constantes, entonces alguno de los factores $R(x)$ o $S(x)$ sería de primer grado, $pues\ gr\big(P(x)\big) = gr\big(R(x)\big) + gr(S(x)))$, y entonces $P(x)$ tendría una raíz.

Corolario 5. - Si $P(x) \in K[x]$ es un polinomio y $\alpha_1, \alpha_2, \dots, \alpha_r$ son raíces distintas de $P(x)$, entonces $P(x)$ admite la factorización:

$$P(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_r)Q(x)$$

Comparando los grados de ambos miembros en esta ecuación, obtenemos la siguiente consecuencia importante:

Corolario 6. - Si K es un cuerpo y $P(x) \in K[X]$ es un polinomio de grado n, $P(x)$ no puede tener más de n raíces en K.

Corolario 7. - Si K es un cuerpo infinito, y $P(x), Q(x) \in K[x]$ son dos polinomios que originan la misma función polinómica $f_P = f_Q\ \ o\ \ sea\ P(a) = Q(a)$ para todo $a \in K$, luego son iguales. En efecto, $P(x) - Q(x)$ debe anularse para todos los elementos de K y como K es infinito, por el corolario anterior; esto solo puede suceder si $P(x) - Q(x)$ es el polinomio nulo.

Corolario 8. - Si K es un cuerpo, y $P(x) \in K[x]$ es un polinomio de grado n

$$P(x) = \sum_{i=0}^{n} a_i x^i \ \ con\ a_n \neq 0$$

que tiene exactamente n raíces distintas $\alpha_1, \alpha_2, \dots, \alpha_r$ en K, se tiene que:

$$P(x) = a_n(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_r)Q(x)$$

siendo a_n el coeficiente principal de $P(x)$.

Demostración

Por el *Corolario 5*, $Q(x)$ debe ser de grado cero, es decir un polinomio constante. Igualando entonces los coeficientes principales, vemos que $Q(x) = a_n$.

3.7. RAÍCES RACIONALES

En general, para polinomios de grado alto, no existe un método general para determinar sus raíces, pero para polinomios de coeficientes reales, existen métodos numéricos para determinarlas aproximadamente con tanta precisión como se desee, lo cual es suficiente para cualquier aplicación práctica.

Sin embargo, existe un método general para determinar todas las posibles raíces racionales de un polinomio con coeficientes racionales. Sea $P(x) \in \mathbb{Q}[x]$:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \quad con \quad a_i \in \mathbb{Q}$$

Multiplicando a $P(x)$ por el mínimo común múltiplo de los denominadores de los a_i, podemos suponer que todos sus coeficientes son enteros, es decir que $P(x) \in \mathbb{Z}[X]$. Entonces, se tiene el siguiente teorema:

3.7.1. Criterio de Gauss

Si $P \in \mathbb{Z}[X]$ y $a = \frac{p}{q} \in \mathbb{Q}$ es una raíz racional de $P(x)$, escrita como fracción irreducible, $p \ y \ q$ coprimos, se tiene que $p \mid a_0$ y $q \mid a_n$.

En particular, si P es Mónico, las posibles raíces racionales de $P(x)$ deben ser enteras.

Demostración:

Como $P(a) = 0$, tendremos:

$$a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \cdots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n = 0$$

luego:

$$p(a_n p^{n-1} + a_{n-1}p^{n-2}q + a_{n-2}p^{n-3}q^2 + \cdots + a_2 pq^{n-1} + a_1 q^{n-1}) = -a_0 q^n$$

en particular:

$$p \mid a_0 q^n$$

Pero como p es coprimo con q, p es coprimo con q^n, por el teorema fundamental de la aritmética. Por lo tanto, p debe dividir a a_0.

Similarmente:

$$q(a_{n-1} p^{n-1} + a_{n-2}p^{n-2}q + \cdots + a_2 p^2 q^{n-3} + a_1 pq^{n-2} + a_0 q^{n-1}) = -a_n q^n$$

por lo tanto

$$q \mid a_n p^n$$

pero como q es coprimo con p, q es coprimo con p^n; y, en consecuencia, $q \mid a_n$.

3.8. MULTIPLICIDAD DE RAÍCES

Definición 22. - Sea $P(x) \in K[x]$ un polinomio, y sea $a \in K$ una raíz de $P(x)$. Decimos que a es una raíz de $P(x)$ de multiplicidad m $(m \in \mathbb{N})$ si $P(x)$ admite la factorización:

$$P(x) = (x-a)^m Q(x)$$

donde el polinomio $Q(x)$ no se anula en $x = a$, o sea $Q(a) \neq 0$.

Si $m = 1$, entonces a es una raíz simple, si $m = 2$ que es doble, etc.

Teorema 11. - Si $P(x)$ es un polinomio que tiene en K las raíces: $a_1, a_2, \ldots, a_r$ con multiplicidades $m_1, m_2, \ldots, m_r$, respectivamente, entonces $P(x)$ admite la factorización

$$P(x) = (x-a_1)^{m_1}(x-a_2)^{m_2} \ldots (x-a_r)^{m_r} Q(x)$$

donde $Q(a_i) \neq 0$ para $0 \leq i \leq r$.

Veremos a continuación otra caracterización de la multiplicidad de las raíces. Para ello, necesitaremos introducir el concepto de derivada de un polinomio. Si $K = \mathbb{R}$, este concepto coincidirá con el concepto de derivada visto en los cursos de análisis. Sin embargo, en un cuerpo cualquiera K es posible introducir este concepto de una manera totalmente algebraica, sin referencia alguna a conceptos analíticos.

Definición 20. - Sea $P(x) \in K[x]$ un polinomio.

$$P(x) = \sum_{k=0}^{n} a_k x^k$$

entonces, definimos el polinomio derivado $P'(x)$ por:

$$P'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

Teorema 12. - (**La fórmula de Taylor para Polinomios).** Si $P \in K[X]$ es un polinomio con $gr(P) \leq n$ y $a \in K$, tenemos que:

$$P(x) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(x-a)^k$$

<u>Demostración:</u> Para demostrar la fórmula de Taylor, primero la demostramos para monomios de la forma $P(x) = x^m$. En este caso las derivadas de $P(x)$ son:

$$P'(x) = mx^{m-1}$$

$$P^{(2)}(x) = m(m-1)x^{m-2}$$

$$P^{(3)}(x) = m(m-1)(m-2)x^{m-3}$$

y siguiendo de esta manera, se induce que:

$$P^{(k)}(x) = m(m-1)(m-2)\ldots(m-k+1)x^{m-k} \quad si \quad k \leq m$$

mientras que

$$P^{(k)}(x) = 0 \quad si \;\; k > m$$

usando la expresión de los números combinatorios:

$$\binom{m}{k} = \frac{m(m-1)(m-2)\dots(m-k+1)}{k!}\,, \qquad (0 \le k \le m)$$

y el teorema del binomio de Newton, vemos que:

$$\sum_{k=0}^{m} \frac{P^{(k)}(a)}{k!}(x-a)^k = \sum_{k=0}^{m} \binom{m}{k} a^k (x-a)^{m-k} = (a+(x-a))^m = x^m$$

3.9. TEOREMA FUNDAMENTAL DEL ALGEBRA

Todo polinomio de grado *"n"*, con coeficientes complejos, tiene exactamente *"n"* raíces, no forzosamente distintas, es decir contadas con su orden de multiplicidad (cuantas veces un número es raíz de un polinomio).

