

*La criptografía, recurso didáctico para la  
enseñanza aritmética de las matrices y la  
solución de sistemas de ecuaciones lineales*

CLAUDIA PATRICIA MANCIPE CAICEDO  
LICENCIADA EN MATEMÁTICAS



UNIVERSIDAD NACIONAL DE COLOMBIA  
FACULTAD DE CIENCIAS  
BOGOTÁ, D.C.  
27 DE JUNIO DE 2014

*La criptografía, recurso didáctico para la  
enseñanza aritmética de las matrices y la  
solución de sistemas de ecuaciones lineales*

CLAUDIA PATRICIA MANCIPE CAICEDO  
LICENCIADA EN MATEMÁTICAS

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE  
MAGISTER EN ENSEÑANZA DE LAS CIENCIAS EXACTAS Y  
NATURALES

DIRECTOR  
PH.D. AGUSTÍN MORENO CAÑADAS  
PROFESOR ASOCIADO



UNIVERSIDAD NACIONAL DE COLOMBIA  
FACULTAD DE CIENCIAS  
BOGOTÁ, D.C.  
27 DE JUNIO DE 2014

# **La criptografía, recurso didáctico para la enseñanza aritmética de las matrices y la solución de sistemas de ecuaciones lineales**

## **Cryptography, Didactic Resource for Teaching Arithmetic Arrays and Solving Systems of Linear Equations**

### **Resumen**

En la actualidad, los sistemas criptográficos no pueden ser considerados sólo como retos que activan el ingenio de los seres humanos, es por ello que las matemáticas aplicadas proponen nuevos desafíos que generan diferentes preguntas acerca de la enseñanza de las matemáticas escolares; con base en esto, el presente trabajo se centra en el diseño de una secuencia didáctica en la solución de problemas que involucren mensajes ocultos, enigmas o secretos para los estudiantes de educación secundaria de la Escuela Normal Superior Distrital María Montessori. El propósito es promover el aprendizaje de los objetos matemáticos, en particular las estructuras de matrices y la solución de sistemas de ecuaciones lineales a través de la Criptografía, debido a que sus aplicaciones contribuyen al avance de la ciencia y la tecnología. Los fundamentos teóricos que apoyan las actividades realizadas en clase incluyen la revisión de algunos aspectos históricos, epistemológicos, pedagógicos y didácticos..

**Palabras Claves:** Criptografía, Descifrar, Matrices, Sistemas de ecuaciones lineales, Resolución de problemas.

### **Abstract**

Nowadays, cryptographic systems cannot be considered only as riddles that activate the ingenuity of human beings, that way applied mathematics proposes new challenges that generate different questions about the teaching of school mathematics; based on this, the present work focuses on the design of a teaching sequence on solving problems involving hidden messages, riddles or enigmas for students of secondary education of Escuela Normal Superior Distrital María Montessori. The aim of this document is to promote the learning of mathematical objects, particularly the structures of matrices and solving systems of linear equations by means of the Cryptography, since its applications contribute to problem solving for the advance of the science and technology. The theoretical foundations that support the activities implemented in class include the review of some historical, epistemological, pedagogical and didactic aspects.

**Keywords:** Cryptography, Decrypt, Matrix, Systems of linear equations, problem solving.

## Nota de aceptación

---

Jurado

---

Jurado

---

Jurado

---

Director  
Ph.D. Agustín Moreno Cañadas

Bogotá, D.C., 27 de junio de 2014

---

---

Dedicado a

---

---

*MIS PADRES Y FAMILIA...*

---

---

# Agradecimientos

---

---

*“Lo poco que he aprendido carece de valor,  
comparado con lo que ignoro y no desespero  
en aprender”*

*René Descartes*

A Dios por los retos que me ha presentado para alcanzar entre muchas, esta meta.

A mis Padres Omar Mancipe y Carmenza Caicedo quienes siempre me han apoyado y orientado con disciplina y amor en esta grandiosa tarea de enseñar.

Al profesor Agustín Moreno Cañadas que con su saber, experiencia y espiritualidad se convirtió en excelente guía para el desarrollo de este proyecto.

Agradezco a la Escuela Normal Superior Distrital María Montessori por permitirme aplicar cada una de las actividades aquí propuestas; y a las personas que facilitaron a que este trabajo fuera realidad.

---

---

# Índice general

---

---

Índice general	I
Índice de tablas	IV
Índice de figuras	V
Introducción	VII
<b>1. REFERENTES HISTÓRICOS-EPISTEMOLÓGICOS</b>	<b>1</b>
1.1. Historia de la Criptografía . . . . .	1
1.1.1. Edad Antigua . . . . .	2
1.1.2. Edad Media . . . . .	4
1.1.3. Edad Moderna . . . . .	5
1.1.4. Edad Contemporánea . . . . .	6
1.2. Sistemas de Ecuaciones y Matrices. Desarrollo histórico . . . . .	9
1.2.1. Sistemas de Ecuaciones . . . . .	9
1.2.2. Matrices . . . . .	11
<b>2. REFERENTE DISCIPLINAR</b>	<b>13</b>
2.1. Congruencias . . . . .	13
2.1.1. Notación de Congruencia . . . . .	13
2.1.2. El Teorema de Fermat . . . . .	18
2.1.3. Teorema de Wilson . . . . .	19
2.1.4. La función de Euler $\phi(m)$ . . . . .	20
2.1.5. Ecuaciones de Congruencia Lineales . . . . .	23

---

2.1.6. Congruencias Algebraicas . . . . .	25
2.1.7. Sistema de Cubrimiento para los Números Enteros . . . . .	26
2.2. Sistema de Ecuaciones Lineales . . . . .	28
2.3. Determinantes . . . . .	29
2.3.1. Propiedades de los Determinantes . . . . .	31
2.4. Matrices . . . . .	35
2.4.1. Operaciones con Matrices . . . . .	36
2.4.2. Transformaciones elementales . . . . .	37
2.4.3. Matrices Invertibles . . . . .	37
<b>3. CRIPTOGRAFÍA Y ESTEGANOGRAFÍA</b>	<b>40</b>
3.1. Métodos Criptográficos . . . . .	42
3.1.1. Cifrado por Desplazamiento . . . . .	42
3.1.2. Criptosistema Afín . . . . .	43
3.1.3. El Criptosistema de Vigenère . . . . .	45
3.1.4. Cifrado por Transposición Geométrica . . . . .	45
3.1.5. Criptosistema de Hill . . . . .	46
3.1.6. Esquema de Shamir . . . . .	49
3.2. Esteganografía . . . . .	54
<b>4. CONSECUENCIA DE PATRONES CON EL USO DE LA ESTE- GANOGRAPHÍA Y CRIPTOGRAFÍA</b>	<b>57</b>
4.1. Números de Catalan . . . . .	57
4.1.1. Algunas Propiedades de los Números de Catalan . . . . .	62
4.1.2. Números de Delannoy . . . . .	65
4.2. Números Poligonales y Criptografía . . . . .	68
<b>5. ASPECTOS PEGADÓGICOS Y DIDÁCTICOS</b>	<b>76</b>
5.1. Acerca de Aprendizaje Significativo . . . . .	76
5.2. Metodología de Resolución de Problemas . . . . .	77
5.3. Álgebra Escolar . . . . .	81
5.3.1. Enseñanza de los Sistemas de Ecuaciones Lineales . . . . .	82
5.3.2. Obstáculos de Aprendizaje . . . . .	83
5.4. La Criptografía en la Escuela . . . . .	85



---

<b>6. PROPUESTA DIDÁCTICA</b>	<b>87</b>
6.1. <i>Actividad 0</i> : El Escarabajo de Oro . . . . .	88
6.2. <i>Actividad 1</i> : Te Reto a Descifrarlo . . . . .	91
6.3. <i>Actividad 2</i> : ¿Cuál será el Camino? . . . . .	94
6.4. <i>Actividad 3</i> : Ocultando Mensajes . . . . .	98
6.5. <i>Actividad 4</i> : Matriz Recargado . . . . .	103
6.6. <i>Actividad 5</i> : Compartiendo Secretos . . . . .	107
6.7. <i>Actividad 6</i> : DESCUBRE EL ENIGMA . . . . .	110
 <b>7. APLICACIÓN Y ANÁLISIS DE RESULTADOS</b>	 <b>114</b>
 Conclusiones	 <b>121</b>
 Trabajo futuro	 <b>123</b>
 Anexos	 <b>124</b>

---

---

## Índice de tablas

---

---

3.1. Alfabeto Español . . . . .	42
3.2. Texto Criptosistema Afín . . . . .	44
3.3. Texto Criptosistema de Vigenère . . . . .	45
3.4. Tranposición Geométrica por Columna . . . . .	46
3.5. Transposición Geométrica Triangular . . . . .	46
3.6. Texto Criptosistema Hill . . . . .	47
7.1. Ficha Técnica ICFES . . . . .	114
7.2. Escala de Valoración ENSDMM . . . . .	117

---



---

# Índice de figuras

---



---

1.1. Piedra Roseta . . . . .	2
1.2. Alfabeto Atbash . . . . .	3
1.3. Scitala Espartana . . . . .	4
1.4. Al-Kandi . . . . .	4
1.5. Disco de Alberti . . . . .	5
1.6. Libro Polygraphiae . . . . .	6
1.7. Enigma . . . . .	7
1.8. Factorización . . . . .	8
1.9. Papiro de Rhind y Tratado Nueve Capítulos del Arte Matemático . . .	10
1.10. Inversa de una Matriz-Arthur Cayley . . . . .	12
3.1. Rejilla de Cardano y Scitala Espartana . . . . .	54
3.2. Técnica Esteganográfica . . . . .	56
4.1. Números de Catalan - Diagrama $n=6$ . . . . .	58
4.2. Trayectoria Reticular (0,0) y (2,2) . . . . .	59
4.3. Trayectoria Reticular (1,1) y (0,0) . . . . .	59
4.4. Triángulo de Pascal $n=6$ . . . . .	60
4.5. Triángulo de Pascal y Números de Catalan . . . . .	61
4.6. Trayectorias Reticulares y Números de Catalan . . . . .	62
4.7. Clave Esteganográfica - Números de Catalan . . . . .	64
4.8. Trayectorias Números de Delannoy . . . . .	65
4.9. Diagrama $D$ asociados al texto claro . . . . .	66
4.10. Números Poligonales . . . . .	69

---

4.11. Propiedad de los Números Cuadrados . . . . .	69
4.12. Propiedad Suma de Números Impares . . . . .	69
4.13. Claves con el Triángulo de Pascal . . . . .	70
4.14. Conjunto de Números, si $j = 4$ . . . . .	71
5.1. Aprendizaje Significativo . . . . .	77
5.2. Tipos de Dificultades Algebraicas . . . . .	84
7.1. Desempeño estudiantes grado Noveno según Prueba Saber 2012 . . . .	115
7.2. Resultados Encuesta . . . . .	116
7.3. Desempeño de los estudiantes del Grupo control y Experimental . . . .	117
7.4. Desempeño de los estudiantes del Grupo control y Experimental Fi- nalizado el 2013 . . . . .	118
7.5. Comparativo de Desempeños . . . . .	119

---

---

# Introducción

---

---

*“La matemática tiene las progresiones geométricas que elevan los números a maravillosa altura, las sociedades tienen la educación”*

*José Martí*

La criptografía es el arte que permite construir mensajes secretos y la sofisticación de sus técnicas está en relación directa con los avances de la ciencia. Es así, que a través de la historia de la humanidad tal arte se ha convertido en una medida del avance tecnológico y cultural de las civilizaciones, debido a que ha posibilitado solucionar situaciones problemas que afectan a los seres humanos. Se puede anotar que en la cultura egipcia la Criptografía se aplicaba en mensajes jeroglíficos, mientras que actualmente la usamos para proteger información que se transmite a través de distintos tipos de medios electrónicos.

La relación entre la cultura y el avance de la ciencia, también permite identificar que para alcanzar las metas propuestas en la vida del ser humano se necesitan diversos factores y herramientas que contribuyan a tal logro. La vida escolar forma parte esencial para adquirir habilidades y destrezas a través del proceso de enseñanza aprendizaje que, progresivamente, permiten al estudiante implementar elementos de juicio para afrontar la solución de problemas.

En la escuela, las matemáticas y sus aplicaciones constituyen un recurso esencial para la fundamentación y adquisición de la estructura lógica que necesita una persona para generar estrategias de solución ante cualquier situación que afecte su entorno o el de los demás.

Desde el primer acercamiento a las formas y tamaños de elementos reales hasta la abstracción propia de los conceptos del álgebra y el cálculo, se presentan al estudiante una serie de conocimientos que inciden en el desarrollo de las etapas físicas, mentales y sociales que se evidencian en su proceder en la cotidianidad.

Paralelamente año tras año, los estudiantes también van encontrando barreras para adquirir el conocimiento matemático; generando diversas corrientes que estudian las dificultades que conlleva la enseñanza-aprendizaje de esta ciencia tan importante,

que en ocasiones parece exclusiva para pocos. Es así que investigaciones realizadas en la enseñanza del álgebra escolar, por autores como *Wagner, Kieran, Bednarz, Lee, Filloy, Rojano y Puig* según Socas [43]; demuestran las dificultades de los alumnos en la transición desde la aritmética hasta el álgebra, debido a que, pocas veces se enfrenta a los jóvenes a la resolución de problemas, olvidando la contextualización entre los objetos matemáticos, la dinámica de los estudiantes y la generalización de los conceptos presentados en clase.

Esta situación, se refleja en la solución de sistemas de ecuaciones lineales con los estudiantes de la Escuela Normal Superior Distrital María Montessori, quienes consideran las matemáticas como un cuerpo ya finalizado de estructuras y algoritmos complejos que no se ejercitan sino en el aula de clase aislado de sus contextos y necesidades.[30] Cabe anotar, que uno de los estándares descrito para el grado Noveno en el Pensamiento Variacional y Sistemas Algebraicos según el Ministerio de Educación Nacional [11]; define que los estudiantes deben identificar diferentes procesos para solucionar sistemas de ecuaciones lineales; sin embargo el método menos aplicado, para este fin, es el método matricial a pesar de que éste brinda la posibilidad de estudiar de manera adicional el álgebra matricial. Es así, que el estudio riguroso de estas estructuras permitirá no sólo resolver sistemas de ecuaciones lineales sino también algunos problemas de matemática aplicada que se involucran en el aula de clase.

Por tanto, la propuesta didáctica tiene como propósito diseñar actividades con acertijos o mensajes secretos que favorezcan la enseñanza y aprendizaje de conceptos matemáticos, en especial el de la estructura de las matrices en la solución de ecuaciones lineales  $2 \times 2$ ; con la ayuda de una de las aplicaciones más atractivas de la Aritmética Modular: la criptografía.

*La Criptografía es un excelente vehículo para presentar conceptos matemáticos fundamentales al alumnado mediante la resolución de problemas y promoción el trabajo colaborativo en el aula. Al respecto argumentamos que la criptografía contiene elementos de motivación e intriga como el suspenso o el espionaje que hacen que se perciba como un juego consistente en salvaguardar los propios secretos e intentar romper los secretos ajenos. Además los alumnos de principio de siglo XXI suelen estar más expuestos y habituados que sus mayores a conceptos referidos a la codificación gracias al uso de teléfonos móviles, video consolas o juegos de ordenador. P. Caballero (2004)[2]*

Las actividades diseñadas se proyectan para los estudiantes de grado Noveno de la Escuela Normal Superior Distrital María Montessori, donde pondrán a prueba sus habilidades de encontrar mensajes secretos a través del criptoanálisis (arte y ciencia de descifrar códigos secretos) en acertijos y textos cifrados, que requieran el estudio riguroso de métodos criptográficos clásicos que conlleven a un proceso intuitivo del concepto, su definición formal para llevar a la práctica la solución de este tipo de

enigmas. A partir de esto, se pretende estudiar conceptos de matrices  $2 \times 2$ , sus operaciones, la inversa de una matriz  $2 \times 2$  y solución de ecuaciones; empleando principalmente en el cifrado de Lester Hill y el esquema de Shamir.

El Capítulo 1 tiene como objetivo identificar históricamente las situaciones en tiempo y espacio que han permitido el avance de la criptografía, las matrices y sistemas de ecuaciones, esto como una actividad humana que surge de las necesidades de solucionar situaciones sociales, científicas o para la guerra.

En el Capítulo 2, se realiza un estudio formal de la Aritmética Modular como fuente de teorías para la criptografía, así como la Aritmética Matricial y Sistemas de Ecuaciones Lineales que permitan orientar el diseño de las actividades de la propuesta.

Para los Capítulos 3 y 4, se encontrará la definición de criptografía, los elementos de un sistema criptográfico y los diferentes métodos criptográficos propios de la propuesta didáctica, igualmente se expondrán resultados interesantes sobre patrones que conllevan al estudio de los números de Catalan, Delannoy y algunos números poligonales con el uso de la Esteganografía.

La fundamentación pedagógica y didáctica que se aborda en el Capítulo 5 sustenta las actividades de aula diseñadas del Capítulo 6, finalmente se realiza un análisis sencillo de la implementación de las actividades para el grupo experimental y control.

# CAPÍTULO 1

---

---

## REFERENTES HISTÓRICOS-EPISTEMOLÓGICOS

---

---

*“No hay nada más interesante para los seres humanos que resolver acertijos-problemas”*

*(Agustín Moreno C. 2012)*

La perspectiva histórica descrita en este capítulo, ofrece la oportunidad de enmarcar en el tiempo y espacio las ideas y problemas de cada época para la criptografía, las matrices y sistemas de ecuaciones entre otros; resaltando la importancia de la construcción del conocimiento matemático como una actividad humana que surge de las necesidades de solucionar situaciones sociales, científicas o para la guerra. De la misma manera, la historia sirve como agente motivador de la enseñanza de las matemáticas, pues permite contextualizar los conceptos a abordar y visualiza alternativas de solución que en la actualidad son sencillos y de mucha utilidad para el desarrollo de nuestra civilización.

### 1.1. Historia de la Criptografía

**Criptografía:** Etimológicamente, la palabra criptografía proviene de la unión de los términos griegos *κρυπτος* (krypto), que significa “oculto” y *γραφειν* (graphos), que significa “escritura”. Así, su traducción literal es “escritura oculta” y su definición, según el Diccionario de la Real Academia de la Lengua Española, es: “Arte de escribir con clave secreta o de un modo enigmático”; aunque, hace mucho tiempo dejó de ser un arte para convertirse en una técnica y más exactamente, en una serie de técnicas que se utilizan para ocultar una información sea de la naturaleza que esta sea; lo anterior descrito por Palma (2011)[32]



El avance de la ciencia y la tecnología, se encuentra estrechamente ligado al arte de la criptografía por su vínculo con la escritura, ésta como sistema de representación gráfica de una lengua y que históricamente ha formado parte de las civilizaciones, dada su necesidad de comunicar o ocultar sus saberes, hace inevitable realizar un recorrido de la evolución de la criptografía en la humanidad.

### 1.1.1. Edad Antigua

En **Egipto**, 3.000 a.C, la criptografía no tenía un fin militar o político, sino un objetivo religioso; se escribían este tipo de textos principalmente para ahuyentar los ladrones de tumbas. Durante siglos, investigadores intentaron descubrir los misterios de la escritura del antiguo Egipto, a la que denominaron jeroglífica por su carácter religioso “escrituras sagradas”. La dificultad de esta escritura y la incapacidad de conocer su significado, hizo que los jeroglíficos se convirtieran en enigmas complejos difíciles de interpretar. Este es el caso de la Piedra Rosseta, una estela egipcia que contenía un decreto del faraón Ptolomeo V, pero sólo hasta 1822, el filólogo francés Jean-François Champollion logra descifrar los secretos de la Piedra de Rosetta, identificando que en las tres secciones de la piedra se encuentra el mismo texto en griego, hierático (sacerdotes) y demótico (pueblo).

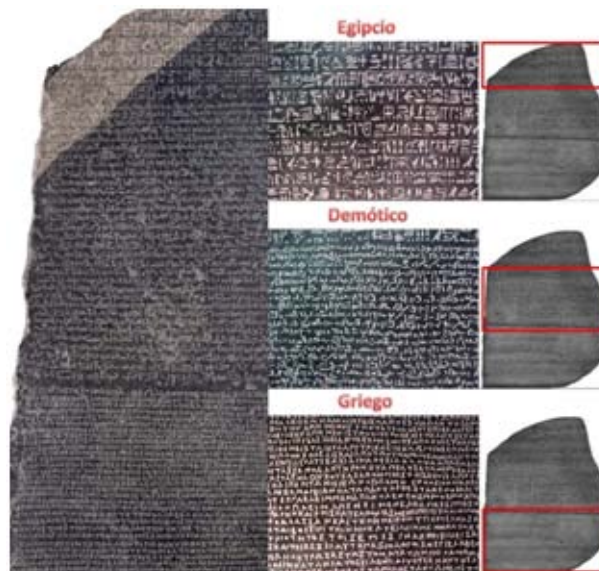


FIGURA 1.1. Piedra Roseta

**Atbash hebreo**, 600 a.C. En la biblia se emplea un clase de criptografía denominada atbash, la cual se identifica principalmente en el Antiguo Testamento en el texto de Jeremías: 25:26, 51:41, 51:1, ésta consiste en permutar la primera letra del alfabeto hebreo por la ultima y viceversa, análogamente la segunda por la antepenúltima, y así sucesivamente en el texto de Jeremías se aplica esta técnica para nombres de personas y ciudades como es el caso de la palabra Babilonia, en hebreo: Babel se convierte en Sheshach reemplazando la B por Sh y l por ch. La tabla de sustitución de atbash para el alfabeto hebreo es la siguiente:



FIGURA 1.2. Alfabeto Atbash

Así mismo, en el libro de Brahmin Vatsyayana del Kamasutra, escrito en el siglo IV a.C se encuentra que una de las habilidades de una mujer es la de mlecchita-vikalpa, el arte de la escritura secreta, ésta para ocultar los detalles de sus relaciones amorosas. Esta habilidad consistía en dividir el alfabeto por la mitad, emparejar las letras resultantes dos a dos de forma aleatoria. Cada emparejamiento constituía una clave como lo explica Xifre[44]. Por ejemplo:

A	S	C	D	N	R	G	X	I	J	K	Z	M
E	O	P	Q	R	B	T	U	V	W	H	Y	L

Así, la A queda sustituida por la E, la D por la Q, etc, y viceversa.

**Grecia**, Homero (siglo VIII a.C.) expresa en algunos pasajes de su obra *Ilíada* cómo se podía usar criptografía en Grecia. La narración involucra a Estenebea, esposa del rey Preto, quien se enamora de Belerofonte. Sin embargo, Estenebea al no conseguir su objetivo de seducción con Belerofonte, lo acusa ante su esposo Preto, éste enojado lo envía con una carta cifrada para el rey Lobates a Licia, solicitando que asesine a Belerofonte, pero para no matarlo Lobates le solicita matar la quimera.

Explica A.Moreno [7] que Herodoto, en su libro *Las Historias*, hizo una crónica de los conflictos entre Grecia y Persia, según Herodoto, fue el arte de la escritura secreta lo que salvo a Grecia de ser ocupada por Jerjes, líder de los persas. Debido a que Demarato, un exiliado griego en Persia, grabó los planes persas en un par de tablillas de madera y después los cubrió con cera, ocultando así el mensaje. Ya en su destino, Gorgo, esposa del rey Leonidas, quien puede ser considerada la primera criptógrafa, descubrió que debajo de la cera debería encontrarse el mensaje.

En la historia de Histaiaeo, Herodoto describe cómo se afeitaba a los mensajeros para escribir el mensaje sobre su cabeza, se esperaba a que creciera el cabello para que luego éste marchara a su destino, cabe anotar que, ya que la rapidez en la recepción del mensaje no era el elemento principal. En estas historias más que una técnica criptográfica, se empleó la esteganografía como arte de ocultar información.

**Scitale Espartano**, Siglo V a.C. Gracias a su desarrollo militar, en Esparta se estableció el primer sistema de criptografía militar, denominada la scitale espartana. Se describe como una vara redonda en el que se enrolla una cinta de pergamino larga y estrecha como una correa, sobre la cual se escribía el mensaje en forma longitudinal; al desenrollar la cinta, las letras aparecían en otro orden, formando una secuencia sin sentido, por lo que era preciso que el receptor del mensaje dispusiera de otro bastón exactamente igual que el del emisor para recuperar el mensaje enrollándolo

de nuevo en la cinta. Sin conocer el diámetro del bastón que había jugado el papel de clave, era imposible descifrar el mensaje; como se muestra en la Figura 1.3. Es de resaltar que esta técnica entre otras, corresponde más a la **Esteganografía**, que se encarga de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación.



FIGURA 1.3. Scitala Espartana

**Roma**, Los romanos quienes ya habían desarrollado su escritura y luchaban contra los bárbaros que no sabían leer emplearon el método desarrollado por el emperador Julio César (100-44 a.C.) para enviar mensajes secretos a sus legiones a través del cifrado de desplazamiento, el cual consistía en trasladar una letra ordenada tres lugares más adelante dada su localización lexicográfica.

### 1.1.2. Edad Media

Entre los años 800 y 1200, los árabes tuvieron un periodo de logros intelectuales, sin embargo en Europa por la misma época sólo los monasterios estudiaban la biblia buscando significados ocultos.

**Arabia**, 855 d.C. aparece el primer manuscrito sobre criptografía titulado “Sobre el desciframiento de mensajes criptográficos ” escrito por el sabio árabe Al- Kindi, el cual se basó en el análisis de frecuencia, es decir, se estudia la frecuencia con la que aparecen los distintos símbolos en un lenguaje determinado y luego la frecuencia con la que aparecen en los mensajes cifrados.



FIGURA 1.4. Al-Kandi

La palabra ciframiento fue acuñada por árabes para hablar sobre escritura secreta. Esto se ve claramente reflejado en los cuentos de Mil y una noches, donde se describen anagramas y referencias de criptografía en las narraciones hechas por Sherezade al sultán persa, así mismo como en los cuentos de Azis y Aziza

Reino Unido, Roger Bacon (1214-1294) monje franciscano que escribió el libro *La Epistola sobre las obras de arte secretas y la nulidad de la magia*. Describió métodos para mantener secretos mensajes y advertía, según Singh [40] “*Sólo un loco escribe un secreto de una forma que no lo oculte del vulgo*”

A finales del siglo XIV, en el año 1379 Gabriele de Lavinde de Parma, secretario del Papa Clemente VII, escribió una serie de claves para la correspondencia del Papa. Las claves eran sustituciones simples a las que se les añadía una lista conteniendo una docena de palabras y sus correspondientes signos para reemplazarlos. Su manual se tituló *Tratatti in cifra*; las claves de Lavinde constituyen los primeros ejemplos de Nomenclátor, es decir, un sistema de cifras y letras para ocultar la información.

### 1.1.3. Edad Moderna

En esta época, la criptografía presenta un auge debido a que los países establecen relaciones diplomáticas, por lo que requieren desarrollar métodos para asegurar las comunicaciones.

**Francia-España.** Para el siglo XVI el Rey Enrique IV contrata a François Viète (1540-1603), para descifrar cartas que intercambiaban Felipe con su jefe militar Juan de Moreo y su embajador Manosse. Es importante recordar que Viète se considera como el padre del álgebra.

Para 1585 otro francés Blaise de Vigenère publica su libro “*Tractié de Chiffre*” en donde presenta el primer sistema polialfabético con autoclave, esto significa que usa el mismo texto para hacer el cifrado, se conoció como “*Le chiffre indéchiffrable*” aunque más adelante se le cambiará el nombre por el de el cifrado de Vigenère. La idea de la autoclave perdurará en el tiempo y se aplicará en los algoritmos futuros como el DES en los modos CBC y CFB.

**Italia.** En 1466 Leon Battista Alberti, uno de las figuras líderes del Renacimiento Italiano, publica su libro “*Modus scribendi in ziferas*”, en donde habla por primera vez del disco de Alberti, el primer sistema polialfabético que se conoce. Alberti es el secretario de un cuerpo oficial perteneciente a la corte papal que se encarga únicamente de labores relacionadas con la criptografía. Por todo esto, Alberti será conocido como el “padre de la criptografía”. En Xifre (2009) [44]



FIGURA 1.5. Disco de Alberti

**Alemania**, Johannes Trithemius (1462-1516), también considerado el padre de la criptografía moderna escribe dos libros, el primero en 1499 *Esteganografía* y el segundo cuyo título es “*Polygraphiae*” en 1518, escrito por el abad en lengua alemana; durante todo el siglo XVI este era el libro prohibido, oculto, en el que se describen cifrados polialfabéticos con las nuevas tablas de sustitución rectangulares. Cabe anotar que la tecnología tuvo que avanzar hasta 1998 para que su tercer libro sobre el tratado de *Esteganografía* fuera descifrado por Jimm Reeds de los laboratorios AT&T.



FIGURA 1.6. Libro *Polygraphiae*

#### 1.1.4. Edad Contemporánea

Durante esta época los métodos criptográficos que se fundamentaban en sustituciones, transposiciones o tablas cifradoras, se experimentaron cambios debido a las guerras mundiales en las que se reinventaron claves y códigos para favorecer el espionaje, así mismo el avance en la tecnología permitió crear dispositivos y máquinas para cifrar y descifrar mensajes. Es de resaltar que la historia de la criptografía se relaciona con el desarrollo de la escritura y la tecnología de las civilizaciones; por tal motivo se tomarán algunos apartes que denotan los sucesos más relevantes para el auge de esta ciencia en la época.

Como lo expresa Xifré, citado por Palma [32], en la primera Guerra Mundial (1914-1918) los cifrados todavía se basaban por permutación permutaciones del alfabeto y los mensajes eran llevados por el hombre, usando medios de transporte muy lentos, de tal forma que había lugares a los cuales era imposible llevar el mensaje, como a barcos, aviones y submarinos, por lo que se comenzó a usar el teléfono, el telégrafo y la radio. Este último era fácil de transportar, lo que cambió radicalmente las comunicaciones; sin embargo, de este modo los mensajes eran también fácilmente interceptados. Esto justificó incrementar el uso de la criptografía.

**Europa**, En 1918 los alemanes Arthur Scherbius y Richard Ritter inventan la primera Enigma, Figura 1.7. Al mismo tiempo, la máquina de rotores es inventada y patentada por Alexander Koch en los Países Bajos y Arvid Damm en Suecia. En 1926 la marina alemana decidió comprar la máquina ENIGMA, que fue patentada hasta 1928, fecha en que Scherbius murió. Irónicamente en 1929 su invento se vendió en todo el mundo.



FIGURA 1.7. Enigma

**Estados Unidos**, La primera pareja de esposos criptógrafos fue Friedman y su esposa, su acercamiento se debió a que en Alemania se capturó un mensaje que venía de la India antes de la rebelión de Mahatma Gandhi. Este mensaje llegó a manos de Friedman quien lo descifró, advirtiéndole sobre la revuelta contra el imperio británico. Más adelante escribió el libro *El Índice de Coincidencia*, que describe de manera detallada la forma de descifrar el método de Vigenère. Friedman es uno de los criptógrafos más ejemplares, tuvo que luchar contra un grupo secreto japonés denominado J, para ello lideró el grupo Magic, para descifrar toda la información que llegaba a la embajada japonesa en Estados Unidos; los japoneses resolvieron esta dificultad con el Pacto del Eje con Alemania, quien les brindó tecnología para desarrollar la versión mejorada de Enigma usada por Japón denominada Purpura.

En 1929 **Lester S. Hill** publica el artículo “Cryptography in an Algebraic Alphabet”. El cifrado de Hill, que propone utilizar las reglas del álgebra de matrices en las técnicas de criptografía.

En la segunda Guerra Mundial se emplearon métodos como los de Playfair, Viernam; Friedman lideró el equipo de criptoanalistas de SIS para recrear purpura y crackearla, se realizaron grandes esfuerzos para romper los códigos del Eje.

Para los años 70 y 80 se inicia con la criptografía de clave simétrica y pública, con el avances de los circuitos integrados y el desarrollo en los algoritmos, concretamente, el uso de las matemáticas modernas. En 1975, el sistema Data Encryption Standard (DES) es publicado por IBM; en 1976, W. Diffie y M. Hellman originan el concepto de Criptosistema de clave publica, es decir, un sistema donde la clave de cifrado se puede encontrar en un directorio publico de usuarios; sin embargo, la clave de descifrado es diferente y no se obtiene fácilmente de la primera. [44]. Para 1978 se crea el Criptosistema de clave pública más seguro y usado hasta la fecha, el RSA denominada así por sus inventores Ronald Linn Rivest, Adi Shamir y Len Adleman.

Expuesto por Xifré, según Palma [32] Adleman del MIT (Instituto de Tecnología de Matshachusetts ) propone la función de un solo sentido que utiliza el exponente módulo un número entero  $n$ , producto de dos números primos y que tiene como seguridad la dificultad de factorizar a un número  $n$  de entre 100 y 200 dígitos. La



necesidad de romper este Criptosistema desarrolla la teoría de factorizar números grandes, cosa que después justifica la aparición de las curvas elípticas en criptografía.

En 1988 se crea el European Institute for System Security, que entre sus objetivos esta el desarrollar investigación en todos los campos que tengan que ver con la seguridad de la información, en particular con la criptografía. Varios de sus miembros son reconocidos matemáticos. Muchas áreas de las matemáticas han podido ser usadas para crear Criptosistema, como los campos finitos y factorización de números enteros.[44]

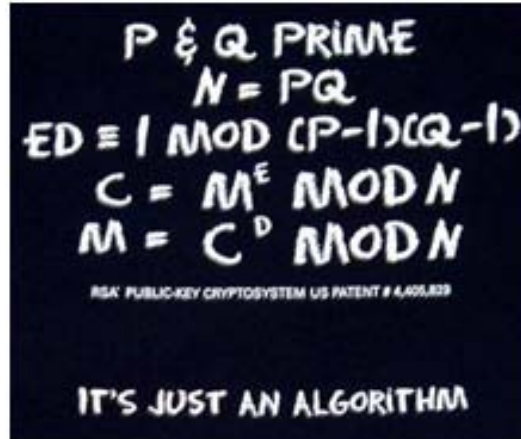


FIGURA 1.8. Factorización

Para resolver problemas de factorización se piensa en los computadores cuánticos, idea introducida por Richard Feynman en 1982, el cual usa qubits en un estado inicial controlado que representa un problema y los manipula a través de compuertas lógicas; el cálculo finaliza una vez la medición de todos los estados colapsa cada qubit a uno de dos estados puros, ahora los criptógrafos se preocuparían por la criptografía postcuántica, es decir la criptografía multivariada.

El esquema de Matsumoto-Imai (1988), es una de las propuestas iniciales de criptografía multivariada, que implica que la seguridad de este tipo de esquemas se basa en la dificultad de resolver una gran cantidad de ecuaciones polinómicas en varias variables.

La situación se tornó difícil para la criptografía, basada en los problemas de factorización y logaritmo discreto; como consecuencia al desarrollo de los computadores cuánticos es entonces, que en 1994 Moni Naor y Adi Shamir pensaron en la Criptografía visual, como posible solución a estos desafíos tecnológicos; esta técnica se sustenta en el hecho de compartir un secreto en un subconjunto de individuos de tal manera que sólo se revelará en secreto cuando todos se reúnan. Expresa A. Moreno [7] que en este tipo de esquemas el proceso de decodificación no requiere cálculos computacionales o dispositivos electrónicos, y los humanos podemos identificar más fácilmente una imagen que un computador.

Hoy en día existen varios grupos de investigación, talentosos matemáticos-científicos auspicados por grandes multinacionales están dedicados a mejorar los métodos de criptoanálisis y criptografía, apoyados en el avance de la ciencia y la tecnología.

## 1.2. Sistemas de Ecuaciones y Matrices. Desarrollo histórico

En esta sección se presenta una breve revisión del desarrollo de los sistemas de ecuaciones y las matrices a través de la historia, elemento esencial que permitirá generar en los educandos el deseo por comprender conceptos matemáticos que se desarrollarán en el Capítulo 6

### 1.2.1. Sistemas de Ecuaciones

La historia de las ecuaciones inicia a mediados del siglo XVI a. C. en Egipto con el *papiro de Rhind*, según Luzardo [33] los primeros indicios de lo que hoy se conoce como Álgebra lineal se han encontrado en este escrito matemático más antiguo que se ha conservado llegado hasta nuestros días; se encuentran algunos fragmentos en el Brooklyn Museum, y es conocido como el Libro de Cálculo, el cual fue escrito por el sacerdote egipcio Ahmés hacia el año 1650 a.C. Allí se observan las ecuaciones de primer grado, donde la incógnita aparece representada por un “*ibis*” que significa *escarbando en el suelo*, posiblemente por su aplicación a la agrimensura. Este documento contiene 85 problemas redactados en escritura hierática y fue concebido originalmente como un manual práctico para los no iniciados.