Así, todo polinomio con coeficiente complejos $P(x) \in \mathbb{C}[X]$ no constante, tiene alguna raíz en el cuerpo de los números complejos, es decir existe $\alpha \in \mathbb{C}$ tal que $P(\alpha) = 0$.

Corolario 8. - Todo Polinomio con coeficientes complejos

$$P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[X] \qquad a_i \in \mathbb{C}, \;\; a_n \neq 0$$

no constante se factoriza como producto de polinomios lineales, en la forma:

$$P(x) = a_n(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\dots(x-\alpha_r)^{m_r}$$

donde $\alpha_1, \alpha_2, \dots, \alpha_r$ son las distintas raíces complejas de $P(x)$,

$m_1, m_2, \dots, m_r$ son las correspondientes multiplicidades y

α_n es el coeficiente principal del polinomio $P(x)$.

Demostración:

Por el Teorema 11.

$$P(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \dots (x - \alpha_r)^{m_r}.Q(x)$$

donde $Q(\alpha_1) \neq 0$ para $0 \leq i \leq r$.

Demostraremos que $Q(x)$ debe ser constante: supongamos que no, por el Teorema Fundamental del Algebra, $Q(x)$ debe tener alguna raíz $\alpha \in \mathbb{C}$, pero toda raíz de $Q(x)$ es raíz de $P(x)$. Luego $\alpha = \alpha_i$ para algún i, lo que es una contradicción pues $Q(\alpha_i) \neq 0$.

Como $Q(x)$ debe ser constante, al igualar los coeficientes principales de ambos miembros, deducimos que $Q(x)$ debe coincidir con el coeficiente principal de $P(x)$.

Comparando los grados de ambos miembros, en la descomposición del corolario anterior deducimos que:

$$n = gr(P) = m_1 + m_2 + \cdots + m_r$$

La suma representa la cantidad de raíces de $P(x)$, si contamos las raíces múltiples de acuerdo con su multiplicidad.

Corolario 9. Un polinomio $P(x) \in \mathbb{C}[x]$ tiene exactamente n raíces complejas, si las contamos de acuerdo con su multiplicidad.

En particular, hemos demostrado que en $\mathbb{C}[X]$ los únicos polinomios irreducibles son los lineales.

3.10. RAÍCES COMPLEJAS DE POLINOMIOS REALES

Definición 24. - Si $z = a + bi \in \mathbb{C}$ entonces su complejo conjugado $\bar{z}$ se define por $\bar{z} = a - bi \in \mathbb{C}$.

Teorema 13. - El complejo conjugado satisface las siguientes propiedades:

1. $z = \bar{z}$ sí y solo si $z \in \mathbb{R}$.
2. Si $z, w \in \mathbb{C}$ entonces

$$\overline{z + w} = \bar{z} + \bar{w}$$

$$\overline{z.w} = \bar{z}.\bar{w}$$

3. $z + \bar{z} = 2Re(z)$.
4. $z.\bar{z} = |z|^2$.

Sabemos que si $P(x) = ax^2 + bx + c$ es un polinomio cuadrático con coeficientes reales y discriminante $\Delta = b^2 - 4ac$ negativo, $P(x)$ tiene dos raices complejas conjugadas dadas por:

$$\alpha_1 = \frac{-b + \sqrt{-\Delta i}}{2a};\ \alpha_2 = \frac{-b - \sqrt{-\Delta i}}{2a}$$

las raíces complejas de un polinomio cuadrático forman un par de raíces conjugadas.

Generalizando a polinomios con coeficientes reales de mayor grado, para lo cual consideremos un polinomio con coeficientes complejos:

$$P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$$

y definimos el polinomio conjugado $\bar{P}(x)$ por

$$\bar{P}(x) = \sum_{i=0}^{n} \overline{a_i} x^i$$

Usando los resultados del Teorema 2.8.1. tenemos que:

$$\bar{P}(z) = \bar{P}(z)$$

Además, si $P(x), Q(x) \in \mathbb{C}[x]$ son polinomios:

$$\overline{P(x) + Q(x)} = \bar{P}(x) + \bar{Q}(x)$$

$$\overline{P(x).Q(x)} = \bar{P}(x).\bar{Q}(x)$$

En particular, si los coeficientes de $P(x)$ son reales (esto es $P(x) \in \mathbb{R}[x]$), tendremos que $\bar{P}(x) = P(x)$, y resulta que:

$$\overline{P(z)} = P(\bar{z})$$

En particular si $P(z) = 0$, tenemos que $P(\bar{z}) = 0$, es decir, hemos demostrado que las raices complejas de un polinomio con coeficientes reales se presentan de pares de raíces conjugadas:

Teorema 14. - Sea $P(x) \in \mathbb{R}[x]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de $P(x)$, entonces su complejo conjugado $z = a - bi$ también es raíz de $P(x)$.

Teorema 15. Sea $P(x) \in \mathbb{R}[x]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de $P(x)$ con multiplicidad m, entonces su complejo conjugado $z = a - bi$ también es raíz de $P(x)$ con multiplicidad m.

Demostración:

Como z es raíz de $P(x)$ de multiplicidad m, entonces $P(x)$ admite la factorización:

$$P(x) = (x - z)^m Q(x)$$

donde $Q(z) \neq 0$.

Tomando conjugado, tenemos:

$$\bar{P}(x) = \overline{(x - z)^m.Q(x)} = \overline{(x - z)^m}.\bar{Q}(x) = (x - \bar{z})^m.\bar{Q}(x)$$

Pero como P tiene coeficientes reales, $\bar{P}(x) = P(\mathrm{x})$ y como

$$P(\bar{z}) = 0, \quad \bar{Q}(\bar{z}) \neq 0$$

esto diremos que $\bar{z}$ es una raíz de $P(x)$ de multiplicidad m.