Para el año 2000 a.C. los babilonios también aportaron en la historia de los sistemas de ecuaciones, pues, sabían como resolver problemas concretos que involucraban ecuaciones de primer y segundo grado, empleando métodos de completación de cuadrados o sustitución, así como también ecuaciones cúbicas y bicuadráticas, y sistemas de ecuaciones lineales y no lineales tales como:

$$\left\{ \begin{array}{l} x \pm y = a \\ x^2 \pm y^2 = b \end{array} \right\}, \quad \left\{ \begin{array}{l} x \pm y = a \\ xy = b \end{array} \right\}, \quad \left\{ \begin{array}{l} ax + y + cz = d \\ mx + ny + p = h \\ rx + sy + qz = 0. \end{array} \right.$$

En las *tablillas de Croquetta* (2100 a.C.) se encuentra un ejemplo de estos problemas:

*“Existen dos campos cuyas áreas suman 1800 yardas cuadradas. Uno produce granos en razón de 2/3 de saco por yarda cuadrada, mientras que el otro produce granos en razón de 1/2 saco por yarda cuadrada. Si la producción total es de 1100 sacos, ¿cuál es el tamaño de cada campo?”*

Los matemáticos chinos en los siglos III y IV a.C. continuaron con el estudio de la solución de sistemas de ecuaciones con un método conocido como la regla “fan-chen”,



que en esencia, es el famoso método de eliminación gaussiana de nuestros días. En el tratado *Nueve capítulos sobre el Arte Matemático*, escrito por el científico Chuan Tsanong en el año 152 a.C. incluye los conocimientos matemáticos de la época, el cual se publicó durante la Dinastía Han, donde aparece el siguiente ejemplo de sistema lineal:

*“Hay tres clases de granos; tres gavillas de primera clase, dos de la segunda clase y una de la tercera hacen 39 medidas; dos de la primera, tres de la segunda y una de la tercera hacen 34 medidas; y una de la primera, dos de segunda y tres de la tercera hacen 26 medidas. ¿Cuántas medidas de granos están contenidas en una gavilla de cada clase?”*

$$\begin{cases} 3x + 2y + z = 39 \\ 2x + 3y + z = 34 \\ x + 2y + 3z = 26 \end{cases}$$

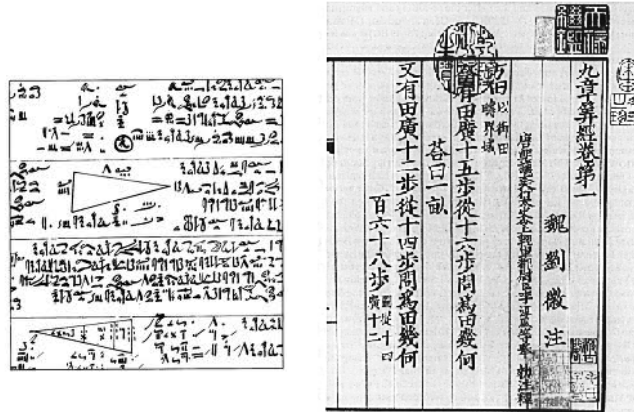


FIGURA 1.9. Papiro de Rhind y Tratado Nueve Capítulos del Arte Matemático

Este tratado fue consultado por el matemático Carl Friederich Gauss (1777-1855) en un estudio sobre la órbita del asteroide Pallas, donde obtiene un sistema de seis ecuaciones lineales en seis incógnitas y da un método sistemático para resolver tales ecuaciones, hoy día conocido como eliminación gaussiana.[33]

Leibniz y Cramer a mediados del siglo XVIII estudiaron metódicamente los sistemas de ecuaciones lineales. En 1750 Gabriel Cramer publicó la regla que lleva su nombre, para solucionar los sistemas de orden 3. A mediados del siglo XIX fue Cayley, al estudiar las matrices, quien dedujo la fórmula general para la regla y expuso la condición necesaria para que un sistema  $n \times n$  de ecuaciones lineales tuviera solución única, para ello, la matriz debería ser invertible.

A principios del siglo XIX, Gauss dedujo un método que permite resolver cualquier sistema de ecuaciones lineales, sin embargo era más complejo que la presentación matricial hecha por Cayley y por Frobenius. Jordan consiguió un algoritmo alternativo al cálculo de la inversa de una matriz presentada por Cayley, que se conoce como el algoritmo de Gauss-Jordan.

A medida que en otras disciplinas científicas se iba encontrando que los problemas se podían plantear en términos de sistemas de ecuaciones lineales, los matemáticos se empezaron a preocupar por aspectos como el número de operaciones en un algoritmo. Pronto se dieron cuenta que para el cálculo de la inversa considerada un gran número de operaciones, mientras que el método de Gauss exigía un número considerablemente menor.

Como lo explica Benitez en [27], actualmente se utiliza el método de la pivotación parcial, una ligera variante del método de Gauss, para intentar que los errores parciales sean los menores posibles. En 1948, el matemático inglés Alan Turing desarrolló la factorización LU.

### 1.2.2. Matrices

De nuevo se encuentra referenciado el libro “Nueve capítulos sobre el Arte Matemático”; en el capítulo séptimo “, Ni mucho ni poco” del chino Jiu Zhang SuanShu como uno de los primeros textos sobre el uso del método de matrices para resolver sistemas de ecuaciones; en 1683 un japonés SekiKōwa habló sobre determinantes, dos mil años antes de Gottfried Leibniz quien desarrolló su teoría a finales del siglo XVII.

En 1693, Leibniz usó un conjunto sistemático de índices para los coeficientes de un sistema de tres ecuaciones lineales con tres incógnitas obteniendo un determinante. La solución de ecuaciones lineales de dos, tres y cuatro incógnitas fue obtenida por Maclaurin en 1748 y publicada en su *Treatise of algebra*; más adelante en 1750 Gauss en el libro *Introduction à l'analyse des lignes courbes algébriques* describió la regla para determinar los coeficientes de una cónica general pasando por 5 puntos dados utilizando determinantes. En 1776 el matemático francés Bezout demostró que la anulación del determinante de un sistema de dos ecuaciones con dos incógnitas homogéneo es una condición necesaria y suficiente para que haya soluciones no nulas.

Como lo menciona Benítez [27], para el año de 1776 otro francés Alexandre-Théophile Vandermonde, fue el primero en dar una exposición coherente y lógica de la teoría de los determinantes para la solución de los sistemas de ecuaciones lineales; desarrolló una regla para calcular determinantes por medio de submatrices de orden 2. En un ensayo de 1772 “Recherches sur le calcul intégral et sur le système du monde”, Laplace generalizó el método de Vandermonde.

Gauss fue el primero en emplear la palabra *determinante* para el discriminante de la forma cuadrática  $ax^2 + 2bxy + cy^2$ ; la disposición de los elementos en tabla y la notación de subíndices dobles se le debe Augustin Cauchy quien los usó en un artículo publicado en 1815. El matemático Jacques Philippe Marie Binet investigó los fundamentos de la teoría de matrices iniciada por Cayley y otros; descubrió la regla para la multiplicación de matrices en 1812, demostrado correctamente por Cauchy, que en notación moderna es  $\det(AB) = \det(A) \det(B)$ .

Según Kine[23] El campo de las matrices estuvo bien formado aún antes de crearse. Los determinantes fueron estudiados a mediados del siglo XVIII. Un determinante contiene un cuadro de números y parecía deducirse de la inmensa cantidad de trabajos sobre los determinantes que el cuadro podía ser estudiado en sí mismo y manipulado para muchos propósitos. Quedaba por reconocer que al cuadro como tal se le podía proporcionar una identidad independiente de la del determinante. El cuadro por sí mismo es llamado matriz. La palabra matriz fue usada por primera vez por el inglés James Joseph Sylvester en 1850.

La idea de matriz como lo expone Benitez [27] es anterior a la de determinante, como lo planteó Cayley pero históricamente el orden fue el inverso. Cayley fue el primero en desarrollar de modo independiente el concepto de matriz en un artículo publicado en 1855, *A memoir on the theory of matrices*. Definió las matrices nula y unidad, la suma de matrices y señala que esta operación es asociativa y conmutativa. Cayley toma directamente de la representación del efecto de dos transformaciones sucesivas la definición de multiplicación de dos matrices. Cayley señala que una matriz  $m \times n$  puede ser multiplicada solamente por una matriz  $n \times p$ . Así mismo explica en el artículo que una matriz tiene inversa si y sólo si su determinante es nulo. Este matemático prueba que

$$A^{-1} = \frac{1}{\det(A)} \text{Adj}(A^t)$$

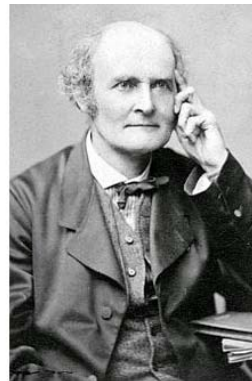


FIGURA 1.10. Inversa de una Matriz-Arthur Cayley

Cayley afirmó que el producto de dos matrices puede ser la matriz nula siendo las dos matrices invertibles. Cayley no tuvo la razón: Si  $AB = 0$ , entonces A ó B no tienen inversa. A partir de este momento los trabajos sobre matrices aumentan considerablemente; como lo fueron los trabajos de Jordan, Eugène Rouché y alemán Ferdinand Georg Frobenius. En el siglo XX la teoría de matrices es empleada en casi todos los tópicos de la matemática aplicada.

En particular Nazarosa y Roiter en los años 70s encontraron su demostración de la segunda conjetura de Brauer - Thrall sobre clasificación de álgebras, reduciéndola a un problema matricial. De hecho a un problema de la teoría de representación de conjuntos parcialmente ordenados.

## CAPÍTULO 2

---

---

### REFERENTE DISCIPLINAR

---

---

*“Tanta es la ventaja de un lenguaje bien construido que su notación simplificada a menudo se convierte en fuente de teorías profundas”*      *Pierre Simon Laplace*

### ARIMÉTICA MODULAR

#### 2.1. Congruencias

El objetivo de esta sección es introducir algunas definiciones de la Aritmética Modular, según James H. Davenport [20] y A. Moreno [6] que permitan iniciar el estudio del concepto de relación de congruencia en Criptografía desde una mirada formal y que contribuyan al diseño de las actividades de la propuesta del capítulo 6

Las congruencias constituyen una de las partes de la aritmética modular que estamos más acostumbrados a utilizar; siendo el caso del reloj la muestra más cercana a nuestra cotidianidad.

##### 2.1.1. Notación de Congruencia

La notación de congruencia, introducida por Gauss, en su obra publicada en 1801 *Disquisitiones Arithmeticae*, [45] sirve para expresar de una forma conveniente el hecho de que dos enteros  $a$  y  $b$  tienen el mismo resto al dividirlos por un número natural fijo  $m$ . Se dice que  $a$  es congruente con  $b$  respecto de la módulo  $m$ , o, en símbolos,

$$a \equiv b \pmod{m}$$

El significado de esto, entonces, es simplemente que  $a - b$  es divisible por  $m$  de otra forma es si  $m \mid a - b$ . La notación facilita los cálculos en los que múltiplos diferentes de  $m$  tienen el mismo resto, haciendo hincapié en la analogía entre la congruencia y igualdad. La congruencia, de hecho, significa “igualdad excepto por la adición de algún múltiplo de  $m$ ”.

Algunos ejemplos de congruencias válidos son:

$$24 \equiv 0 \pmod{3}, \quad 8 \equiv -1 \pmod{9}, \quad 5^2 \equiv -1 \pmod{13}$$

Una congruencia con módulo 1 es siempre válida, cualquiera que sean los dos números, ya que cada número es un múltiplo de 1.

De manera más general se tiene que si  $m$  divide a  $a$  lo cual se nota  $m \mid a$  existe un entero  $t$  tal que  $a = mt$ .

Supongamos que  $a, b$  y  $m > 0$  son números enteros. Diremos que  $a$  y  $b$  son congruentes módulo  $m$  si  $m \mid a - b$  y se simbolizará como  $a \equiv b \pmod{m}$ .

Para un entero  $m \geq 0$  fijo, se define la relación  $R_m$  sobre el conjunto de los enteros  $\mathbb{Z}$  de forma tal que se satisfaga la siguiente condición para  $(a, b) \in \mathbb{Z}^2$ :

$$(a, b) \in R_m \text{ si y solo si } b - a = tm, \text{ para algún } t \in \mathbb{Z}.$$

Que  $(a, b) \in R_m$  frecuentemente se nota  $a \equiv b \pmod{m}$ .

Con el siguiente teorema se prueba que  $R_m$  es una relación de equivalencia:

**Teorema 2.1.** *Dado un entero no negativo  $m$  fijo entonces para todo entero  $a, b, c$  se cumple:*

1.  $a \equiv a \pmod{m}$
2. Si  $a \equiv b \pmod{m}$  entonces  $b \equiv a \pmod{m}$ .
3. Si  $a \equiv b \pmod{m}$  y  $b \equiv c \pmod{m}$  entonces  $a \equiv c \pmod{m}$

### Demostración

Como  $a - a = 0 = 0m$ , para todo entero  $a$  entonces  $a \equiv a \pmod{m}$ , con lo que  $R_m$  es reflexiva

Si  $a \equiv b \pmod{m}$  entonces  $a - b = tm$ , para algún entero  $t$ , luego  $b - a = (-t)m$ , de donde  $b \equiv a \pmod{m}$ , por lo que  $R_m$  es simétrica.

Por último, si  $a \equiv b \pmod{m}$  y  $b \equiv c \pmod{m}$  entonces existen enteros  $t, t'$  tales que:

$a - b = tm$  y  $b - c = t'm$  al sumar estas dos igualdades obtenemos:

$a - c = m(t + t')$ . De donde se concluye que  $a \equiv c \pmod{m}$  y  $R_m$  es transitiva.  $\square$

El teorema que se presenta a continuación define las relaciones de equivalencia vía el algoritmo de la división.

**Teorema 2.2.** *Sea  $m$  un entero fijo entonces*

1. *Si  $a = qm + r$  entonces  $a \equiv r \pmod{m}$*
2. *Si  $0 \leq r' < r < m$ , entonces  $r \equiv r' \pmod{m}$*
3.  *$a \equiv b \pmod{m}$  si y solo si  $a$  y  $b$  tienen el mismo residuo al dividir por  $m$*

**Demostración.**

1. La primera afirmación es una consecuencia directa de la definición de relación de congruencia.
2. La segunda proposición, se obtiene al observar que si  $r \equiv r' \pmod{m}$  entonces  $m \mid r - r'$  y por lo tanto  $m \leq r - r'$ . Pero  $r - r' \leq r < m$ . Lo cual es contradictorio.
3. Si  $a \equiv b \pmod{m}$ ,  $a = qm + r$  y  $b = q'm + r'$  entonces  $a - b = hm = (q - q')m + (r - r')$ , para algún  $h \in \mathbb{Z}$ , por lo que  $r - r' = 0$  y  $r = r'$ . Por otro lado, si  $a$  y  $b$  tienen el mismo residuo al dividir por  $m$  entonces  $a = qm + r$  y  $b = q'm + r$ , luego  $a - b = m(q - q')$ , con lo que se concluye  $a \equiv b \pmod{m}$ .  $\square$

**Corolario 2.3.** *Dado  $m \geq 0$  todo entero  $a$  es congruente módulo  $m$  a exactamente uno de los números  $0, 1, 2, \dots, m - 1$*

**Demostración** Para demostrar este hecho se considera el algoritmo de la división el cual afirma que  $a \equiv r \pmod{m}$ , donde  $0 \leq r < m$ , como  $r$  es un entero concluimos  $r \in \{0, 1, 2, \dots, m - 1\}$ .

Además si  $a$  es congruente a dos de estos enteros  $r, r' \pmod{m}$ , contradiciendo la segunda parte del teorema anterior. Por lo que  $a$  solo puede ser congruente a un número en el conjunto  $\{0, 1, 2, \dots, m - 1\}$

En el caso que un entero  $t$  sea congruente a un número  $a$ ,  $0 \leq a \leq m - 1$ , se dirá que  $t$  está en la clase de  $a$  módulo  $m$ , lo cual se escribe frecuentemente en la forma  $t \in [a]$ .  $\square$

**Definición 2.4.** Sea  $a$  un entero cualquiera, entonces la clase de congruencia de  $a$  módulo  $m$ , es el conjunto

$$[a] = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}$$

El teorema 2.2 y Corolario 2.3 prueba que si  $m \in \mathbb{Z}$  es fijo, entonces, el cardinal de  $\mathbb{Z}_m = m$  esto es  $\mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$ , por ejemplo:

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$

El siguiente resultado permite definir la suma y el producto en un conjunto  $\mathbb{Z}_m$

**Teorema 2.5.** *Dos congruencias pueden sumarse, restarse o multiplicarse entre sí, siempre que todas las congruencias tengan el mismo módulo, esto es*

$$a \equiv \alpha \pmod{m} \quad \text{y} \quad b \equiv \beta \pmod{m}$$

*luego*

$$\begin{aligned} a + b &\equiv \alpha + \beta \pmod{m}, \\ a - b &\equiv \alpha - \beta \pmod{m}, \\ ab &\equiv \alpha\beta \pmod{m} \end{aligned}$$

**Demostración:** Las dos primeras de estas afirmaciones son inmediatas; por ejemplo  $(a + b) - (\alpha + \beta)$  es un múltiplo de  $m$  debido a que  $a - \alpha$  y  $b - \beta$  son ambas múltiplos de  $m$ .

El tercero no es tan inmediato y la mejor prueba es en dos pasos. primero  $ab \equiv \alpha b$  porque  $ab - \alpha b = (a - \alpha)b$ , y  $a - \alpha$  es un múltiplo de  $m$ . Siguiendo,  $\alpha b \equiv \alpha\beta$ , por una razón similar. Por lo tanto  $ab \equiv \alpha\beta \pmod{m}$ .  $\square$

Una congruencia se puede multiplicar por cualquier entero: si  $a \equiv \alpha \pmod{m}$ , entonces  $ka \equiv k\alpha \pmod{m}$ . De hecho, éste es un caso especial del tercer resultado anterior, donde  $b$  y  $\beta$  son ambos  $k$ ; sin embargo no siempre es posible cancelar un factor de la congruencia. Por ejemplo

$$42 \equiv 12 \pmod{10}$$

Se identifica que no es admisible para cancelar el factor de 6 a partir de los números 42 y 12, ya que esto daría una falsedad  $7 \equiv 2 \pmod{10}$ . La justificación sería que la primera congruencia afirma que  $42 - 12$  es un múltiplo de 10, pero esto no implica que  $\frac{1}{6}(42 - 12)$  es un múltiplo de 10. La cancelación de un factor en una congruencia es válida si el factor es un primo relativo con el módulo.

Lo anterior se describe en los siguientes resultados

**Teorema 2.6.** Si  $c > 0$ , entonces

$$a \equiv b \pmod{m} \text{ si y sólo si } ac \equiv bc \pmod{mc}$$

**Teorema 2.7. Ley de Cancelación** Si  $ac \equiv bc \pmod{m}$  y  $d = (m, c)$ , entonces

$$a \equiv b \left(\frac{m}{d}\right)$$

**Demostración:** Como  $m \mid (ac - bc)$ , se tiene que  $m \mid c(a - b)$ , y luego  $\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}(a - b)\right)$ . Por su parte, como

$$\left(\frac{m}{d}, \frac{c}{d}\right) = 1, \left(\frac{m}{d}\right) \mid (a - b),$$

se tiene

$$a \equiv b \left(\frac{m}{d}\right).$$

De lo anterior se puede verificar que si  $ac \equiv bc \pmod{m}$  y  $(c, m) = 1$ , entonces  $a \equiv b \pmod{m}$ .  $\square$

Un ejemplo del uso de las congruencias, es proporcionado por las conocidas reglas para la divisibilidad de un número por 3 o 9 o 11. La representación usual de un número  $n$  por dígitos en la escala de 10 es realmente una representación de  $n$  en la forma

$$n = a + 10b + 100c + \dots,$$

donde  $a, b, c, \dots$  son los dígitos del número, leído de derecha a izquierda, por lo que  $a$  es el número de unidades,  $b$  el número de decenas, y así sucesivamente; donde  $10 \equiv 1 \pmod{9}$ , se tiene también  $10^2 \equiv 1 \pmod{9}$ ,  $10^3 \equiv 1 \pmod{9}$  y siguientes. De ahí se deduce que la representación de  $n$  es

$$n \equiv a + b + c + \dots \pmod{9}$$

En otras palabras,  $n$  es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9. Lo mismo ocurre con el 3 en lugar del 9.

La regla para 11 se basa en el hecho de que  $10 \equiv -1 \pmod{11}$ , de manera que  $10^2 \equiv -1 \pmod{11}$ ,  $10^3 \equiv -1 \pmod{11}$  y así sucesivamente. por lo tanto

$$n \equiv a - b + c - \dots \pmod{11}$$

De ello se deduce que  $n$  es divisible por 11 si y sólo si  $a - b + c - \dots$  es divisible por 11. Por ejemplo, para comprobar la divisibilidad del 9581 por 11 formamos  $1 - 8 + 5 - 9$ , o  $-11$ . Dado que éste es divisible por 11, también lo es 9581.

Otra propiedad de las congruencias se puede observar en el teorema a continuación:



**Teorema 2.8.** Si  $\text{mcd}(a, m) = 1$  y  $r_1, r_2, \dots, r_m$  es un sistema completo de residuos módulo  $m$ , entonces  $ar_1, ar_2, \dots, ar_m$  también lo es.

**Demostración:** Se sabe que cualquier sistema completo de residuos módulo  $m$  debe tener  $m$  elementos, así, para ver que los enteros  $ar_1, ar_2, \dots, ar_m$  que son  $m$ , forman un sistema completo de residuos módulo  $m$ , basta demostrar que este conjunto no tiene elementos repetidos en el sentido de que dos elementos estén en una misma clase de equivalencia, es decir, si  $r_i \equiv r_j \pmod{p}$  si  $i = j$ . Esto debe ser cierto ya que si  $ar_i \equiv ar_j \pmod{p}$  implicaría por la ley de cancelación, que  $r_i \equiv r_j \pmod{p}$ . Esto último es una contradicción ya que  $r_1, r_2, \dots, r_m$  es un sistema completo de residuos módulo  $m$ .  $\square$

Los Teoremas de Fermat, Wilson y la función de Euler resaltan resultados valiosos en el estudio de la teoría de Números que contribuyen significativamente al desarrollo de esta propuesta; los cuales se presentan a continuación.

### 2.1.2. El Teorema de Fermat

El teorema de Fermat es uno de los teoremas clásicos de Teoría de Números relacionado con la divisibilidad. Fermat descubrió que si el módulo es un número primo, digamos  $p$ , entonces cada  $x$  enteros no congruente a 0 satisface

$$a^{p-1} \equiv 1 \pmod{p} \quad (2.1.1)$$

Esto quiere decir que, si se eleva un número a la  $p$ -ésima potencia y al resultado se le resta  $a$ , lo que queda es divisible por  $p$ . Su interés principal está en su aplicación al problema de la primalidad y en criptografía.

Para demostrar el teorema de Fermat se utiliza el teorema anterior de un sistema completo de residuos modulo  $m$ .

**Demostración:** Suponemos primero que  $p \nmid a$ . Como  $0, 1, 2, 3, \dots, p-1$  es un sistema completo de residuos módulo  $p$  y  $\text{mcd}(a, p) = 1$  se sabe que por el teorema sistema completo de residuos modulo  $p$  que  $0a, 1a, 2a, \dots, (p-1)a$  también es un sistema completo de residuos módulo  $p$ . Como  $0a = 0$  se tiene que  $1a, 2a, \dots, (p-1)a$  es un reordenamiento, módulo  $p$  de  $1, 2, \dots, p-1$ . Así,

$$\begin{aligned} 1a, 2a, \dots, (p-1)a &\equiv 1, 2, \dots, p-1 \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ p(a^{p-1} - 1)(p-1)! & \end{aligned}$$

Dado que  $p \nmid (p-1)!$ , pues  $p$  es primo, se tiene que  $a^{p-1} - 1 \equiv 0 \pmod{p}$ , es decir  $a^{p-1} \equiv 1 \pmod{p}$  de donde se obtiene el resultado. Para completar la demostración basta multiplicar  $a^{p-1} \equiv 1 \pmod{p}$  por  $a$ , para obtener  $a^p \equiv a \pmod{p}$  que sería cierto para  $p \nmid a$ , y es cierta en el caso que  $p \mid a$ .  $\square$

Teniendo en cuenta lo descrito anteriormente, esto es equivalente a decir que el orden de cualquier número es un divisor de  $p - 1$ . El resultado 2.1.1 se mencionó por Fermat en una carta a Frénicle de Bessy el 18 de octubre de 1640, en la que también afirmó que no tenía una prueba. Pero como con la mayoría de los descubrimientos de Fermat, la prueba no fue publicada o reservada. La primera prueba conocida fue dada por Leibniz (1646-1716). Demostró que  $x^p \equiv x \pmod{p}$ , que es equivalente a 2.1.1, escribiendo  $x$  como una suma  $1 + 1 + \dots + 1$  de  $x$  unidades (suponiendo que  $x$  es positiva), y luego la expansión de  $(1 + 1 + \dots + 1)^p$  por el teorema multinomial. Los términos  $1^p + 1^p + \dots + 1^p$  dan  $x$ , y los coeficientes de todos los otros términos son divisible por  $p$ .

### 2.1.3. Teorema de Wilson

Este teorema fue publicado por primera vez por Waring en su *Meditationes Algebraicae* de 1770, y fue atribuida por él a Sir John Wilson (1741-1793), un abogado que había estudiado matemáticas en Cambridge.

El siguiente resultado se conoce como el Teorema de Wilson

**Teorema 2.9.** *Si  $p$  es primo entonces  $(p - 1)! \equiv -1 \pmod{p}$*

**Demostración:** La siguiente prueba fue dada por Gauss, esta se basa en asociar cada uno de los números  $1, 2, \dots, p - 1$  con su recíproco  $\pmod{p}$ . El recíproco de  $a$  es  $a'$  para el cual  $aa' \equiv 1 \pmod{p}$ . Cada número de la serie  $1, 2, \dots, p - 1$  tiene exactamente un recíproco en el conjunto. El recíproco de  $a$  puede ser el mismo, pero, esto sólo ocurre si  $a^2 \equiv 1 \pmod{p}$ , es decir, si  $a \equiv \pm 1 \pmod{p}$ , el cual requiere  $a = 1$  o  $a = p - 1$ . Además de estos dos números, los restantes  $2, 3, \dots, p - 2$  se pueden combinar de manera que el producto de aquellos en cualquier par es  $\equiv 1 \pmod{p}$ . Resulta que

$$2 \times 3 \times 4 \times \dots \times (p - 2) \equiv 1 \pmod{p}$$

Multiplicando por  $p - 1$ , que es  $\equiv -1 \pmod{p}$ , se obtiene el resultado del Teorema 2.9. La prueba que se acaba de dar demuestra un error si  $p$  es 2 ó 3, pero se comprueba inmediatamente que el resultado sigue siendo cierto.  $\square$

El teorema de Wilson es uno de una serie de teoremas que se refieren a la simétrica funciones de los números  $1, 2, \dots, p - 1$ . Se afirma que el producto de estos números es congruente a  $-1 \pmod{p}$ . También se conocen muchos resultados relativos a otras funciones simétricas. Como ejemplo, se considera la suma de las potencias  $k$ ésimas de estos números:

$$S_k = 1^k + 2^k + \dots + (p - 1)^k$$

donde  $p$  es un número primo mayor que 2. Se puede demostrar que  $S_k \equiv 0 \pmod{p}$  excepto cuando  $k$  es un múltiplo de  $p - 1$ . En este último caso, cada término de la suma es  $\equiv 1$  por el teorema de Fermat, y hay  $p - 1$  términos, de modo que la suma es  $\equiv p - 1 \equiv -1 \pmod{p}$ .

### 2.1.4. La función de Euler $\phi(m)$

La función de Euler y algunos teoremas como los de Fermat y Wilson permiten observar la potencia de esta teoría para resolver problemas de la Aritmética Modular.

Euler definió esta función así: Si un número natural  $n$  tiene una descomposición en factores primos de la forma  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  entonces la función de Euler,  $\phi$ , le asigna a  $n$  el producto

$$n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

Entre una de las propiedades de la función de Euler se encuentra:

*Si  $p$  es primo y  $m$  un número natural, entonces*

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1) \quad (2.1.2)$$

Se podría probar lo anterior, sabiendo que  $\phi(p^a) = p^a \left(1 - \frac{1}{p}\right) = \phi(p)$

Así mismo, la determinación de  $\phi(m)$  para los valores generales de  $m$  se efectúa probando que esta función es multiplicativa la cual determina otra propiedad.

*Si  $a$  y  $b$  dos números primos relativos entre sí, luego*

$$\phi(ab) = \phi(a)\phi(b) \quad (2.1.3)$$

Para probar esto, se inicia por observar un principio general: si  $a$  y  $b$  son primos relativos entre sí, dos congruencias simultáneas de la forma

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b} \quad (2.1.4)$$

son precisamente equivalente a una congruencia con el módulo  $ab$ . Para la primera congruencia significa que  $x = \alpha + at$  donde  $t$  es un número entero. Esto satisface la segunda congruencia si y sólo si

$$\alpha + at \equiv \beta \pmod{b}, \quad at \equiv \beta - \alpha \pmod{b}$$

es una congruencia lineal soluble para  $t$ . De ahí las dos congruencias 2.1.4 son simultáneamente solubles. Si  $x$  y  $x'$  dos soluciones, tenemos  $x \equiv x' \pmod{a}$  y  $x \equiv x' \pmod{b}$ , y por lo tanto  $x \equiv x' \pmod{ab}$ . Es decir, hay exactamente una solución para el módulo  $ab$ . Este principio, que se extiende a varias congruencias, con la condición de que los módulos sean primos relativos se llama “**el teorema chino de los residuos**”. El cual asegura la existencia de los números que dejan residuos prescritos en la división por los módulos en cuestión.

Se representará la solución de los dos congruencias 2.1.4 por

$$x \equiv [\alpha, \beta] \pmod{ab}$$

de manera que  $[\alpha, \beta]$  es un número determinado dependiendo de  $\alpha$ ,  $\beta$ ,  $a$  y  $b$  que se establece de forma única para el módulo  $ab$ .

Para ilustrar la situación anterior planteada; para  $\phi(a)\phi(b)$  se asignan los valores de  $a = 5$  y  $b = 8$ ; los posibles valores para  $\alpha$  son 0, 1, 2, 3, 4, y de  $\beta$  son 0, 1, 2, 3, 4, 5, 6, 7. De estos hay cuatro valores de  $\alpha$  que son primos relativos a  $a$ , dado que  $\phi(5) = 4$ , y cuatro valores de  $\beta$  que son primos relativos para  $b$ , debido a que  $\phi(8) = 4$ , de acuerdo con la fórmula 2.1.2. Para este ejemplo se tiene dieciséis que son primos relativos entre 40 y menores de 40, verificando de este modo que  $\phi(40) = \phi(5)\phi(8) = 4 \times 4 = 16$ .

Si ahora se evalúa  $\phi(m)$  para cualquier número  $m$ . La factorización de  $m$  en potencias primas sería

$$m = p^a q^p \dots$$

A continuación, se sigue de 2.1.2 y 2.1.3 que

$$\phi(m) = (p^a - p^{a-1})(q^b - q^{b-1}) \dots$$

o, de otra manera,

$$\phi(m) = m \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \dots \quad (2.1.5)$$

Por ejemplo

$$\phi(40) = 40 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 16$$

y

$$\phi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 16$$

La función  $\phi(m)$  tiene una notable propiedad, primero dada por Gauss en su *Disquisitiones*. Es que la suma de los números  $\phi(d)$ , puede extenderse sobre todos los divisores  $d$  de un número  $m$ , es igual al mismo  $m$ . Por ejemplo, si  $m = 12$ , la divisores son 1, 2, 3, 4, 6, 12, y tenemos

$$\begin{aligned} \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ = 1 + 1 + 2 + 2 + 2 + 4 = 12 \end{aligned}$$

Una prueba general puede basarse ya sea en 2.1.5, o directamente en la definición de la función.

Se prosigue a enunciar el Teorema Chino de los Residuos que tiene importantes aplicaciones en criptografía, en especial para reducir operaciones con números enormes mediante el paso a congruencias.

**Teorema 2.10.** *Si  $m$  y  $m'$  son primos relativos entonces las congruencias:*

$$x \equiv b \pmod{m}, \quad x \equiv b' \pmod{m'}$$

*tienen una solución común. Además las dos soluciones son congruentes  $\pmod{mm'}$ .*

**Demostración:** Toda solución de la primera congruencia tiene la forma  $x = b + km$ , para algún entero  $k$ .

Entonces, se debe encontrar  $k$  tal que  $b + km \equiv b' \pmod{m'}$ . Esto es,  $km \equiv b - b' \pmod{m'}$ . Como  $(m, m') = 1$ , se puede asegurar la existencia de tal  $k$  debido a que existen enteros  $s, s'$  tales que  $sm + s'm' = 1$ . De hecho  $k \equiv m^{-1}(b - b') \pmod{m'}$ .

Ahora si  $y$  es otra solución entonces  $m$  y  $m'$  dividen a  $x - y$ . Luego  $mm' \mid x - y$  y por lo tanto  $x \equiv y \pmod{mm'}$ .  $\square$

El caso general:

Si  $m_1, m_2, \dots, m_r$  son números primos relativos dos a dos y  $a_1, a_2, \dots, a_r$  son enteros. Entonces el sistema de congruencias de  $x \equiv a_i \pmod{m_i} (1 \leq i \leq r)$  tiene una única solución módulo  $M = m_1 \times m_2 \times \dots \times m_r$ . Dada por

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

En donde  $M_i = M/m_i$  y  $y_i = M_i^{-1} \pmod{m_i}, 1 \leq i \leq r$ .

A modo de ejemplo para el siguiente sistema de congruencias

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ 3x &\equiv -6 \pmod{15} \end{aligned}$$

El anterior sistema es equivalente, aplicando propiedades de las congruencias a

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv -2 \pmod{5} \end{aligned}$$

Como  $(8, 5) = 1$  Se aplica el Teorema Chino de los residuos, con el cual se tiene, el módulo  $M = (8)(5) = 40$

$i$	Congruencia	$m_i$	$M_i = \frac{M}{m_i}$	$a_i$	$y_i = M_i^{-1} \pmod{m_i}$
1	$x \equiv 3 \pmod{8}$	8	5	3	$5^{-1} \pmod{8} = 5$
2	$x \equiv -2 \pmod{5}$	5	8	-2	$8^{-1} \pmod{5} = 2$

Se tiene

$$x = (3 \times 5 \times 5) + (-2 \times 8 \times 2) \pmod{40}$$

$$x = 43 \pmod{40} \equiv 3 \pmod{40}$$

Para este ejemplo, la solución es  $x = 3$

Para continuar con el estudio de las congruencias, se examinará lo concerniente a ecuaciones de congruencias lineales, temática importante para la propuesta didáctica y sistemas criptográficos del capítulo 3

### 2.1.5. Ecuaciones de Congruencia Lineales

Se tiene que cada número entero es congruente módulo  $m$  a exactamente uno de los números

$$0, 1, 2, \dots, m - 1 \quad (2.1.6)$$

Para que se pueda expresar un número entero en forma  $qm + r$ , donde  $0 \leq r < m$ , y éste congruente con  $r \pmod{m}$ . Existen otros conjuntos de números, además del conjunto 2.1.6, que tienen la misma propiedad, por ejemplo, cualquier número entero es congruente  $\pmod{5}$  exactamente a uno de los números  $0, 1, -1, 2, -2$ . Se dice que cualquier conjunto de números puede constituir un conjunto completo de los residuos módulo  $m$ . Otra forma de expresar la definición, es decir que un conjunto completo de residuos  $\pmod{m}$  es un conjunto de números  $m$ , donde no hay dos números congruentes entre sí.