Sea $P(x) \in \mathbb{R}[x]$ y $\alpha_1, \alpha_2, \ldots \alpha_r$ sus raíces reales distintas, además consideremos sus raíces complejas con parte imaginaria no nula, que se presentan en pares de raíces conjugadas:

$$\beta_1, \overline{\beta_1},\ \beta_2, \overline{\beta_2}\ , \ldots\ \beta_S, \overline{\beta_S}$$

Por otra parte, llamemos m_i a la multiplicidad de α_i como raíz de $P(x)$ y f_i a la multiplicidad de β_i como raíz de $P(x)$ y también es la multiplicidad de $\overline{\beta_\iota}$, entonces: $P(x)$ admite en $\mathbb{C}[x]$ la factorización dada por:

$$P(x) = a_n(x-\alpha_1)^{m_1} \ldots (x-\alpha_r)^{m_r}(x-\beta_1)^{f_1}\left(x-\overline{\beta_1}\right)^{f_1}(x-\beta_2)^{f_2}\left(x-\overline{\beta_2}\right)^{f_2} \ldots (x - \beta_S)^{f_S}(x-\overline{\beta_S})^{f_S}$$

Para obtener su factorización en $\mathbb{R}[x]$, debemos agrupar los factores correspondientes a cada par de raíces conjugadas: para ello observamos que

$$Q_{\beta_i}(x) = (x-\beta_i)\left(x-\overline{\beta_\iota}\right) = x^2 - 2\,Re(\beta_i)x + |\beta_i|^2$$

es un polinomio cuadrático con coeficientes reales y discriminante negativo, pues no tiene raíces reales.

Con lo cual se obtiene

Teorema 16. - Si $P(x) \in \mathbb{R}[x]$ es un polinomio con coeficientes reales, entonces $P(x)$ admite la factorización:

$$P(x) = a_n(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2} \ldots (x-\alpha_r)^{m_r}.\, Q_{\beta_1}^{f_1}(x)Q_{\beta_2(x)} \ldots Q_{\beta_S}^{f_S}(x)$$

donde a_n es el coeficiente principal de $P(x)$, las α_i son las raíces reales de $P(x)$ y los $Q_{\beta_i}(x)$ son polinomios cuadráticos con coeficientes reales y discriminante negativo, correspondientes a cada par de raíces complejas de $P(x)$.

En particular, vemos que en $\mathbb{R}[x]$ los polinomios irreducibles son las lineales y los polinomios cuadráticos con discriminante negativo.

3.11. DEFINICIÓN DE CONGRUENCIA

Sea $m \in \mathbb{Z}^+$, diremos que dos enteros a y b son congruentes módulo m, y usamos la notación:

$$a \equiv b(mod\ m) \Leftrightarrow m \mid a - b$$

La definición anterior es equivalente a decir que "a es congruente a b módulo m si existe un entero k, tal que: $a = b + km$".

Cuando a y b no son congruentes módulo m, diremos que son **in-congruentes** y lo denotaremos por $a \not\equiv b(mod\ m)$.

Teorema 17.

Sean $a, b, c \in \mathbb{Z}$, entonces se tiene

1. $a \equiv a(mod\ m)$
2. Si $a \equiv b(mod\ m)$, entonces $b \equiv a(mod\ m)$.
3. Si $a \equiv b(mod\ m)$, y $b \equiv c(mod\ m)$, entonces $a \equiv c(mod\ m)$.

Demostración:

1. Sabemos que m divide a $0 = a - a$, por definición de congruencia se tiene

$$a \equiv a(mod\ m)$$

2. De $a \equiv b(mod\ m) \Leftrightarrow m|(b-a) \Leftrightarrow m|-(b-a) \Leftrightarrow m|(b-a) \Leftrightarrow b \equiv a(mod\ m)$.

3. Por hipótesis, se tiene

$$\begin{cases} a \equiv b(mod\ m) \Leftrightarrow m|(b-a) \\ b \equiv c(mod\ m) \Leftrightarrow m|(c-b) \end{cases} \Leftrightarrow m|(b-a)+(c-b) \Leftrightarrow m|(c-a) \Leftrightarrow a \equiv c(mod\ m) \quad \blacksquare$$

Los tres resultados del teorema nos dicen que relación de congruencia es una relación de equivalencia, generando de esta manera una partición en el conjunto de los enteros en clases de equivalencia disjuntas, las cuales llamaremos **clases de congruencia módulo m**.

Definición 25. -

Sea $a \in \mathbb{Z}$, entonces la clase de congruencia de a módulo m, es el conjunto

$$[a] = \{x\ entero\ /\ x \equiv a(mod\ m)\}$$

El entero a en la definición anterior se llama el **representante de la clase** y puede ser elegido arbitrariamente de entre los elementos de la clase: esto es, si $b \equiv a(mod\ m)$ entonces $[a] = [b]$.

Teorema 18. -

Si $a \equiv b(mod\ m)$, y $c \in \mathbb{Z}$, se cumple

1. $a + c \equiv b + c\ (mod\ m)$
2. $ac \equiv bc\ (mod\ m)$

Demostración:

1) Si $a \equiv b(mod\ m)$, se tendrá entonces $m|b-a$. Luego $m|(a+c)-(b+c)$, y de aquí obtenemos

$$a + c \equiv b + c\ (mod\ m)$$

2) Se tiene $m|a-b$, y por lo tanto $m|(a-b)c$. Luego $m|ac-bc$, lo cual implica

$$ac \equiv bc\ (mod\ m)$$

Teorema 19. - Sean $a, b, c \in \mathbb{Z}$ tales que.

$$a \equiv b\ (mod\ m)$$

$$c \equiv d\ (mod\ m)$$

entonces:

1. $a + c \equiv b + d\ (mod\ m)$
2. $ac \equiv bd\ (mod\ m)$
3. $ka \equiv kb\ (mod\ m),\ \forall k \in \mathbb{Z}$

Demostración:

1) Si

$$\begin{cases} a \equiv b\ (mod\ m) \Longrightarrow \exists k \in \mathbb{Z} : a = b + km \\ c \equiv d\ (mod\ m) \Longrightarrow \exists h \in \mathbb{Z} : c = d + hm \end{cases}$$, luego

$$a + c = b + d + (h + k)m$$

Por tanto

$$a + c \equiv b + d\ (mod\ m)$$

2) De la misma forma se tiene

$$ac = (b + km)(d + hm) = bd + (bh + dk + hkm)m$$

y de esto se sigue que $ac \equiv bd\ (mod\ m)$.