Una congruencia lineal, por analogía con una ecuación lineal es de la forma

$$ax \equiv b \pmod{m} \quad (2.1.7)$$

Es un hecho importante que este tipo de congruencia es soluble para  $x$ , siempre que  $a$  sea primo relativo con  $m$ . El teorema que se presente a continuación describe lo anterior

**Teorema 2.11.** *Si  $(a, m) = 1$  entonces la congruencia  $ax \equiv b \pmod{m}$  tiene solución para  $x$  y dos de tales soluciones son congruentes módulo  $m$ .*

**Demostración:** Como  $(a, m) = 1$  entonces existen enteros  $s, t$ , tales que  $as + mt = 1$ , luego  $asb + mtb = b$ , con lo se concluye  $asb \equiv b \pmod{m}$  y de esto  $asb \equiv b \pmod{m}$ , por lo que  $x = sb$  es la solución buscada.

Si  $y$  es otra solución entonces  $ax \equiv ay \pmod{m}$  y por lo tanto  $m \mid a(x - y)$  y como  $(a, m) = 1$  entonces  $m \mid x - y$  y por lo tanto  $x \equiv y \pmod{m}$ .

**Corolario 2.12.** *Si  $a$  no es divisible por un primo dado  $p$  entonces la congruencia  $ax \equiv b \pmod{p}$  siempre tiene solución.*

**Demostración:** Como  $p$  es primo y  $p \nmid a$  entonces  $(a, p) = 1$ .

Otra forma de probar los resultados anteriores, es observar que si  $x$  va a través de los números de un conjunto completo de residuos, los valores correspondientes de  $ax$

también constituyen un conjunto completo de los residuos. Porque hay  $m$  de estos números, y no hay dos de ellos que sean congruentes, donde  $ax_1 \equiv ax_2 \pmod{m}$  implicaría  $x_2 \equiv x_1 \pmod{m}$ , por la ley de cancelación del factor  $a$  (permitido desde que  $a$  sea primo relativo con  $m$ ).

Debido a que los números  $ax$  forman un conjunto completo de los residuos, habrá exactamente uno de ellos congruentes con el número dado  $b$ .

Como ejemplo, se considera la congruencia

$$3x \equiv 5 \pmod{11}$$

Si se dan a  $x$  los valores  $0, 1, 2, \dots, 10$  (un conjunto completo de los residuos módulo 11),  $3x$  toma los valores  $0, 3, 6, \dots, 30$ . Estos forman otro conjunto completo de residuos módulo 11, y de hecho son congruentes, respectivamente, a

$$0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8.$$

El valor 5 se produce cuando  $x = 9$ , y por lo que  $x = 9$  es una solución de la congruencia. Naturalmente cualquier número congruente a 9 módulo 11 también satisface la congruencia; se puede decir que la congruencia tiene *una* solución, lo que significa que hay una solución en cualquier conjunto completo de los residuos. En otras palabras, todas las soluciones son mutuamente congruentes. Lo mismo se aplica a la congruencia 2.1.7; una congruencia tal (siempre que  $a$  sea primo relativo con  $m$ ) equivale exactamente a la congruencia  $x \equiv x_0 \pmod{m}$ , donde  $x_0$  es una solución particular.

El hecho de que la congruencia 2.1.7 tiene una solución única, en el sentido, sugiere que se puede utilizar esta solución como una interpretación para la fracción  $\frac{b}{a}$  para el módulo  $m$ . Cuando se hace esto, se obtiene una aritmética módulo  $m$  en el que la suma, resta y multiplicación son siempre posibles, la división también es posible con la condición de que el divisor sea primo relativo con  $m$ . En esta aritmética sólo hay un número finito distintos, a saber  $m$  de ellos, ya que dos números que son mutuamente congruentes módulo  $m$  son tratados como iguales. Si se toma 11 como el módulo  $m$ , algunos ejemplos de “la aritmética módulo 11” son:

$$5 + 7 \equiv 1, \quad 5 \times 6 \equiv 8, \quad \frac{5}{3} \equiv 9 \equiv -2$$

Cualquier relación que conecta los números enteros o fracciones en el sentido ordinario sigue siendo cierto cuando se interpreta en esta aritmética. Por ejemplo, la relación

$$\frac{1}{2} + \frac{2}{3} = \frac{7}{6}$$

se convierte en  $\pmod{11}$

$$6 + 8 \equiv 3$$

porque la solución de  $2x \equiv 1$  es  $x \equiv 6$ , que de  $3x \equiv 2$  es  $x \equiv 8$ , y que de  $6x \equiv 7$  es  $x \equiv 3$ . La interpretación dada a una fracción depende del módulo, por ejemplo  $\frac{2}{3} \equiv 8 \pmod{11}$ , pero  $\frac{2}{3} \equiv 3 \pmod{7}$  la única limitación de este tipo de cálculos que se acaba de mencionar, a saber, que los denominadores de las fracciones deben ser primos relativos al módulo. Si el módulo es un primo (como en los ejemplos anteriores con 11), la limitación toma una forma muy simple, que el denominador no debe ser congruente a 0 mód  $m$ , y esto es exactamente análogo a la limitación en la aritmética ordinaria que el denominador no debe ser igual a 0.

### 2.1.6. Congruencias Algebraicas

La analogía entre las congruencias y ecuaciones sugiere la consideración de congruencias algebraicas, es decir, congruencias de la forma

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x_1 + a_0 \equiv 0 \pmod{m} \quad (2.1.8)$$

donde  $a_n, a_{n-1}, \dots, a_0$  son números enteros, y  $x$  es un desconocido. Es interesante preguntar hasta qué punto la teoría de ecuaciones algebraicas se aplica a congruencias algebraicas, y de hecho el estudio de congruencias algebraicas constituye en diversas formas una parte importante de la teoría de los números.

Si  $n = 1$ , para el grado de la congruencia, en la fórmula 2.1.8 se reduce a  $a_1 x + a_0 \equiv 0 \pmod{m}$  que es una congruencia lineal. Si un número  $x_0$  satisface una congruencia algebraica para el módulo  $m$ , a continuación, lo mismo ocurre con cualquier número  $x$  que es congruente a  $x_0 \pmod{m}$ . Por lo tanto dos soluciones para la congruencia pueden ser consideradas como la misma, el número de soluciones de la congruencia es algún conjunto completo de residuos mód  $m$ , por ejemplo, en el conjunto  $0, 1, \dots, m-1$ . La congruencia  $x^3 \equiv 8 \pmod{13}$  se cumple cuando  $x \equiv 2$  o  $5$  o  $6 \pmod{13}$ , y no de otro modo, y por lo tanto tiene tres soluciones.

Un principio importante en las congruencias algebraicas; es que para de determinar el número de soluciones de una congruencia, es suficiente tratar el caso cuando el módulo es la potencia de primo.

Para ver esto, se supone que el módulo  $m$  se puede factorizar como  $m_1 m_2$ , donde  $m_1$  y  $m_2$  son primos entre sí. Una congruencia algebraica

$$f(x) \equiv 0 \pmod{m} \quad (2.1.9)$$

se satisface por un número  $x$  si y sólo si ambas congruencias lo son también.

$$f(x) \equiv 0 \pmod{m_1} \quad y \quad f(x) \equiv 0 \pmod{m_2} \quad (2.1.10)$$



Si cualquiera de ellas es insoluble, a continuación, la congruencia dada es insoluble. Si ambas son solubles, entonces la solución estaría dada por

$$x \equiv \xi_1, x \equiv \xi_2, \dots \pmod{m_1}$$

y los de este último por

$$x \equiv \eta_1, x \equiv \eta_2, \dots \pmod{m_2}$$

Cada solución de 2.1.9 corresponde a alguna de las  $\xi$  y las  $\eta$ . Por el contrario, si seleccionamos una de las  $\xi$ , por ejemplo  $\xi_i$ , y uno de los  $\eta$ , decir  $\eta_j$ , las congruencias simultáneas

$$x \equiv \xi_i \pmod{m_1} \quad y \quad x \equiv \eta_j \pmod{m_2}$$

son equivalentes, exactamente a una congruencia para el módulo  $m$ . De ello se deduce que si  $N(m)$  denota el número de soluciones de la congruencia 2.1.9, y  $N(m_1)$  y  $N(m_2)$  denotan los números de soluciones de las dos congruencias 2.1.10, luego

$$N(m) = N(m_1)N(m_2)$$

En otras palabras,  $N(m)$  es una función multiplicativa de  $m$ . Si  $m$  se factoriza en potencias de primas de la forma usual, entonces

$$N(m) = N(p^a)N(q^b) \dots \quad (2.1.11)$$

Es decir, si se conoce el número de soluciones de una congruencia algebraica para cada módulo de potencia prima, se puede deducir que el número de soluciones para un módulo en general por la multiplicación. En particular, si uno de los números  $N(p^a)$  es cero para una de las potencias primas que componen  $m$ , entonces la congruencia es insoluble.

Un resultado similar se mantiene para congruencias algebraicas. El número de soluciones de una congruencia

$$f(x, y) \equiv 0 \pmod{m}$$

con dos incógnitas (y de manera similar en cualquier número de incógnitas) es de nuevo una función multiplicadora del módulo.

### 2.1.7. Sistema de Cubrimiento para los Números Enteros

Un problema curioso es el de encontrar conjuntos de congruencias, a módulos distintos, de tal modo que cada número satisface al menos una de las congruencias.

Un sistema de cubrimiento es una colección de congruencias de la forma  $x \equiv a_i \pmod{m_i}$  con  $1 \leq i \leq k$  y  $m_i \geq 1$  enteros tales que todo entero satisface al menos una de las congruencias. Las congruencias

$$x \equiv 0 \pmod{2}, \quad 0 \pmod{3}, \quad 1 \pmod{4}, \quad 1 \pmod{6}, \quad 11 \pmod{12}$$

constituyen un conjunto de cubrimiento. Los dos primeros cubren todos los números excepto los congruentes a 1 o 5, 7 o 11 módulo 12. De éstos, 1 y 5 están cubiertos por  $x \equiv 1 \pmod{4}$ , 7 está cubierto por  $x \equiv 1 \pmod{6}$ , y 11 está cubierto por la última congruencia.

Erdős ha propuesto el problema: dado cualquier número  $N$ , existe un conjunto de congruencias que cubra sólo los módulos mayores que  $N$ ? probablemente esto es cierto, pero no es fácil ver cómo dar una prueba. Erdős mismo tiene un ejemplo: dado un conjunto que no utiliza el módulo 2, con módulos diferentes de 120. También se describen otros casos en R.K. Guy [19] como los de Churchouse el cual ha dado un conjunto para el cual el menor módulo es 9; aquí los módulos son diversos factores de 604.800; también Choi ha demostrado que hay un conjunto con menos de módulo 20, y Gibson uno con menos de módulo 25. La cuestión de si existe o no un sistema con cada módulo impar es todavía una pregunta abierta.

Existe otro resultado interesante que se muestra en el siguiente teorema:

**Teorema 2.13.** *No hay sistemas de cubrimientos exactos con módulos distintos*

**Demostración:** Sean  $m_1 \dots m_k$  los distintos módulos de las congruencias en un sistema de cubrimiento exacto. Para  $1 \leq i \leq k$ , los enteros positivos que satisfacen la congruencia  $x \equiv a_i \pmod{a_i}$  y que están representadas por la función de generación

$$x^{a_i} + x^{a_i+m_i} + x^{a_i+2m_i} + \dots = \frac{x^{a_i}}{1-x^{m_i}}$$

Por lo tanto  $\sum_{i=1}^k \frac{x^{a_i}}{1-x^{m_i}} = \frac{1}{1-x}$

Debido a que  $1/(1-x)$  es la función generadora para el conjunto de todos los enteros positivos.

Ahora, al lado derecho es una función racional con sólo una discontinuidad (llamado polo) en  $x = 1$ . Sea  $m$  el máximo de  $m_i$  (los cuales son distintos). En el lado izquierdo del término  $x^{a_m}/(1-x^{m_i})$  tiene una discontinuidad en  $x = e^{2\pi i m}$  y ninguna otra discontinuidad para cancelar. Esto es una contradicción, Por lo tanto, no hay un sistema exacto de cubrimiento con módulos distintos.  $\square$

Caso contrario para este ejemplo:

$$x \equiv a_i \pmod{m_i}$$

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{2} \end{cases}$$

$\mathbb{Z}_2$  es un sistema de cubrimiento exacto.

# SISTEMAS DE ECUACIONES LINEALES Y DETERMINANTES

## 2.2. Sistema de Ecuaciones Lineales

Los sistemas de ecuaciones lineales también objeto de estudio en esta propuesta se definen a continuación, según A. Kurosh [24] Capítulo 2 y A.Cofré [21]. Para este trabajo  $K$  es el campo de los números reales.

Se define una *ecuación lineal* con  $n$  incógnitas a una ecuación de tipo

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b \quad (2.2.12)$$

Los números  $a_1, \dots, a_n$  se denominan coeficientes de las incógnitas, al número  $b$  se le llama término independiente. La colección ordenada de números  $(k_1, k_2, \dots, k_n)$  es una solución de la ecuación si

$$a_1k_1 + a_2k_2 + \dots + a_nk_n = b$$

Si  $b = 0$  la ecuación se dice homogénea. Debido que alguno de los coeficientes  $a_i$  en 2.2.12 debe ser distinto de cero, se puede suponer que  $a_1 \neq 0$ . Se asignan valores arbitrarios  $k_2, k_3, \dots, k_n$  a las incógnitas  $x_2, x_3, \dots, x_n$ , entonces

$$x_1 = \frac{b - a_2k_2 - a_3k_3 - \dots - a_nk_n}{a_1}$$

La colección ordenada  $\left(\frac{b - a_2k_2 - a_3k_3 - \dots - a_nk_n}{a_1}, k_2, k_3, \dots, k_n\right)$  es una posible solución de la ecuación. Puesto que esta es solución independientemente de cuáles son los valores de  $k$  se concluye que 2.2.12 tiene infinitas soluciones.

**Definición 2.14.** Sean

$$a_1x_1 + \dots + a_nx_n = c_1 \quad (2.2.13)$$

$$b_1x_1 + \dots + b_nx_n = c_2 \quad (2.2.14)$$

Sean  $\alpha$  y  $\delta$  números arbitrarios, se dirá que la ecuación

$$\alpha(a_1x_1 + \dots + a_nx_n) + \beta(b_1x_1 + \dots + b_nx_n) \quad (2.2.15)$$

es una combinación lineal de las ecuaciones anteriores. 2.2.13 y 2.2.14.

Sea  $(k_1, k_2, \dots, k_n)$  una solución común de las ecuaciones 2.2.13 y 2.2.14. Entonces  $\alpha(a_1x_1 + \dots + a_nx_n) + \beta(b_1x_1 + \dots + b_nx_n) = \alpha c_1 + \beta c_2$  y  $(k_1, k_2, \dots, k_n)$  es solución de la ecuación 2.2.15

Se concluye que si una ecuación es combinación lineal de dos o más ecuaciones lineales entonces toda solución común de las ecuaciones que participan en la combinación lineal es solución de la ecuación.

**Nota:** A una colección ordenada del tipo  $(k_1, k_2, \dots, k_n)$  se llamará  $n$ -tupla.

**Definición 2.15.** Un sistema de ecuaciones lineales de  $n$  incógnitas es un conjunto de  $m$  ecuaciones en la forma:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = c_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = c_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = c_m \end{cases} \quad (2.2.16)$$

Se dice que la  $n$ -tupla  $(k_1, k_2, \dots, k_n)$  es solución del sistema si es solución de cada una de las  $m$  ecuaciones. Si  $c_1 = c_2 = \dots = c_m = 0$  se constituirá como un sistema homogéneo.

En particular, en un sistema de ecuaciones lineales con dos incógnitas y dos ecuaciones se tiene sólo uno de los tres siguientes casos.

1. El sistema tiene única solución si y sólo si  $a_{11}a_{22} - a_{12}a_{21} \neq 0$
2. Si  $a_{11}a_{22} - a_{12}a_{21} = 0$  y  $a_{11}, a_{12}$  y  $b_1$  son múltiplos de  $a_{12}, a_{22}$  y  $b_2$  respectivamente, entonces el sistema tiene infinitas soluciones.
3. Si  $a_{11}a_{22} - a_{12}a_{21} = 0$  y  $a_{11}, a_{12}$  son múltiplos de  $a_{12}, a_{22}$ , pero  $b_1$  no lo es de  $b_2$ , entonces el sistema no tiene solución

## 2.3. Determinantes

Sea  $A = (a_{ij})$  una matriz cuadrada de  $n \times n$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \quad (2.3.17)$$

Se consideran todos los productos posibles de  $n$  elementos de  $(a_{ij})$  donde cada producto contiene exactamente un elemento de cada fila y uno de cada columna, esto es, todos los productos de la forma

$$a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n} \quad (2.3.18)$$

donde los subíndices  $\alpha_1, \alpha_2 \dots \alpha_n$  constituyen un arreglo de donde los números  $1, 2, \dots, n$ . Para formar 2.3.18 se puede elegir primero un elemento de la primera fila de  $(a_{ij})$ , a saber  $a_{1\alpha_1}$ , luego uno de la segunda fila,  $a_{2\alpha_2}$  donde  $a_{2\alpha_2}$  no puede estar en la columna  $\alpha_1$ , esto es,  $\alpha_1 \neq \alpha_2$ , luego uno de la tercera fila  $a_{3\alpha_3}$ , así mismo  $a_{3\alpha_3}$  no puede estar en las columnas  $\alpha_1$  o  $\alpha_2$  esto es  $\alpha_1 \neq \alpha_2 \neq \alpha_3$  y así se continua hasta la fila  $n$ , se puede concluir que hay  $n!$  de estos productos ya que en 2.3.18 los índices fila siempre pueden escribirse en el orden natural.

Para determinar el signo de los productos en 2.3.18, se tiene que si la sustitución es par se mantiene dicho signo, si es impar se multiplica por  $-1$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix}$$

A la suma algebraica de estos  $n!$  productos de la forma  $a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n}$  con los signos adjudicados mediante la regla enunciada, se denomina *determinante* de orden  $n$  correspondiente a la matriz  $(a_{ij})$ . Si  $n = 1$  se dirá que  $a_{11}$  es el determinante de orden 1 de la matriz  $(a_{11})$

El determinante de una matriz  $A = (a_{ij})$  se denota por

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$\det A = \sum_{\alpha} (sgn \alpha) a_{1\alpha(1)} a_{2\alpha(2)} \cdots a_{n\alpha(n)},$$

donde la suma se toma sobre todas las permutaciones de los elementos de  $S = 1, \dots, n$ . Cada término de la suma es un producto de  $n$  elementos, cada uno tomado de un renglón diferente de  $A$  y  $sgn \alpha$ . El número  $n$  se llama orden del determinante.