3) La demostración es inmediata, pues:

$$a \equiv b\ (mod\ m) \Leftrightarrow \exists r \in \mathbb{Z} : a = b + rm$$

$ka = kb + krm$, la igualdad se cumple para cualquier entero k

$$ka \equiv kb\ (mod\ m)\ \blacksquare$$

3.12. ENTEROS MÓDULO m

Consideremos $m \in \mathbb{Z}^+$, sea $\mathbb{Z}_m$ el conjunto cociente de $\mathbb{Z}$ respecto a la relación de congruencia módulo m , a la clase de equivalencia de un $a \in \mathbb{Z}$ se le denota por $[a]_m$ o simplemente $[a]$ modulo m, $\mathbb{Z}_m = \{[0]_m;\ [1]_m;\ \ldots;\ [m-1]_m\}$. sabiendo que $[i]_m$ representa al conjunto de todos los enteros que son congruentes con mod m. A este conjunto cociente se le conoce como el conjunto de restos o residuos (modulo m), también se le conoce con el nombre clases residuales modulo m.

Los enteros 0, 1, 2, … , *m* - 1 están en clases residuales distintas, todo entero se puede escribir de manera única en la forma $n = mq + r\ , con\ q \in \mathbb{Z}\ \ y\ \ 0 \leq r \leq m-1$, entonces existen *m* clase residuales modulo *m*; y cualquier conjunto de enteros incongruentes de módulo *m* constituyen un sistema residual completo

Teorema 20. - Si $\{a_1, \ldots,\ a_m\}$ es un sistema residual completo y $(k, m) = 1$, entonces el conjunto $\{ka_1, \ldots,\ ka_m\}$ también es un sistema residual completo.

Demostración:

Si $ka_i \equiv ka_j (mod\ m)$ entonces $m \mid k(a_i - a_j)$ pero como *k* y *m* son primos entre sí, se tiene $m \mid (a_i - a_j)$, es decir, que los ka_i son incongruentes entre si modulo *m* y por lo tanto forman un sistema residual completo.

3.12.1. Operaciones en $\mathbb{Z}_m$

En $\mathbb{Z}_m$ definimos dos operaciones la suma $+ : \mathbb{Z}_m x \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ y el producto $\cdot : \mathbb{Z}_m x \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ como

1. **Suma módulo** m,

$$[a] + [b] = [a + b]$$

2. **Producto módulo** m, definida por

$$[a] \cdot [b] = [a \, . \, b]$$

Demostraremos que estas operaciones están bien definidas, es decir, si sumamos dos clases usando distintos representantes se obtendrá el mismo resultado; en efecto, sean $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, tales que

$$[a_1] = [a_2] \quad \text{y} \quad [b_1] = [b_2]$$

$$\text{De} \begin{cases} [a_1] = [a_2] \implies a_1 \equiv a_2 \, mod \, m \\ [b_1] = [b_2] \implies b_1 \equiv b_2 \, mod \, m \end{cases} \implies a_1 + b_1 \equiv a_2 + b_2 \, mod \, m$$

$$\implies [a_1 + b_1] = [a_2 + b_2] \Leftrightarrow [a_1] + [b_1] = [a_2] + [b_2]$$

De igual manera, para el producto

$$[a_1] \cdot [b_1] = [a_2] \cdot [b_2]$$

Por tanto, la suma y el producto módulo m están bien definidas.

Teorema 21. - Sea $m \in \mathbb{Z}^+$, entonces el conjunto $\mathbb{Z}_m$ con las operaciones de suma y producto $módulo \, m$ es un anillo conmutativo con unidad.

Demostración:

La suma y el producto satisfacen las condiciones de las definiciones 10, 11 y 12, por tanto, es un anillo conmutativo con unidad.

Además

- $[0]$ es elemento neutro para $(\mathbb{Z}_m\ , +)$
- $[1]$ es el elemento neutro para $(\mathbb{Z}_m\ ,\ \cdot)$
- $-\ [a] = [-\ a]$ es elemento opuesto para $[a]$ en $(\mathbb{Z}_m\ , +)$

Satisface la propiedad cancelativa $[a] \cdot [c] = [b] \cdot [c]\ \Rightarrow [a] = [b]$ en $(\mathbb{Z}_m\ , +)$

Teorema 22. - Sea $m \in \mathbb{Z}^+$ y $(a, m) = d,\ e$ntonces si $ab \equiv ac\ mod\ m$, se tiene:

$$b \equiv c\ mod\ \frac{m}{d}$$

Demostración:

De $ab \equiv ac\ mod\ m\ \Leftrightarrow\ m|a(b-c)$, se tiene que $\frac{m}{d}$ divide a $\frac{a}{d(b-c)}$ y además $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$. Luego concluimos que $\frac{m}{d}$ divide a $b - c$, de donde se obtiene

$$b \equiv c\ \ mod\ \frac{m}{d} \qquad \blacksquare$$

Teorema 23. - Sea p un primo y $a \in \mathbb{Z}^+$, tal que $(p, a) = 1$, entonces si

$$ab \equiv ac\ mod\ p, \quad \text{se tiene} \quad b \equiv c\ mod\ p$$

Teorema 24. - El anillo de clases de congruencias $\mathbb{Z}_m$ es un cuerpo si y solo si m es primo.

3.13. ECUACIONES LINEALES DE CONGRUENCIA

Definición 26. - Sean $a, b \in \mathbb{Z}\ ,\ \ m \in \mathbb{Z}^+$, y $x \in \mathbb{Z}$ una variable, la ecuación de tipo

$$a.x \equiv b\ mod\ m$$

se llama ***ecuación lineal de congruencia***.

Teorema 25. - Si x_0 es solución de la ecuación que se presenta en la definición 25, y x_1 es otro entero tal que $x_1 \equiv x_0 \, mod \, m$, entonces x_1 también será solución de la ecuación.

Demostración:

Como x_0 es solución, entonces $a.x_0 \equiv b \, mod \, m$, además $x_1 \equiv x_0 \, mod \, m \implies x_0 = x_1 + km$ reemplazando en la ecuación dada se tiene

$$a.(x_1 + km) = b + rm \iff a.x_1 + a.km \equiv b + rm \iff a.x_1 \equiv b + rm - a.km$$

$$\iff a.x_1 \equiv b + (r - a.k)m \iff a.x_1 \equiv b + Km \iff a.x_1 \equiv b \, mod \, m \quad \blacksquare$$

De este teorema se deduce que la ecuación de la *Definición 25* posee solución, entonces posee infinitas. Sin embargo, solo nos interesan aquellas soluciones que no sean congruentes entre sí.

La ecuación de la *Definición 25* se puede expresar

$$a.x - m.y = b$$

donde y es un entero a determinar, esta ecuación se le conoce como ***ecuación lineal diofántica*** en las variables x e y. Las soluciones de esta ecuación son números enteros.

Teorema 26. - La ecuación diofántica

$$ax + by = c$$

tiene solución si y solo si $d|c$, donde $d = (a, b)$.

Demostración:

Sabemos que $d|a$, y $d|b$ .Si la ecuación tiene solución (x, y) se tiene que

$$d|(ax + by) \implies d|c$$

Recíprocamente, supongamos que $d|c$. Dividiendo entre d la ecuación original, nos da

$$a'.x + b'.y = c'$$

Donde $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ y $c' = \frac{c}{d}$, luego esta ecuación tiene solución, por tanto $ax + by = c$ también posee solución y viceversa, de aquí se tiene que ambas ecuaciones son equivalentes.

Si $(a', b') = 1$, entonces existen enteros x_0' e y_0' tales que:

$$a'x_0' + b'y_0' = 1$$

luego, $x_0 = c'x_0'$ e $y_0 = c'y_0'$ es solución de

$$a'.x + b'.y = c'$$

De donde se tiene que también es solución de $a.x + b.y = c$ ■

Teorema 27. - Si la ecuación lineal diofántica $a.x + b.y = c$ tiene solución y $(x_0.y_0)$ es una solución particular, entonces toda otra solución (x, y) es de la forma

$$x = x_0 + \frac{b}{d}t\ ,\ \ y = y_0 - \frac{a}{d}t$$

donde $t \in \mathbb{Z}$.

Demostración:

Demostremos que x e y son solución. En efecto

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t = ax_0 + by_0 = c$$

Por otro lado, si (x, y) es cualquier solución de $a.x + b.y = c$, también lo será de $a'.x + b'.y = c'$ y, en consecuencia

$$a'(x - x_0) + b'(y - y_0) = a'x - a'x_0 + b'y - b'y_0 = (a'x + b'y) - (a'x_0 + b'y_0)$$

$$= c' - c' = 0$$

de donde

$$a'(x - x_0) = -b'(y - y_0)$$

luego

$$a'|b'(y - y_0) \Longrightarrow a'|(y - y_0) \Leftrightarrow y = y_0 + a't, \;\; t \in \mathbb{Z}$$

análogamente para $x = x_0 + b's\,, \;\; t \in \mathbb{Z}$.

Probaremos que $s = -t$, sustituimos la solución (x, y) en $a'.x - b'.y = c'$

$$a'(x_0 + b's) + b'(y_0 + a't) = c'$$

$$a'x_0 + b'y_0 + a'b'(s + t) = c'$$

como (x_0, y_0) es solución de $a'.x - b'.y = c' \Longrightarrow a'x_0 + b'y_0 = c'$, y por lo tanto

$$c' + a'b'(s + t) = c' \Longrightarrow a'b'(s + t) = 0 \Longrightarrow s = -t \qquad \blacksquare$$

Teorema 28. - La ecuación lineal de congruencia

$$ax \equiv b \; mod \; m$$

posee solución si y solo si $d|b$, donde $d = (a, m)$. Si x_0 es una solución particular, entonces la solución general viene dada por

$$x \equiv x_0 \; mod \; \frac{m}{d}$$

<u>Demostración:</u>

La ecuación $ax \equiv b \; mod \; m \;\Leftrightarrow\; ax - my = b$, por el *Teorema 28*, sabemos que tiene solución, y además la solución general para la x viene expresada mediante:

$$x = x_0 + \frac{m}{d}t \;\Leftrightarrow\; x \equiv x_0 \; mod \; \frac{m}{d}$$

Como consecuencia se tiene que las d soluciones

$$x_0, x_0 + \frac{m}{d}, \dots, x_0 + \frac{(d-1)m}{d}$$

son todas distintas modulo m. ■

Ejemplo 1.- *Determinar si la siguiente ecuación de congruencia tiene solución, indicar cuantas raíces presenta y resolverla completamente:*

$$12x \equiv 20 \ (mod\ 8)$$

Solución:

Por el *Teorema 28*, la ecuación lineal de congruencia "$ax \equiv b\ mod\ m$", posee solución si y solo si $d|b$, donde $d = (a, m)$. En tal caso hay d soluciones y estas son de la forma:

$$x = \left[x_0 + \frac{m}{d}t\right] (mod\ m), \forall t \in 0, 1, 2, 3, \dots d-1$$

Siendo x_0 la solución de la ecuación:

$$\frac{a}{d}x_0 \equiv \frac{b}{d}\ (mod\ \frac{m}{d})$$

Para este ejercicio: $a = 12$, $b = 20$ y $m = 8$

Hacemos: $d = (12\ , 8) = 4$

Luego, como $d|b = 4 \mid 20$, entonces esta ecuación si tiene solución y el numero de raíces que presenta son $d = 4$ raices.

Hacemos: $d = (12\ , 8) = 4 \mid 20$. Por lo tanto, esta ecuación si tiene solución.

Luego, como $d = 4$, esta ecuación presenta 4 raíces.

Para determinar cuáles son las raíces, hacemos, por el *Teorema 22*, se plantea:

$$\frac{12}{4}x_0 \equiv \frac{20}{4}\left(mod\ \frac{8}{4}\right) = 3x_0 \equiv 5\ (mod\ 2)$$

$3x_0 \equiv 5\ (mod\ 2)$, por definición de congruencia se escribe: $3x_0 = 5 + 2k, k \in \mathbb{Z}^+$

$3x_0 = 5 + 4 + 2k \Rightarrow 3x_0 \equiv 9\ (mod\ 2)$, luego por el *Teorema 18 parte 2*:

$3x_0 \equiv 9\ (mod\ 2) = x_0 \equiv 3\ (mod\ 2)$, finalmente:

$$x = \left[3 + \frac{8}{4}t\right](mod\ 8), \forall t \in 0, 1, 2, \dots 4 - 1$$

Por lo tanto, las raices de esta ecuación serán:

$x_1 = [3](mod\ 8) = \{\dots, -13, -5, 3, 11, 19, 27, \dots\}$

$x_2 = [5](mod\ 8) = \{\dots, -11, -3, 5, 13, 21, 29, \dots\}$

$x_3 = [7](mod\ 8) = \{\dots, -9, -1, 7, 15, 23, 31, \dots\}$

$x_4 = [9](mod\ 8) = \{\dots, -7, 1, 9, 17, 25, 33, \dots\}$

Ejemplo 2.- *Determinar si la siguiente ecuación de congruencia tiene solución e indicar cuantas raíces presenta.*

$$12x \equiv 19\ (mod\ 8)$$

Solución:

Por el *Teorema 28*, la ecuación lineal de congruencia "$ax \equiv b\ mod\ m$", posee solución si y solo si $d|b$, donde $d = (a, m)$.