Se puede describir el caso para  $n = 2$  con el siguiente ejemplo

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\begin{vmatrix} -5 & 8 \\ 3 & 2 \end{vmatrix} = (-5) \cdot 2 - 8 \cdot 3 = -34$$

Para  $n = 3$  se observa el ejemplo

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$$

$$\begin{vmatrix} 4 & -1 & 3 \\ 2 & 0 & -2 \\ 1 & -3 & 1 \end{vmatrix}$$

$$= 4 \cdot 0 \cdot 1 + (-1) \cdot (-2) \cdot 1 + 3 \cdot 2 \cdot (-3) - (-1) \cdot 2 \cdot 1 - 3 \cdot 0 \cdot 1 - 4 \cdot (-2) \cdot (-3) = -26$$

En general, un determinante de orden  $n$  será la suma de  $n!$  productos.

### 2.3.1. Propiedades de los Determinantes

Se necesario, definir primero cómo es la transpuesta de una matriz para introducir las propiedades de los determinantes.

**Definición 2.16.** Sea  $A = (a_{ij})$  una matriz cuadrada de orden  $n$ , se obtiene la matriz transpuesta de  $A$  como  $A^t$  poniendo las filas de  $A$  como columnas de  $A^t$

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$$

**Propiedad 1:** El determinante de  $A$  es igual al determinante  $A^t$

Ambos determinantes tienen los mismos términos, hay que demostrar que el mismo término tiene el mismo signo en  $\det A$  y en  $\det A^t$ .

Sea

$$a_{1\alpha_1} a_{2\alpha_2} \cdots a_{n\alpha_n}$$

un término del  $\det A$ . Si a  $B = (b_{ij})$  se llama  $A^t$  tal término es en  $\det B$

$$b_{1\alpha_1} b_{2\alpha_2} \cdots b_{n\alpha_n}$$

Si se reordena los factores de modo que el producto quede en la forma canónica  $b_{1\gamma_1} b_{2\gamma_2} \cdots b_{n\gamma_n}$ , esto sería lo mismo que llevar la sustitución

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 2 & \cdots & n \end{pmatrix} \text{ a la forma } \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \gamma_1 & \gamma_2 & \gamma_3 & \cdots & \gamma_n \end{pmatrix}$$

Pero esta última tiene la paridad que  $\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ 1 & 2 & \cdots & n \end{pmatrix}$  la cual a su vez tiene la misma paridad que  $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix}$  la suma del número de inversiones es la misma.

Se concluye que  $a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n}$  tiene el mismo signo considerado como término de  $\det B$

**Propiedad 2:** Si alguna de la fila de un determinantes contiene ceros, el determinante es cero, es decir, para algún  $i$   $1 \leq i \leq n$ ,  $a_{ij} = 0$  para todo  $j = 1, 2, \dots, n$  entonces  $\det A = 0$

En efecto, cada término contiene un factor de la  $i$ -ésima fila, luego todos los términos son iguales a cero.

**Propiedad 3:** Si un determinante se obtiene de otro permutando dos filas todos los términos del primer determinante serán términos del segundo pero con signos contrarios, es decir, al permutar dos filas el determinante sólo cambia de signo.

Supongamos que permutamos las filas  $i$  y  $j$ ,  $i < j$ . Sea  $(b_{ij})$  la matriz que se obtiene al permutar las filas.

Se considera un término cualquiera del determinante original.

$$a_{1\alpha_1} a_{2\alpha_2} \dots a_{i\alpha_i} \dots a_{j\alpha_j} \dots a_{n\alpha_n}$$

y su signo está determinado por la paridad de

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_i & \cdots & \alpha_j & \cdots & \alpha_n \end{pmatrix}$$

En el nuevo determinante él es

$$b_{1\alpha_1} b_{2\alpha_2} \dots b_{i\alpha_i} \dots b_{j\alpha_j} \dots b_{n\alpha_n}$$

si signo esta determinado por la paridad de

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_i & \cdots & \alpha_j & \cdots & \alpha_n \end{pmatrix}$$

Puesto que  $1, 2, \dots, j, \dots, i, \dots, n$ , mediante una trasposición, ambas permutaciones tienen paridad contraria y por consiguiente ambas sustituciones tienen paridad contraria.

Se concluye que  $a_{1\alpha 1}a_{2\alpha 2}\dots a_{n\alpha n}$  aparece en el nuevo determinante con signo opuesto al que tenía en el determinante original.

**Propiedad 4:** Un determinante con dos filas iguales es igual a cero.

Supongamos que  $\det A = d$  y que las fila  $i, j$  son iguales. Entonces al intercambiar las filas  $i, j$  obtenemos el mismo determinante, pero por la propiedad 3, obtenemos el determinante con signo opuesto luego  $d = -d \quad d = 0$ .

**Propiedad 5:** Si se multiplican todos los elementos de una fila del determinante por un número  $k$ , el determinante queda multiplicado por  $k$ .

Supongamos que multiplicamos todos los elementos de la fila  $i$  por  $k$ . Por la definición de determinante cada término queda multiplicado por  $k$ .

**Propiedad 6:** Un determinante con dos filas proporcionales es igual a cero.

Supongamos que  $a_{ir} = ka_{jr} \quad r = 1, 2, \dots, n$ . Por la propiedad 5 es posible extraer factor común de la fila  $j$ , queda así un determinante con dos filas iguales.

**Propiedad 7:** Si todos los elementos de la  $i$ -ésima fila de un determinante de orden  $n$  esta dado como la suma de dos términos.

$$a_{ij} = b_j + c_j, \quad j = 1, 2, \dots, n$$

Entonces  $\det A$  es igual a la suma de dos determinantes cuyas filas son, salvo la fila  $i$ , las mismas que las del original, y la fila  $i$  del primer sumando es  $b_1b_2\dots b_n$  y la fila  $i$  del segundo sumando es  $c_1c_2\dots c_n$

En efecto,

$$\begin{aligned} a_{1\alpha 1}a_{2\alpha 2}\dots a_{i\alpha i}\dots a_{n\alpha n} &= a_{1\alpha 1}a_{2\alpha 2}\dots (b_{\alpha i} + c_{\alpha i})\dots a_{n\alpha n} \\ &= a_{1\alpha 1}a_{2\alpha 2}\dots b_{\alpha i}\dots a_{n\alpha n} + a_{1\alpha 1}a_{2\alpha 2}\dots c_{\alpha i}\dots a_{n\alpha n} \end{aligned}$$

Pero el primer sumando es un término del determinante original salvo que su fila  $i$  ha sido reemplazada por  $b_1b_2\dots b_n$ , análogamente para el segundo sumando.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 + c_1 & b_2 + c_2 & \cdots & b_n + c_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \cdots & b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \cdots & c_n \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$



**Definición 2.17.** Se dirá que la  $i$ -ésima fila de  $\det a$  es combinación lineal de las demás filas del determinante si hay constantes  $k_1, k_2, \dots, k_{i-1}, k_{i+1}, \dots, k_n$  tales que

$$a_{ij} = \sum_{r=1}^{i-1} k_r a_{rj} + \sum_{r=i+1}^n k_r a_{rj} \quad j = 1, 2, \dots, n$$

**Propiedad 8:** Si una de las filas del determinante es combinación lineal de las demás, el determinante es igual a cero.

Supongamos que la  $i$ -ésima fila es combinación lineal de las demás filas. Se descompone el determinante en una suma de determinantes cuyas filas son todas iguales a las del determinante original salvo la  $i$ -ésima, tal como lo permite la propiedad 7. Cada uno de estos, o bien tiene una fila de ceros, o bien tiene dos filas proporcionales, en ambos casos el sumando en cuestión es igual a cero.

**Propiedad 9:** El determinante no cambia si a los elementos de una fila se agregan los elementos de otra fila multiplicados por un mismo número.

Supongamos que a la  $i$ -ésima fila se le agrega la  $j$ -ésima multiplicada por  $k$ . Se obtiene un determinante cuya  $i$ -ésima fila es  $a_{ir} + ka_{jr}$ ,  $r = 1, 2, \dots, n$ .

A continuación se muestran un interesante determinante por su aplicación en la interpolación polinomial necesario en el esquema criptográfico de Shamir explicado en el Capítulo 3

El determinante de Vandermonde

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{vmatrix}$$

En forma sucesiva restamos a la fila  $k$  la fila  $k - 1$  multiplicada por  $a_1$ ,  $k = n, n - 1, n - 2, \dots, 2$ . Entonces

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 & \dots & a_n - a_1 \\ 0 & a_2(a_2 - a_1) & a_3(a_3 - a_1) & \dots & a_n(a_n - a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_2^{n-2}(a_2 - a_1) & a_3^{n-2}(a_3 - a_1) & \dots & a_n^{n-2}(a_n - a_1) \end{vmatrix}$$

$$\Delta = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1)d$$

donde  $d$  es un determinante de Vandermonde de orden  $n - 1$ .

## ARIMÉTICA DE MATRICES

Esta sección tiene como objetivo fundamentar la aritmética de matrices y en especial identificar cuando una matriz tiene inversa, esto debido a que se emplearán estas matrices en algunas actividades del Capítulo 6 y requeridas en el Criptosistema de Hill, expuesto en el Capítulo 3

### 2.4. Matrices

Una matriz sobre un campo  $\mathbf{K}$  es un arreglo rectangular de escalares. El arreglo se escribirá en la forma

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad (2.4.19)$$

Una matriz con  $m$  renglones y  $n$  columnas se llama matriz  $m \times n$ .

Se presentan las siguientes definiciones

#### Definiciones:

1. Dada  $A \in M_{n \times m}(K)$  se dirá que  $A$  es cuadrada si  $n = m$ . Se denotará por  $M_{n \times n}(K)$
2. Dada  $A = (a_{ij}) \in M_{n \times m}(K)$  se define la matriz opuesta de  $A$  a  $-A = (b_{ij}) \in M_{n \times m}(K)$  donde  $b_{ij} = -a_{ij}$   $1 \leq i \leq n, 1 \leq j \leq m$ .
3. Se define la matriz  $0_{n \times m} = c_{ij} \in (M_{n \times m}(K))$  donde  $c_{ij} = 0, 1 \leq i \leq n, 1 \leq j \leq m$
4. Sea  $A = (a_{ij}) \in M_{n \times m}(K)$   
 $A$  es una matriz fila si  $n = 1$   
 $A$  es una matriz columna si  $m = 1$
5. Sea  $A = (a_{ij}) \in M_n(K)$   
 $A$  es diagonal si  $a_{ij} = 0$  si  $i \neq j$   
 $A$  es triangular superior si  $a_{ij} = 0$  si  $i > j$   
 $A$  es triangular inferior si  $a_{ij} = 0$  si  $i < j$   
 $A$  es simétrica si  $A^T = A$ .  
 $A$  es antisimétrica si  $A^T = -A$  Si una matriz cuadrada es antisimétrica entonces la diagonal principal es el vector nulo.
6. La **matriz identidad**  $I_n$  de  $n \times n$  cuyos elementos de la diagonal principal son iguales a 1 y todos los demás son 0. Esto es

$I_n = (b_{ij})$  donde

$$b = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \quad (2.4.20)$$

### 2.4.1. Operaciones con Matrices

Sea  $K$  un cuerpo y  $n, m, r \in \mathbb{N}^*$

#### 1. *Suma*

Si  $A = (a_{ij}) \in M_{n \times m}(K)$  y  $B = (b_{ij}) \in M_{n \times m}(K)$  se define  $A + B = (c_{ij}) \in M_{n \times m}(K)$  donde  $c_{ij} = a_{ij} + b_{ij}$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq m$

$$A + B = (a_{ij} + b_{ij}) = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1m} + b_{1m} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2m} + b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nm} + b_{nm} \end{pmatrix} \quad (2.4.21)$$

$(M_{n \times m}(K), +)$  es un grupo abeliano.

#### 2. *Multipliación de una matriz por un escalar*

Si  $A = (a_{ij})$  es una matriz de  $n \times m$  y si  $\alpha$  es un escalar, entonces la matriz  $n \times m$ ,  $\alpha A$ , esta dada por:

$$\alpha A = \alpha(a_{ij}) = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1m} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{n1} & \alpha a_{n2} & \cdots & \alpha a_{nm} \end{pmatrix} \quad (2.4.22)$$

#### 3. *Producto*

Si  $A = (a_{ij}) \in M_{n \times m}(K)$  y  $B = (b_{ij}) \in M_{m \times r}(K)$  se define  $AB = (c_{ij}) \in M_{n \times r}(K)$  donde  $c_{ij} = \sum_{k=1}^m a_{ik}b_{kj}$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq r$ .

**Proposición 2.18.** Sean  $K$  un cuerpo y  $n, m, r, s \in \mathbb{N}^*$

1. Si  $A \in M_{n \times m}(K)$ ,  $B \in M_{m \times r}(K)$  y  $C \in M_{r \times s}(K)$  entonces  $(AB)C = A(BC)$ .
2. Si  $A \in M_{n \times m}(K)$ ,  $B, C \in M_{m \times r}(K)$  entonces  $A(B + C) = AB + AC$
3. Si  $A \in M_{n \times m}(K)$ , entonces  $AI_m = A$  y  $I_n A = A$
4. No Conmutativa, si  $A \in M_{n \times m}(K)$ ,  $B \in M_{m \times r}(K)$ ,  $AB$  no siempre coincide con  $BA$

El conjunto  $M_{n \times m}(K)$  con las leyes suma y producto de matrices se dice que tiene una estructura de anillo unitario no conmutativo.

### 2.4.2. Transformaciones elementales

Sea  $A \in M_{n \times m}(K)$ . Las transformaciones elementales de  $A$  son:

1. Intercambiar dos filas (columnas) de  $A$
2. Si  $\alpha \in K, \alpha \neq 0$ , sustituir una fila (columna) por el producto de  $\alpha$  por esta fila (columna).
3. Si  $\alpha \in K$ , sustituir una fila (columna) de  $A$  por la suma de ésta más otra fila (columna) multiplicada por  $\alpha$

### 2.4.3. Matrices Invertibles

Los resultados que se enuncian a continuación reconocer la existencia de matrices inversibles.

**Teorema 2.19.** *Sea  $A$  una matriz cuadrada  $n \times n$ . Entonces*

$$AI_n = I_n A = A$$

*Es decir  $I_n$ , conmuta con toda matriz  $n \times n$  y la deja sin cambio después de la multiplicación por la derecha o por la izquierda.*

**Demostración** Sea  $c_{ij}$  el elemento  $ij$  de  $AI_n$ . Entonces

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$$

Por definición de matriz identidad, esta suma es igual a  $a_{ij}$ . Así  $AI_n = A$ .  $\square$

**La Inversa de una matriz** Sean  $A$  y  $B$  dos matrices  $n \times n$ . Se tiene

$$AB = BA = I \tag{2.4.23}$$

Entonces  $B$  se llama la **inversa** de  $A$  y se denota por  $A^{-1}$ .

$$AA^{-1} = A^{-1}A = I \tag{2.4.24}$$

Puesto que  $\det AB = \det A \det B = 1$ , para que  $B$  pueda existir  $A$  debe ser no singular.

Si  $A$  tiene inversa, entonces se dice que  $A$  es invertible

**Teorema 2.20.** *Si una matriz  $A$  es invertible, entonces su inversa es única.*

**Demostración.** Suponga que  $B$  y  $C$  son dos inversas de  $A$ . Se puede demostrar que  $B = C$ . Por definición se tiene que  $AB = BA = I$  y  $AC = CA = I$ ,  $B(AC) = (AB)C$  por ley asociativa de la multiplicación de matrices. Entonces

$$B = BI = B(AC) = (BA)C = IC = C$$

Entonces  $B = C$ .  $\square$

**Nota:** se puede recordar que la matriz traspuesta de  $A = (a_{ij})$  es la matriz  $A^t = (b_{ij})$  donde  $b_{ij} = a_{ji}$ .

**Definición 2.21.** Sea  $A = (a_{ij})$  matriz de  $n \times n$ . Se llamará matriz adjunta de  $A$  a la matriz de  $n \times n$   $A^* = (b_{ij})$ , donde  $b_{ij} = A_{ji}$ , esto es, el elemento que está en la intersección de la fila  $i$  y la columna  $j$  de  $A^*$  es el adjunto del elemento correspondiente de  $A^t$

$$A^* = (A_{ji}) = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \quad (2.4.25)$$

Ahora sea  $A$  no singular y  $d = \det A$ , entonces

$$AA^* = \left( \sum_{k=1}^n a_{ik}(A^*)_{kj} \right) = \left( \sum_{k=1}^n a_{ik}A_{jk} \right)$$

Si  $i = j$ ,  $\left( \sum_{k=1}^n a_{ik}A_{jk} \right) = d$ , si  $i \neq j$ ,  $\left( \sum_{k=1}^n a_{ik}A_{jk} \right) = 0$ , luego  $AA^* = (d\delta_{ij}) = dI$ . Análogamente,

$$AA^* = \left( \sum_{k=1}^n Aa_{ki}a_{kj} \right) = dI$$

Se tiene que  $\det AA^* = d^n$  luego  $\det A^* = d^{n-1}$ , si  $A$  es no singular,  $A^*$  también es no singular.

Sea  $B = \frac{1}{d}A^*$ , entonces  $AB = BA = I$ . Se dirá  $B$  es una matriz inversa de  $A$ .

Sea  $B'$  otra matriz inversa de  $A$ , entonces  $AB' = B'A = I$  luego  $(B'A)B = B$  y  $B'(AB) = B'$ , entonces  $B' = B$ . Se concluye que una matriz no singular  $A$  tiene una inversa única. Se designará por  $A^{-1}$  y  $A^{-1} = \left( \frac{1}{d}A_{ji} \right)$  donde  $A_{ji}$  es el adjunto de  $a_{ji}$ .