Para este ejercicio: $a = 12$, $b = 19$ y $m = 8$

Hacemos: $d = (12, 8) = 4 \nmid 19$. Por lo tanto, esta ecuación no presenta solución.

CAPITULO IV

METODOLOGÍA

4.1. TIPO DE INVESTIGACIÓN

El presente trabajo "Teorema de Lagrange para determinar el número de raíces de una ecuación polinómica modulo p (primo) de grado n", según su tipo de investigación, corresponde a un proyecto de desarrollo explicativo y descriptivo por cuanto se trata de mostrar, en forma explícita, la determinación del número de raíces de las ecuaciones polinómicas de congruencia aplicando la teoría de Lagrange, así mismo es una investigación básica y aplicada dado que corresponde al área de la teoría de números usando la congruencia módulo para así determinar el número de raíces de una ecuación polinómica.

4.2. MÉTODO DE LA INVESTIGACIÓN

El método de investigación del presente estudio modela una investigación deductiva y de análisis por que se utilizó y se analizó una serie de premisas (definiciones – teoremas) para llegar a un resultado o conclusión sobre el número de raíces de una ecuación polinómica usando congruencia modulo.

4.3. DISEÑO DE LA INVESTIGACIÓN

Por el diseño de la investigación, esta es no experimental, transversal dado que es sistemática y empírica pues las variables no se manipulan; los resultados sobre las relaciones entre las variables se realizará sin intervención o influencia directa y dichas relaciones se observan tal y como se han dado en su contexto natural.

.

CAPÍTULO V

RESULTADOS

Teorema 29. - Congruencia de Polinomios

Sea

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \in \mathbb{Z}[x]$$

entonces si $a \equiv b \ (mod\ m)$ se tendrá:

$$P(a) \equiv P(b) \ (mod\ m)$$

Demostración:

De $a \equiv b \ (mod\ m)$, y aplicando el *Teorema 19 parte ii* tantas veces como se desee, deducimos

$$a^i \equiv b^i \ (mod\ m) \quad \forall\, i\,, 1 \leq i \leq n$$

Por el *Teorema 18 parte ii* multiplicando a cada congruencia por su respectivo coeficiente del polinomio se obtiene

$$c_i a^i \equiv c_i b^i \ (mod\ m)$$

Finalmente, podemos sumar todas estas ecuaciones, gracias al *Teorema 19 parte i*

$$c_n a^n + \cdots + c_1 a + c_0 \equiv c_n b^n + \cdots + c_1 b + c_0 \ (mod\ m)$$

se llega al resultado esperado $P(a) \equiv P(b) \ (mod\ m)$ ■

Teorema 30. La congruencia lineal

$$a_1 x_1 + a_2 x_2 + \ \ldots + a_n x_n \equiv c \ mod\ m$$

es soluble si y solo si $d|c$, donde $d = (a_1, a_2, \ldots, a_n, m)$.

El número de soluciones distintas modulo m es dm^{n-1}.

Demostración:

Haremos la demostración para el caso $n = 2$. El caso general se deduce de este caso particular y del principio de inducción.

Consideremos entonces

$$a_1x + a_2y \equiv c \ mod \ m$$

donde $(a_1, a_2, m) = d$ y $d|c$.

Es fácil ver que la condición $d|c$ es necesaria para la existencia de la solución. Probaremos que esta condición es también suficiente.

Sea $(a_2\ , m) = d'$. Luego de $a_1x + a_2y \equiv c \ mod \ m$ obtenemos $a_1x \equiv c \ mod \ d'$

De $(d', a_1) = \big((a_2, m), a_1\big) = d,$ y $d|c$. Luego $a_1x \equiv c \ mod \ d'$ posee d soluciones distintas módulo d', de acuerdo al *Teorema 28*, estas d soluciones, generan $\frac{d.m}{d'}$ soluciones distintas módulo m para x.

Para cada solución x, se reemplaza su valor en la ecuación $a_1x + a_2y \equiv c \ mod \ m$ para obtener

$$a_2y \equiv c - a_1x \ mod \ m$$

Teniendo en cuenta que: $(m, a_2) = d'$, y, además: $d'|c - a_1x$, se deduce entonces que la ecuación anterior posee d' soluciones distintas para y módulo m.

Contando el número de soluciones de $a_1x + a_2y \equiv c \ mod \ m$, se tendrá la ecuación

$$S = S_x \, . S_y$$

donde S = número de soluciones de $a_1x + a_2y \equiv c \ mod \ m$,

S_x = numero de soluciones para x

S_y = número de soluciones para

luego:

$$S = d\frac{m}{d'}d' = d.m \qquad \blacksquare$$

5.1. GRADO DE CONGRUENCIA DE UN POLINOMIO

El grado de congruencia de un polinomio congruente con 0 respecto al módulo *m* es un número entero tal como se detalla:

1. Sea $P(x) = a_n.x^n + a_{n-1}.x^{n-1} + \cdots + a_1.x^1 + a_0.x^0$, si a_n no es congruente con 0 respecto del módulo m, el grado de la congruencia $P(x) \equiv 0(mód\ m)$ es n.
2. Si $a_n \equiv 0(mód\ m)$ y sea k el mayor entero positivo tal que a_k no es congruente con cero respecto del módulo m; entonces el grado de la congruencia es k.
3. Si no hay dicho entero k, es decir, si todos los coeficientes de $P(x)$ son múltiplos de m, entonces no se asigna grado a la congruencia.

El grado de congruencia de $P(x) \equiv 0(mód\ m)$ no es lo mismo que el grado del polinomio $P(x)$. El grado de la congruencia depende del módulo; el grado del polinomio es independiente del módulo.

5.2. CONGRUENCIAS LINEALES

Teorema 31. - Si $(a, m) = 1$, la congruencia $ax \equiv b(mód\ m)$ tiene exactamente una solución módulo m.

Demostración:

Por el *Teorema 21*, el conjunto $\{a, 2a, \ldots, ma\}$ es un sistema residual completo, en particular uno y sólo uno de los residuos será congruente con b módulo m. ■

Ejemplo 3.- *Determinar si la siguiente ecuación de congruencia tiene solución, indicar cuantas raíces presenta y resolverla completamente.*

$$5x \equiv 4\ (mod\ 6)$$

Solución:

Por el *Teorema 28*, la ecuación lineal de congruencia "$ax \equiv b\ mod\ m$", posee solución si y solo si $d|b$.

Para este ejercicio: $a = 5$, $b = 4$ y $m = 6$

Hacemos: $d = (5\ , 6) = 1$

$d|\ b = 1\ |\ 4$ entonces, esta ecuación si tiene solución.

Además, por el *Teorema 31*, esta ecuación lineal de congruencia tiene exactamente una solución.

$5x \equiv 4\ (mod\ 6)$ por definición de congruencia se escribe: $5x = 4 + 6k, k \in \mathbb{Z}^+$

$5x = 4 + 36 + 6k \Rightarrow 5x \equiv 40\ (mod\ 6)$, luego por el *Teorema 18 parte 2*:

$5x \equiv 40\ (mod\ 6) = x \equiv 8\ (mod\ 6)$ y nuevamente por la definición de congruencia:

$x \equiv 8\ (mod\ 6) \rightarrow x = 8 + 6k \rightarrow x = 2 + 6 + 6k \rightarrow x = 2 + 6k$, finalmente:

$x \equiv 2\ (mod\ 6)$, es la única solución.

Luego: $x = [2](mod\ 6) = \{\dots, -10, -4, 2, 8, 14, 20, \dots\}$.

Teorema 32. Sea $(a, m) = d$. Si $d \nmid b$ la congruencia

$$ax \equiv b(mód\ m)$$

no tiene soluciones, mientras que sí $d \mid b$ la congruencia tiene exactamente d soluciones módulo m que vienen dadas por

$$x_1, x_1 + m_1, \dots, x_1 + (d-1)m_1,$$

donde

$$m_1 = \frac{m}{d},\ a_1 = \frac{a}{d},\ b_1 = \frac{b}{d} \quad y \quad x_1$$

es la solución de la congruencia $a_1 x \equiv b_1 (mód\ m_1)$.

Demostración:

Si la $ax \equiv b(mód\ m)$ tiene alguna solución entonces, como $d \mid a$ y $d \mid m$, necesariamente d tiene que dividir a b.

Cualquier solución x de $ax \equiv b(mód\ b)$ debe ser también de $a_1 x \equiv b_1 (mód\ m_1)$. Pero como $(a_1, m_1) = 1$ la solución x_1 es única módulo m_1. Sin embargo la clase residual módulo m_1 a la que pertenece x_1 consta de d clases residuales distintas módulo m: las clases a las que pertenecen los números $x_1, x_1, +m_1, \dots, x_1 + (d-1)m_1$.

Por lo tanto, la congruencia $ax \equiv b(mód\ m)$ tiene exactamente las d soluciones descritas en el enunciado. ■

El *Teorema 32* nos dice que las congruencias lineales se reducen a resolver congruencias donde el módulo y el coeficiente de la x son primos entre sí.

La manera más fácil de resolver la congruencia lineal $ax \equiv b(mód\ m)$ con $(a, m) = 1$ consiste en resolver primero la ecuación $ax \equiv 1(mód\ m)$ utilizando el algoritmo de Euclides y multiplicar dicha solución por b.

5.3. CONGRUENCIAS POLINÓMICAS - TEOREMA DE LAGRANGE

El estudio de congruencias polinómicas de grado superior es más complicado, únicamente para las congruencias de grado dos existe un método razonable para decidir cuando tiene solución. Cuando el módulo es primo tenemos, se tiene

Teorema 33 (Lagrange). - Dado un primo p, sea $P(x) = c_0 + c_1x + \cdots + c_nx^n$ un polinomio de grado n con coeficientes enteros tal que $p \nmid c_n$, entonces la congruencia polinómica $P(x) \equiv 0$ (mód p) tiene, a lo más, n soluciones.

Demostración:

Usaremos el método de inducción sobre el grado del polinomio.

Para el caso de n = 1 ya se ha estudiado anteriormente; La congruencia lineal

$a_0 + a_1x \equiv 0(mód\ p)$ tiene una solución si $(c_1, p) = 1$.

Usando la Hipótesis Inductiva: el teorema es cierto para *n – 1*: si x_1 es una solución de

$$c_0 + c_1x + \cdots + c_nx^n \equiv 0\ (mod\ p)$$

La ecuación $c_1(x - x_1) + \cdots + c_n(x^n - x_1^n) \equiv 0\ (mod\ p)$ se cumple para cualquier otra solución, es decir, existen enteros $a_1, a_2, \ldots, a_n$ tales que

$$(x - x_1)(c_nx^{n-1} + a_2\,x^{n-1} + \cdots + a_n) \equiv 0\ (mod\ p)$$

Debe ser satisfecha por todas las soluciones de nuestra ecuación.

Como p es primo, las soluciones distintas de x_1 deben serlo también de

$$c_nx^{n-1} + a_2\,x^{n-1} + \cdots + a_n \equiv 0\ (mod\ p)$$

Y por la hipótesis inductiva, existen a lo más n-1 soluciones de esta ecuación. ■

Ejemplo 4.- *Determinar si la siguiente ecuación de congruencia tiene solución e indicar cuantas raíces presenta.*

$$5x^2 - 3x + 1 \equiv 0 \ (mod\ 23)$$

Solución:

Por el *Teorema 33 (Teorema de Lagrange)*, se nos indica que, dado una ecuación de congruencia polinómica de grado n de la forma $P(x) \equiv 0 \ (mod\ p)$, con p primo.

Donde: $P(x) = c_0 + c_1x + \cdots + c_nx^n$, la congruencia polinómica tiene, a lo más, n soluciones si: $p \nmid c_n$,

Para este ejercicio: $c_n = 5, p = 23$

Se hace la pregunta ¿ $23 \nmid 5$?, resultando verdadero.

Por lo tanto, esta ecuación presenta a lo más $n = 2$ soluciones.

Ejemplo 5.- *Determinar si la siguiente ecuación de congruencia tiene solución e indicar cuantas raíces presenta.*

$$x^3 - 18x^2 + 117x - 296 \equiv 0 \ (mod\ 19)$$

Solución:

Por el *Teorema 33 (Teorema de Lagrange)*, se nos indica que, dado una ecuación de congruencia polinómica de grado n de la forma $P(x) \equiv 0 \ (mod\ p)$, con p primo.

Donde: $P(x) = c_0 + c_1x + \cdots + c_nx^n$, la congruencia polinómica tiene, a lo más, n soluciones si: $p \nmid c_n$,

Para este ejercicio: $c_n = 1, p = 19$

Se hace la pregunta ¿ $19 \nmid 1$? resultando verdadero.

Por lo tanto, esta ecuación presenta a lo más $n = 3$ soluciones

Corolario10. - Si la congruencia $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + c_nx^n \equiv 0\ (mod\ p)$ tiene más de *n* soluciones, entonces los coeficientes $c_0, c_1, \ldots, c_n$ deben ser múltiplos de p.