El resultado que se muestra a continuación es el caso para una matriz  $2 \times 2$

**Teorema 2.22.** *Sea  $A =$  una matriz  $2 \times 2$  entonces:*

*i.  $A$  es invertible si y sólo si  $\det(A) \neq 0$ .*

*ii. Si  $\det(A) = 0$ , entonces*

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

### Demostración

Suponer que  $\det(A) \neq 0$  y sea  $B = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$ . Entonces

$$BA = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$BA = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{22}a_{11} - a_{12}a_{21} & 0 \\ 0 & -a_{21}a_{12} + a_{11}a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Ahora si  $A$  es invertible, entonces el  $\det(A) \neq 0$ . Para esto se considera el sistema

$$a_{11}x_1 + a_{12}x_2 = b_1$$

$$a_{21}x_1 + a_{22}x_2 = b_2$$

Se sabe que si el sistema tiene única solución, entonces  $a_{11}a_{22} - a_{12}a_{21} \neq 0$ . El sistema se puede escribir

$$A\mathbf{x} = \mathbf{b}$$

con  $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$  y  $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ . Entonces como  $A$  es invertible, el sistema tiene solución única dada por

$$\mathbf{x} = A^{-1}\mathbf{b}$$

El hecho de que el sistema tenga una solución única implica que  $a_{11}a_{22} - a_{12}a_{21} \neq 0$ .  $\square$

En esta propuesta tiene interés especialmente en las matrices  $2 \times 2$  y si es posible  $3 \times 3$ .

## CAPÍTULO 3

---

# CRIPTOGRAFÍA Y ESTEGANOGRAFÍA

---

*El deseo de descubrir secretos está profundamente arraigado en la naturaleza humana. Incluso la mente menos curiosa se excita ante la promesa de acceder a los conocimientos ocultos para otras personas. Algunos tienen la suerte de encontrar un trabajo que consiste en solucionar misterios, pero la mayoría de nosotros tenemos que contentarnos con sublimar ese deseo resolviendo misterios artificiales creados por nuestro entretenimiento. Las historias de detectives o los crucigramas satisfacen las necesidades de la mayoría; el desciframiento de códigos secretos puede ser la tarea de muy pocos.*

*John Chadwick, El desciframiento Lineal B*

En este capítulo se realiza un estudio de los conceptos que apoyan la propuesta didáctica como fuente de formación sobre los objetos matemáticos requeridos en los sistemas criptográficos y esteganográficos, que serán usados como recurso para enriquecer las actividades del Capítulo 6 dentro del aula de clase en la enseñanza de patrones, matrices, sistemas de ecuaciones lineales

Es importante retomar que **Criptografía** significa escritura secreta y su estudio tiene como objetivo primordial, mantener segura la información que dos individuos,  $\alpha$  y  $\beta$  comparten a través de un canal inseguro; en él participan un emisor al que se denominará Alice, un receptor llamado Bob y Eve el Enemigo.

Para ello se define un *sistema Criptográfico o Criptosistema*  $\mathcal{S}$  como una sextupla del tipo:

$$\mathcal{S} = (\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

en donde,  $\mathcal{A}$  es un alfabeto de definición (por ejemplo,  $\mathcal{A} = \{0, 1\}$  si las palabras del código se quieren escribir en lenguaje binario),

$\mathcal{P}$  es un conjunto eventualmente finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

$\mathcal{C}$  es un conjunto eventualmente finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente  $\mathcal{A}$ ),

$\mathcal{K}$  es el conjunto o espacio eventualmente finito de claves o llaves.

Para  $K \in \mathcal{K}$ , existe una regla de ciframiento  $e_K : \mathcal{P} \rightarrow \mathcal{C}$  y una correspondiente regla de desciframiento

$d_K : \mathcal{C} \rightarrow \mathcal{P}$ , tales que  $d_K(e_K(x)) = x$ , para todo texto en claro  $x$ .

$\mathcal{E}$ : es una familia de funciones, cada clave  $e \in \mathcal{K}$  determina de forma única una biyección, que se llama función de cifrado.

$\mathcal{D}$  es la función de descifrado.

En el sistema criptográfico Alice, Bob y Eva se definen como:

### ***ALICE***

$$\mathcal{E}_K : \mathcal{P} \rightarrow \mathcal{C}$$

$$\mathcal{E}_K(x) = c$$

### ***BOB***

$$\mathcal{D}_K : \mathcal{C} \rightarrow \mathcal{P}$$

$$\mathcal{D}_K(c) = x$$

### ***EVE***

Teniendo presente el principio de **Kerckhoffs**, el cual señala que “*El atacante tiene pleno conocimiento del método de cifrado a excepción de la clave*”; por ello Eve conoce la manera como se esta cifrado la información y tiene recursos ilimitados para descubrirla.

De hecho, en este trabajo se consideran sistemas criptográficos en los que  $\mathcal{P}$ ,  $\mathcal{C}$  y  $\mathcal{K}$  son conjuntos infinitos, lo cual será aprovechado en el capítulo 4 para investigar el uso de este tipo de sistemas en la enseñanza de distintos tipos de patrones numéricos.



## 3.1. Métodos Criptográficos

En esta sección se estudiarán los métodos y aplicaciones que fueron centro de enseñanza con los estudiantes de grado noveno, para mejorar y motivar el aprendizaje algebraico.

### 3.1.1. Cifrado por Desplazamiento

Este cifrado es una generalización del cifrado de Julio César; y en este caso se define:

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m, m \text{ fijo.}$$

Para  $\mathcal{K} = \mathbb{Z}_n$  se tiene que

$$e_{\mathcal{K}}(x) = x + \mathcal{K} \text{ mód } m,$$

$$d_{\mathcal{K}}(x) = x - \mathcal{K} \text{ mód } m.$$

Consideremos el siguiente ejemplo con un abecedario de 27 letras, al cual se le asigna un valor numérico como se muestra a continuación

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

TABLA 3.1. Alfabeto Español

Si se tiene el texto: **ES FÁCIL DE DESCIFRARLO**, y tomamos  $\mathcal{K} = 9$  y  $n = 27$ ; entonces el texto en claro

ESFACILDESCIFRARLO

Se cifra convirtiendo el texto en una sucesión de enteros

4 19 5 0 2 8 11 3 4 19 2 8 5 18 0 18 11 15.

A continuación a cada valor se adiciona 9 mód 27 para obtener

13 1 14 9 11 17 20 12 13 1 11 17 14 0 9 0 20 24

Se obtiene el texto cifrado NBÑJLQTMNBLQÑAJATX.

Cabe anotar que la técnica más simple para que un oponente o atacante pueda realizar un ataque exitoso a un sistema criptográfico previamente definido es mediante

la búsqueda exhaustiva de la llave o clave. Lo cual se puede lograr si es el espacio es muy pequeño, tal es el caso del sistema criptográfico por desplazamiento. Por ejemplo, si un atacante obtiene o captura el texto cifrado NBÑJLQTMNBLQÑAJATX obtenido por desplazamiento entonces la llave se obtiene al hacer una búsqueda de la clave de la siguiente forma:

NBÑJLQTMNBLQÑAJATX

nbñjlqtmnblqñajatx

Si  $K = 1$  se obtendría el texto;  $x = \text{manikpslmakpnzizsw}$ , el cual no tiene sentido en el idioma español, por lo que  $K = 1$  no es la clave buscada y por lo tanto se debe continuar realizando la correspondiente búsqueda haciendo  $K = 2$  en cuyo caso se obtendrá el texto:

$x = \text{lzmhjorkljzjomyhyrv}$

éste tampoco tiene sentido en español. Con lo que se debe continuar al proceso hasta encontrar un texto con sentido en el lenguaje del sistema criptográfico. De esta forma se obtienen los siguientes resultados:

Para  $K=3$ ;  $x = \text{kylgiñqikyĩnlxgxqu}$

Para  $K=4$ ;  $x = \text{jxkfhnpijxhnkwfwpt}$

Para  $K=5 = \text{iwjegmohiwgmjvevos}$

Para  $K=6 = \text{hvidflñghvfiuduñr}$

Para  $K=7 = \text{guhceknfguekhtctnq}$

Para  $K=8 = \text{ftgbdjmeftdjgsbsmp}$

Para  $K=9 = \text{esfacildescifrarlo}$

Para  $K=10 = \text{drgzbhkcdrbheqzqlñ}$

Encontrando  $k = 9$

### 3.1.2. Criptosistema Afín

Este sistema se puede describir como:

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{27}$$

$$\mathcal{K} = (a, b) \quad \mathbb{Z}_{27} \times \mathbb{Z}_{27} \quad (a, 27) = 1 \quad .$$

Para  $K = (a, b) \in \mathcal{K}$ , se define

$$e_k(x) = ax + b \pmod{27},$$

$$d_k(y) = a^{-1}(y - b) \pmod{27}, \quad x, y \in \mathbb{Z}_{27}.$$

Se puede observar que si  $(a, b) \in \mathcal{K}$  entonces

$$d_{(a,b)}(e_{(a,b)}(x)) \equiv d_{(a,b)}(ax + b) \pmod{27} \equiv a^{-1}(ax + b - b) \pmod{27} \equiv a^{-1}ax \pmod{27} \equiv x \pmod{27}.$$

A continuación se mostrará un ejemplo; si se quiere cifrar el texto en claro

### ***LASMATEMATICASSONSENCILLAS.***

Como en el caso del cifrado de desplazamiento se inicia escribiendo el mensaje con su equivalente numérico, en el alfabeto español de 27 letras.

L	A	S	M	A	T	E	M	A	T	I	C	A	S
11	0	19	12	0	20	4	12	0	20	8	2	0	19

S	O	N	S	E	N	C	I	L	L	A	S
19	15	13	19	4	13	2	8	11	11	0	19

TABLA 3.2. Texto Criptosistema Afín

Con el que se obtiene el texto como una sucesión de enteros

11 0 19 12 0 20 4 12 0 20 8 2 0 19 19 15 13 19 4 13 2 8 11 11 0 19.

Se aplicará una clave afín de la forma  $(7, 2)$ , es decir, una transformación  $7x + 2$ , para ello a cada número de la sucesión se multiplica por 7 módulo 27 y se adiciona 2 obteniendo la sucesión

25 2 0 5 2 7 3 5 2 7 4 16 2 0 0 26 12 0 3 12 16 4 25 25 2 0 .

Por lo que YCAFCHDFCHEPCAAMADMPEYYCA es el correspondiente texto cifrado.

### ***Ataque al cifrado afín***

Como en el caso del cifrado por desplazamiento, se puede realizar una búsqueda exhaustiva de la clave debido a que  $m$  es pequeño, pero si  $m$  es grande el método resulta complicado. Por lo que en este caso es mejor atacar un texto cifrado afín realizando un análisis estadístico de frecuencia, es decir, se estudia la regularidad con la que aparecen los distintos símbolos en un lenguaje determinado y luego la frecuencia con la que aparecen en los mensajes cifrados.

### 3.1.3. El Criptosistema de Vigenère

Para  $m$  fijo, en este Criptosistema  $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{27}^m$ , esto es, cada texto en claro, texto cifrado o clave es una  $m$ -tupla del tipo  $x = (x_1, x_2, \dots, x_m)$ ,  $y = (y_1, y_2, \dots, y_m)$ ,  $(k_1, k_2, \dots, k_m)$ .

Si  $K = (k_1, k_2, \dots, k_m) \in \mathcal{K}$ , entonces

$$\begin{aligned} e_K(x) &= (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m), \\ d_K(y) &= (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m). \end{aligned} \quad (3.1.1)$$

Si se elige la palabra clave **carmen**, para cifrar el mensaje

todosobtendrancincoenmatematicas

Convertiendo el texto en claro y la clave en dos sucesiones de números, con lo que se tiene

*texto*: 20 15 3 15 19 15 1 20 4 13 3 18 0 13 2 8 13 2 15 4 13 12 0 20 4 12 0 20 8 2 0 19

*clave*: 2 0 18 12 4 13

20	15	3	15	19	15	1	20	4	13	3	18	0	13	2	8
2	0	18	12	4	13	2	0	18	12	4	13	2	0	18	12
22	15	21	0	23	1	3	20	22	25	7	4	2	13	20	20

13	2	15	4	13	12	0	20	4	12	0	20	8	2	0	19
4	13	2	0	18	12	4	13	2	0	18	12	4	13	2	0
17	15	17	4	4	24	4	6	6	12	18	5	12	15	2	19

TABLA 3.3. Texto Criptosistema de Vigenère

Se obtiene

VOUAWBDTVYHECNTTQOQEEXEGGMOCS como el texto cifrado

### 3.1.4. Cifrado por Transposición Geométrica

Este método consiste en la transformación del orden de las unidades del texto original según una clave, si se hace referencia cualquier cifrado de transposición se debe tener en cuenta que el alfabeto se conservan, y que solamente hubo una traslación o un

cambio en el orden de los mismo; estas modificaciones en la ubicación responden generalmente a un orden repetitivo.

Existen métodos de cifrado por transposición como:

Transposición inversa, simple doble, por bloques, columnas, máscara rotativa entre otras. Específicamente cuando se refiere a transposición geométrica se tiene en cuenta que el texto se organice en un cuadrado, triángulo, rectángulo o alguna figura geométrica en especial.

Así como el siguiente ejemplo se tiene una transposición simple por columna con el texto claro *Me gusta la criptografía*

M	E	G	U
S	T	A	L
A	C	R	I
P	T	O	G
R	A	F	I
A			

TABLA 3.4. Tranposición Geométrica por Columna

El texto cifrado sería **MSAPRA ETCTA GAROF ULIGT**. El receptor, usando el proceso inverso, vuelve a obtener el texto claro.

Si se considera otra figura como puede ser el triángulo, se tendría:

				M				
			E	G	U			
		S	T	A	L	A		
	C	R	I	P	T	O	G	
R	A	F	I	A	X	X	X	X

TABLA 3.5. Transposición Geométrica Triangular

Si en la base del triángulo quedan espacios se podrá poner una letra acordada con el receptor o la letra X.

El texto cifrado será: **A CF SRI ETII MGAPA ULTX AOX GX X**

Para este trabajo se observará las claves de transposición que se pueden construir en el triángulo de Pascal y los números poligonales.

### 3.1.5. Criptosistema de Hill

Este sistema critográfico fue creado por Lester Hill 1929, este método esta basado en la substitución poligráfica que cifra bloques de texto de longitud determinada

utilizando como clave una matriz. Esta matriz debe ser cuadrada e invertible. Tiene las siguientes características:

Sea  $m$  un entero positivo fijo,

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{27}^m$$

$$\mathcal{K} = \{ A \in M_m(\mathbb{Z}_{27}) \mid \det(A) \neq 0 \}$$

Para una matriz  $K \in \mathcal{K}$  fija, se definen las siguientes reglas de ciframiento y desciframiento

$$e_k(x) = xK,$$

$$d_k(y) = yK^{-1}$$

$A \in M_m(\mathbb{Z}_{27})$ , denota el hecho de que una matriz cuadrada  $A$  con  $m$  filas y columnas, tiene elementos  $\mathbb{Z}_{27}$

$K^{-1}$ , puede ser obtenida de  $K$  usando el algoritmo de Gauss-Jordan, por ejemplo.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \quad (3.1.2)$$

Se presenta a continuación el siguiente ejemplo para este criptosistema:

Si se tiene el texto claro: *La clave es azul*, se prosigue con su equivalencia numérica descrita anteriormente para el alfabeto español, obteniendo:

L	A	C	L	A	V	E	E	S	A	Z	U	L
11	0	2	11	0	22	4	4	19	0	26	21	11

TABLA 3.6. Texto Criptosistema Hill

El ciframiento de

$$LAClaveESAZUL = 11 \ 0 \ 2 \ 11 \ 0 \ 22 \ 4 \ 4 \ 19 \ 0 \ 26 \ 21 \ 11$$

Con clave

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \text{ se obtiene realizando los productos}$$

$$[11 \ 0] \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = [11 + 0 \quad 22 + 4] = [11 \quad 12]$$

$$\begin{bmatrix} 2 & 11 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 2 + 33 & 4 + 44 \end{bmatrix} = \begin{bmatrix} 8 & 21 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 22 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 0 + 66 & 0 + 88 \end{bmatrix} = \begin{bmatrix} 12 & 7 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 + 12 & 8 + 16 \end{bmatrix} = \begin{bmatrix} 16 & 24 \end{bmatrix}$$

$$\begin{bmatrix} 19 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 19 + 0 & 38 + 0 \end{bmatrix} = \begin{bmatrix} 19 & 11 \end{bmatrix}$$

$$\begin{bmatrix} 26 & 21 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 26 + 63 & 52 + 84 \end{bmatrix} = \begin{bmatrix} 8 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 11 + 3 & 22 + 4 \end{bmatrix} = \begin{bmatrix} 14 & 26 \end{bmatrix}$$

El texto cifrado obtenido será: LMIUMHPXSLIBÑZ

Se observa que esta matriz es válida como clave, dado que  $\det(A) = (1)(4) - (2)(3) = -2 = 25 \pmod{27}$  y  $(25, 27) = 1$

El proceso de desciframiento, requiere calcular  $A^{-1}$  teniendo en cuenta que todas las operaciones involucradas se hacen módulo 27, por lo que, en este caso

$$A^{-1} = (-2)^{-1} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = (-25)^{-1} \begin{bmatrix} 4 & 25 \\ 24 & 1 \end{bmatrix} = (13) \begin{bmatrix} 4 & 25 \\ 24 & 1 \end{bmatrix} = \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix}$$

$$A^{-1} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$$

$$\text{Se nota que } A^{-1}A = \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 28 & 54 \\ 54 & 82 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Luego si para el caso se quiere descifrar el texto ÑZ se deberá hacer el calculo

$$\begin{bmatrix} 14 & 26 \end{bmatrix} \begin{bmatrix} 25 & 1 \\ 15 & 13 \end{bmatrix} = \begin{bmatrix} -1 + 12 & 28 \end{bmatrix} = \begin{bmatrix} 11 & 1 \end{bmatrix} = LB$$

El cifrado de Hill es vulnerable a un ataque de texto claro conocido. Esto es, la clave puede obtenerse si se obtiene un número adecuado de parejas  $(x_i, y_i)$  en donde  $x_i$  es un texto claro y  $y_i$  su correspondiente texto cifrado, lo cual se puede ilustrar en este ejemplo, si suponemos que un ataque se obtiene las parejas:

$$((19, 0); (19, 11)) \text{ y } ((4, 4); (16, 24))$$

El atacante puede obtener la clave al plantear los siguientes sistemas de ecuaciones lineales módulo 27

$$\begin{bmatrix} 19 & 0 \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} = \begin{bmatrix} 19 & 11 \end{bmatrix}$$

$$19k_{11} = 19$$

$$19k_{12} = 11$$

$$\begin{bmatrix} 4 & 4 \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} = \begin{bmatrix} 16 & 24 \end{bmatrix}$$

$$4k_{11} + 4k_{21} = 16$$

$$4k_{12} + 4k_{22} = 24$$

de donde se concluye:  $k_{11} = 1$ ;  $k_{12} = 11 \cdot 19^{-1}$ ;  $k_{21} = 12 \cdot 4^{-1}$ ;  $k_{22} = (24 \cdot -8)4^{-1}$

Luego  $k_{11} = 1$ ,  $k_{12} = 2$ ,  $k_{21} = 84 = 3 \text{ mód } 27$ ,  $k_{22} = (16) \cdot 7 \text{ mód } 27 = 112 \text{ mód } 27 = 4 \text{ mód } 27$

Este ejemplo muestra como el criptoanálisis del sistema criptográfico de Hill, permite el estudio de la solución de sistemas de ecuaciones y los criterios de inversibilidad en matrices.