Demostración:

Supongamos que no es cierto y sea *r* el mayor entero tal que $p \nmid c_r$. La congruencia del corolario es equivalente a la congruencia $c_0 + c_1x + \cdots + c_{r-1}x^{r-1} + c_rx^r \equiv 0\ (mod\ p)$, que tiene a lo más *r* soluciones, cual contradice hemos supuesto que tiene por lo menos n + 1 soluciones.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

1.- Los polinomios algebraicos, de grado n, que pertenecen en el anillo $\mathbb{R}\ [x]$, el teorema de Lagrange garantiza que tiene a lo más n raíces, sin embargo, para las ecuaciones polinómicas modulo p de grado n, no se tiene la seguridad de que tenga n raíces.

2.- Si a las ecuaciones polinómicas módulo p, le exigimos que p sea un numero primo, entonces el teorema de Lagrange nos asegura que tiene a los más n soluciones.

3.- Como consecuencia del teorema de Lagrange para las ecuaciones polinómicas modulo p (primo) de grado n, podría tener mas de n soluciones, siempre que los coeficientes de dicho polinomio sean múltiplos de p.

6.2. RECOMENDACIONES

1.- Profundizar en el curso de teoría de números, la aplicación de la teoría de congruencias en diferentes campos del algebra, en particular a las ecuaciones en general.

2.- A partir de este trabajo, continuar con el estudio de la aplicación del Teorema de Lagrange para ecuaciones no polinómicas.

3.- Continuar el estudio de las ecuaciones polinómicas modulo p (primo), con ls polinomios que no pertenecen a $\mathbb{Z}[x]$.

BIBLIOGRAFÍA

Arenas Suaza, B. S. (2013). *Las ecuaciones lineales, desde situaciones cotidianas.* Medellin: Universidad Nacional de Colombia, Facultad de Arquitectura, Escuela del Hábitat - CEHAP.

De Nápoli, P. (Enero - Abril de 2014). Polinomios. *Apunte de las Teóricas de Álgebra I*, 47. Obtenido de http://mate.dm.uba.ar/~pdenapo/apuntes-algebraI/polinomios.pdf

Gerra, N., López, B., Quintana, M. P., & Suárez, A. (18 de Abril de 2018). Introduccion a las Estructuras Algebraicas. Veracruz. Obtenido de Universidad Veracruzana: https://www.uv.mx/personal/aherrera/files/2014/08/20d.-INTRODUCCION-A-LAS-ESTRUCTURAS-ALGEBRAICAS.pdf

González Gutiérrez, F. J. (Octubre de 2004). *DocPlayer.es.* (D. d. Matemáticas, Ed.) Obtenido de DocPlayer.es Web site: https://docplayer.es/3222045-Apuntes-de-matematica-discreta-10-divisibilidad-algoritmo-de-la-division.html

Guzmán Saavedra, M. Á. (11 de Junio de 2018). *KIPDF.* Obtenido de Copyright © 2018 KIPDF.COM. All rights reserved.: https://kipdf.com/congruencias-definicion-sea-m-un-entero-fijo-diremos-que-dos-enteros-a-y-b-son-c_5aadef951723dd3b6adcb5c7.html

Hernández, L. M. (2007). Estructuras Algebraicas. En L. M. Hernádez, *Estructura Algebraicas* (pág. 13). Caracas, Venezuela: Centro de Cálculo CIentífico y Tecnológico. Recuperado el lunes de julio de 2018

Hurtado Moreno, C. A. (2013). *Analisis didactico de las ecuaciones de primer grado con una incognita y su impacto en la educacion basica.* Cali: Universidad del Valle, Colombia.

ISFD-Tandil, A. d. (14 de Febrero de 1990). *Ecuaciones ISFD10*. Obtenido de Ecuaciones: https://sites.google.com/site/ecuacionesisfd10/home

Molina Iglesias, C. (1983). El estudio de las funciones y ecuaciones polinomicas en 1° de B.U.P.: un enfoque diferente al usual. *Lecciones de Matemáticas 3*, 9-36. Obtenido de http://www.sinewton.org/numeros/numeros/08/Articulo01.pdf

Sánchez, C. M. (2014). *Lecciones de {Algebra.* Buenos Aires, Argentina: Universidad de Buenos Aires. Recuperado el Martes de mayo de 2018

Zumalacárregui Pérez, A. (23 de Enero de 2015). *Biblos-e Archivo.* Recuperado el 11 de Junio de 2018, de Universidad Autónoma de Madrid. Biblioteca: https://www.uam.es/personal_pdi/ciencias/cillerue/Curso/capitulo%203.pdf

FORMATO DE AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS Y TRABAJOS DE INVESTIGACIÓN, PARA OPTAR GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES EN EL REPOSITORIO INSTITUCIONAL DIGITAL - UNASAM

Conforme al Reglamento del Repositorio Nacional de Trabajos de Investigación – RENATI.
Resolución del Consejo Directivo de SUNEDU Nº 033-2016-SUNEDU/CD

1. Datos del Autor:

Apellidos y Nombres: RAMIREZ HUARAC SAUL FELIPE

Código de alumno: 072.0105.344 Teléfono: 979 919 814

Correo electrónico: ramirez.huarac.saul@gmail.com DNI: 46871908

2. Modalidad de trabajo de investigación:

( ) Trabajo de investigación ( ) Trabajo académico

( ) Trabajo de suficiencia profesional (x) Tesis

3. Título profesional o grado académico:

( ) Bachiller (x) Título ( ) Segunda especialidad

( ) Licenciado ( ) Magister ( ) Doctor

4. Título del trabajo de investigación:

"TEOREMA DE LAGRANGE PARA DETERMINAR EL NÚMERO DE RAÍCES DE UNA ECUACIÓN POLINÓMICA MODULO p (primo) DE GRADO n"

5. Facultad de Ciencias

6. Escuela, Carrera o Programa: Escuela académico profesional de Matemática

7. Asesor:

Apellidos y Nombres: Msc. NINAQUISPE CASTILLO MARIO Teléfono: 945 465 600

Correo electrónico: matemario@hotmail.com D.N.I.: 31629062

A través de este medio autorizo a la Universidad Nacional Santiago Antúnez de Mayolo, publicar el trabajo de investigación en formato digital en el Repositorio Institucional Digital, Repositorio Nacional Digital de Acceso Libre (ALICIA) y el Registro Nacional de Trabajos de Investigación (RENATI).

Asimismo, por la presente dejo constancia que los documentos entregados a la UNASAM, versión impresa y digital, son las versiones finales del trabajo sustentado y aprobado por el jurado y son de autoría del suscrito en estricto respeto de la legislación en materia de propiedad intelectual.

Firma: .....

D.N.I.: 46871908

FECHA: 18 de diciembre de 2018