Lo anterior prueba que estos procesos pueden llevarse al aula de clase motivados por las técnicas criptográficas necesarias para analizar este tipo de sistemas.

Para realizar el criptoanálisis de este método debemos conocer el número  $m$  que es el tamaño de la clave y que se ha obtenido  $m$  parejas  $(x_k, y_k)$ ,  $1 < k < m$ . Con los que podemos encontrar un sistemas de  $m$  ecuaciones.

### 3.1.6. Esquema de Shamir

El esquema de compartición de secretos de Shamir es según Vásquez[17] un tipo de esquema umbral, el cual esta basado en la interpolación de polinomios.

Se considera el polinomio de grado  $t - 1$  sobre el campo finito  $K$

$$p[x] = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \quad (3.1.3)$$

este polinomio se construye de tal manera que el coeficiente  $a_0$  es el secreto y los demás coeficientes son elementos aleatorios en el campo  $k$ .

Cada uno de los  $n$  fragmentos serán los puntos  $(x_i, p[x_i])_{1 \leq i \leq n}$ , donde:

$$x_i = x_j \text{ para todo } i = j \text{ y } p[0] = a_0$$



Dados  $t$  fragmentos, se puede determinar de manera única al polinomio, y en consecuencia, se puede calcular  $a_0$  (el secreto) mediante sustitución  $x = 0$  en la función polinomial.

En el caso especial en que  $t = 2$ , sólo se requiere dos fragmentos para recobrar el secreto. En consecuencia, la ecuación del polinomio describe una línea recta. El secreto es el punto en el que la línea intersecta al eje  $y$ .

El esquema de Shamir está basado en la interpolación de polinomios por el hecho que el polinomio invariante  $p[x]$  de grado  $t - 1$  está determinado de manera única por  $t$  puntos  $(x_i, s_i)$  con distintos  $x_i$  pues estos puntos definen  $t$  ecuaciones independientes con  $t$  incógnitas en los coeficientes  $a_i$ .

Los siguientes algoritmos describen las fases del mecanismo de construcción del esquema umbral de Shamir

✓ **Algoritmo 1** Fase inicial de distribuidor  $p_0$

*Necesita:*  $s \geq 0$ , el secreto y  $t$  es el umbral

*Asegura:*  $a_i$  los coeficientes del polinomio.

1.  $p_0$  elige un primo  $p > \max(s, n)$  y define  $a_0 = s$ ;
2.  $p_0$  selecciona aleatoriamente  $(t - 1)$  coeficientes  $a_1, \dots, a_{t-1}$ , con  $0 \leq a_i \leq p - 1$  que define el polinomio aleatoriamente sobre  $\mathbb{F}_p$ .

✓ **Algoritmo 2** Distribución de los fragmentos

*Necesita:* El polinomio  $p[x]$  e índices  $x_i$  para los participantes.

*Asegura:*  $(x_i, s_i = p[x_i])$  los fragmentos para cada participante.

1.  $p_0$  calcula  $s_i = P[x_i] \equiv \text{mód}(\mathbb{Z}_p)$  para cada participante  $x_i$ , y hace la transferencia segura del fragmento con índice público  $x_i$ .

✓ **Algoritmo 3** Reunión de fragmentos

*Necesita:* Un grupo de  $t$  o más fragmentos  $(x_i, s_i)_{1 \leq i \leq t}$ .

*Asegura:* El secreto  $s$

1. Se calcula los coeficientes  $a_j, 1 \leq j \leq t - 1$  del polinomio  $p[x]$  mediante la interpolación de Lagrange. Se recupera el secreto sustituyendo  $x = 0$  en  $p[x]$ , es decir  $p[0] = a_0 = s$ .

Para demostrar que el esquema de Shamir es perfecto, se necesita que el sistema de  $t$  ecuaciones lineales independientes siempre tenga única solución.

En general se tiene dados  $t$  fragmentos

$$s_i k = p[x_i k], \quad 1 \leq k \leq t$$

donde

$$p[x] = a_0 + a_1x + \dots + a_{t-1}x^{t-1}, \text{ con } a_0 = s$$

el sistema de ecuaciones lineales en  $\mathbb{F}_p$  es el siguiente:

$$\begin{aligned} a_0 + a_1x_{i1} + a_2x_{i1}^2 + \dots + a_{t-1}x_{i1}^{t-1} &= s_{i1} \\ a_0 + a_1x_{i2} + a_2x_{i2}^2 + \dots + a_{t-1}x_{i2}^{t-1} &= s_{i2} \\ &\vdots \\ a_0 + a_1x_{it} + a_2x_{it}^2 + \dots + a_{t-1}x_{it}^{t-1} &= s_{it} \end{aligned}$$

Este sistema visto en un sistema matricial es:

$$\begin{pmatrix} 1 & x_{i1} & x_{i1}^2 & \dots & x_{i1}^{t-1} \\ 1 & x_{i2} & x_{i2}^2 & \dots & x_{i2}^{t-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & x_{it} & x_{it}^2 & \dots & x_{it}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} s_{i1} \\ s_{i2} \\ \vdots \\ s_{it} \end{pmatrix}$$

La matriz de la izquierda (denotada por A) se conoce como la matriz *Vandermonde*. Para tal matriz existe una fórmula conocida para su determinante:

$$\det(A) = \prod_{1 \leq j < k \leq t} (x_{ik} - x_{ij}) \mod p \quad (3.1.4)$$

Como los  $x_{ik}$  son distintos entre sí, los términos  $(x_{ik} - x_{ij})$  son distintos de cero. Por lo tanto  $\det(A) \neq 0$ . Esto indica que el sistema posee única solución en el campo  $\mathbb{F}_p$ .

Esto demuestra que cualquier grupo de  $t$  participantes puede recuperar el secreto. Por otro lado, cuando  $t - 1$  participantes reúnen fragmentos, obtiene un sistema de  $t - 1$  ecuaciones. Es claro que existe una solución no única en el campo  $\mathbb{F}_p$ . Por lo tanto el esquema de Shamir es perfecto.

El siguiente ejemplo y la teoría expuesta del Esquema Shamir fueron tomados de Vazquez [17]:

Sean  $p = 23$ ,  $t = 3$ ,  $n = 6$  y las coordenadas públicas  $x_i = i$  para cada participante  $p_i$ , para  $i = 1, \dots, 6$ .

Supongamos que los participantes de  $B = \{p_1, p_3, p_5\}$  se reúnen sus fragmentos, los cuales son respectivamente 6, 16 y 11. Se escribe el polinomio como:

$$p[x] = a_0 + a_1x + a_2x^2$$

Calculando  $p[1], p[3], p[5]$  se obtiene las siguientes tres ecuaciones lineales en  $\mathbb{F}_3$

$$\begin{aligned}a_0 + a_1 + a_2 &= 06 \\a_0 + 3a_1 + 9a_2 &= 16 \\a_0 + 5a_1 + 25a_2 &= 11\end{aligned}$$

Este sistema posee solución única  $a_0 = 4$ ,  $a_1 = 1$  y  $a_2 = 1$  (el secreto compartido es  $a_0 = 4$ ).

Hasta ahora se ha analizado el esquema Shamir desde el punto de vista de resolución de un sistema de ecuaciones lineales sobre el campo  $\mathbb{F}_p$ . Existe un método para la resolución de este sistema basado en polinomios de Lagrange. El método de interpolación de Lagrange da una fórmula explícita para el polinomio de grado a lo más  $t - 1$ , los coeficientes de tal polinomio  $p[x]$  de grado menor que  $t$ , definido por los puntos  $(x_i, s_i)$ ,  $1 \leq i \leq t$  será:

$$p[x] = \sum_{i=1}^t s_i \prod_{1 \leq j \leq t, j \neq i} \frac{x - x_j}{x_i - x_j} \quad (3.1.5)$$

Dado que el secreto es  $p[0]$ , si se evalúa  $x = 0$  en la ecuación anterior, se obtiene

$$p[0] = \sum_{i=1}^t c_i s_i$$

donde

$$c_i = \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}$$

Los coeficientes  $c_i$  son constantes para un grupo fijo de  $t$  participantes.

Considerando el ejemplo anterior; para los participantes  $p_1, p_3, p_5$ , se tiene los fragmentos 6, 16 y 11 respectivamente. Entonces los índices asociados a estos participantes son  $x_1 = 1$  (para el participante  $p_1$ ),  $x_2 = 3$  (para el participante  $p_3$ ),  $x_3 = 5$  (para el participante  $p_5$ ). De acuerdo a la ecuación formulada por Lagrange se tiene:

$$\begin{aligned}
c_1 &= \prod_{1 \leq j \leq 3, j \neq 1} \frac{x_j}{x_j - x_1} \text{ mód } 23 \\
&= \frac{x_2 \cdot x_3}{(x_2 - x_1)(x_3 - x_1)} \text{ mód } 23 \\
&= \frac{3 \cdot 5}{(2)(4)} \text{ mód } 23 \\
&= \frac{15}{8} \text{ mód } 23 \\
&= (15)(3) \text{ mód } 23 \\
&= 45 \text{ mód } 23 \\
&= 22
\end{aligned}$$

$$\begin{aligned}
c_2 &= \frac{x_1 \cdot x_3}{(x_1 - x_2)(x_3 - x_2)} \text{ mód } 23 \\
&= \frac{5}{-4} \text{ mód } 23 \\
&= (5)(7) \text{ mód } 23 \\
&= 16
\end{aligned}$$

$$\begin{aligned}
c_3 &= \frac{x_1 \cdot x_2}{(x_1 - x_3)(x_2 - x_3)} \text{ mód } 23 \\
&= \frac{3}{8} \text{ mód } 23 \\
&= (3)(3) \text{ mód } 23 \\
&= 9
\end{aligned}$$

Con estos coeficientes, y de acuerdo a la ecuación  $p[0] = \sum_{i=1}^t c_i s_i$ , el secreto es:

$$\begin{aligned}
s = p[0] &= \sum_{i=1}^3 c_i s_i \text{ mód } 23 \\
&= c_1 \cdot s_1 + c_2 \cdot s_2 + c_3 \cdot s_3 \text{ mód } 23 \\
&= 22 \cdot 6 + 16 \cdot 16 + 9 \cdot 11 \text{ mód } 23 \\
&= 487 \text{ mód } 23 \\
&= 4
\end{aligned}$$

### *Propiedades del Esquema de Shamir*

1. *Es perfecto*: Si se conoce  $t-1$  o menos fragmentos, la probabilidad de encontrar el valor secreto compartido en el campo  $\mathbb{F}_p$ , es siempre la misma.
2. *Es ideal*: Como los fragmentos y el secreto pertenecen al campo  $\mathbb{F}_p$  entonces poseen la misma longitud de bits.
3. *Es escalable*: Es posible expandir para nuevos usuarios, esto significa que se puede calcular y distinguir nuevos fragmentos. Por otro lado se puede observar que si un usuario borra su fragmento, el sistema sigue funcionando normalmente, pero hace inaccesible el acceso para este participante.
4. *Es controlable por niveles*: Si se provee al usuario con múltiples fragmentos, le proporciona más control para la recuperación del secreto, pues requiere un número menor (que el umbral  $k$ ) de participantes para su reconstrucción.
5. *Es seguro*: La seguridad del esquema Shamir se basa principalmente en la elección del umbral.

## 3.2. Esteganografía

En esta sección se podrá visualizar algunas técnicas esteganográficas que apoyarán el trabajo.

Del griego steganos (oculto) y graphos (escritura); la **Esteganografía**, se encarga de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación. Consiste simplemente en camuflar el texto intercalándolo dentro de otro mensaje. Podemos elaborar un mensaje de contenido irrelevante pero de forma que siguiendo cierta pauta de eliminación podamos reconstruir el texto original.

Históricamente se ha empleado esta técnica como lo fue la Sciatala Espartana; Heródoto afeitaba la cabeza a sus mensajeros para escribir el texto, para luego esperar a que creciera el cabello y enviarlo con el mensaje; la regilla móvil de Cardano; entre otros.

Por ejemplo si se introduce el siguiente texto en una tabla de 10 columnas, para decodificarla se superpone una matriz perforada visualizando.

En este trabajo se empleará algunas técnicas esteganográficas clásicas, para encontrar patrones numéricos que introduzcan los Números de Catalan, Delannoy y Poligonales.

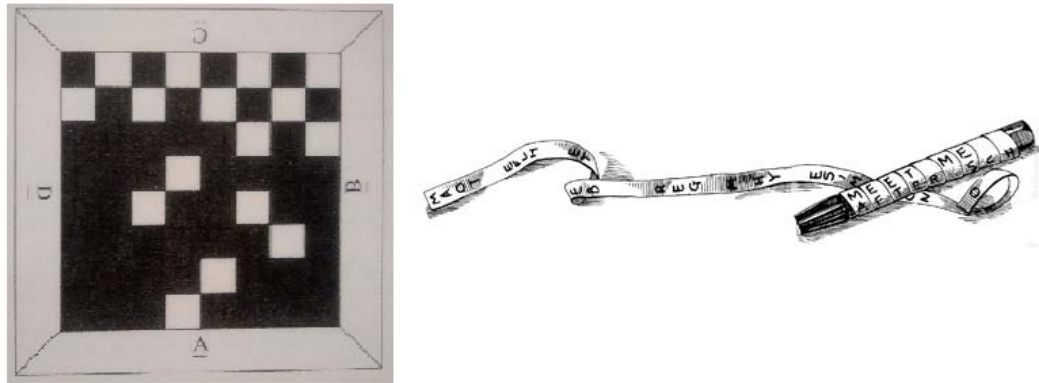


FIGURA 3.1. Rejilla de Cardano y Scitala Espartana

L	A		C	R	I	P	T	O	G										
R	A	F	I	A		C	O	M	O										
R	E	C	U	R	S	O		D	I										
D	A	C	T	I	C	O		E	N										
L	A		E	N	S	E	N	A	N										
Z	A		D	E		L	A	S											
M	A	T	E	M	A	T	I	C	A										
S																			

L	A		C	R	I	P	T	O	G
R	A	F	I	A		C	O	M	O
R	E	C	U	R	S	O		D	I
D	A	C	T	I	C	O		E	N
L	A		E	N	S	E	N	A	N
Z	A		D	E		L	A	S	
M	A	T	E	M	A	T	I	C	A
S									

FIGURA 3.2. Técnica Esteganográfica

## CAPÍTULO 4

---

---

# CONSECUCIÓN DE PATRONES CON EL USO DE LA ESTEGANOGRAFÍA Y CRIPTOGRAFÍA

---

---

*“... realmente dudo que la inteligencia humana pueda concebir un  
enigma que la inteligencia de otro humano no sea capaz de resolver”*

*Edgar Allan Poe*

Para este capítulo, se combinan técnicas criptográficas y esteganográficas clásicas para encontrar distintos tipos de patrones numéricos. Los procesos descritos permitirán estudiar algunos problemas combinatorios que conciernen a los números de Catalan, de Delannoy y algunos números poligonales.

### 4.1. Números de Catalan

En esta sección del trabajo, se usa el sistema criptográfico afín combinado con algunas técnicas esteganográficas clásicas para encontrar los números de Catalan y describir algunas de sus propiedades.

Se considera un sistema criptográfico en bloque (denotado  $\mathcal{C}$ ) definido de la siguiente forma:

$$\begin{aligned} P &= C = \mathbb{N}^n \\ K &= (\mathbb{Q}^* \times \mathbb{N})^n \\ e_k(x_1, x_2, \dots, x_n) &= (k_1x_1 + b_1, k_2x_2 + b_2, \dots, k_nx_n + b_n) \\ d_k(y_1, y_2, \dots, y_n) &= \left(\frac{1}{k_1}y_1 - b_1, \frac{1}{k_2}y_2 - b_2, \dots, \frac{1}{k_n}y_n - b_n\right). \end{aligned} \tag{4.1.1}$$

En donde para  $n \geq 1$ ,  $P$ ,  $C$  y  $K$  denotan el conjunto de unidades de texto en claro, cifrado y claves respectivamente.  $\mathbb{N}$  denota el conjunto de enteros no negativos y  $\mathbb{Q}^*$  es el conjunto de los números racionales distintos de cero. Para  $i \geq 1$  fijo, una clave en este sistema, es una pareja del tipo  $(k_i, b_i)$ ,  $k_i \in \mathbb{Q}$  y  $b_i \in \mathbb{N}$ , para todo  $i$ ,  $1 \leq i \leq n$ .

En adelante, se supondrá que los mensajes se ocultan dentro de mensajes numéricos (recipientes) escritos en tablas o matrices. Los mensajes ocultos se pueden recuperar al superponer a estos arreglos una matriz del mismo tamaño denominada la clave esteganográfica o simplemente la clave con elementos en el conjunto  $\{0, 1\}$ . En este caso un elemento 0 en la clave hace que en la superposición, el elemento correspondiente en el mensaje recipiente deba ser ocultado, mientras que un 1 en la clave es un elemento transparente en la transposición y deja ver el correspondiente elemento del recipiente.

Se ilustra el uso del sistema descrito asumiendo que los números de Catalan han sido cifrados usando el sistema  $\mathcal{C}$  y que tal ciframiento se ha ocultado en un diagrama o matriz  $D = \{(x, y) \mid x, y \in \mathbb{N}\} = \mathbb{N}^2$ . En adelante denotaremos  $D_n \subseteq D$  al subconjunto de  $D$ , tal que  $0 \leq x \leq n$  y  $0 \leq y \leq n$ . El siguiente diagrama ilustra el caso para  $n = 6$ .

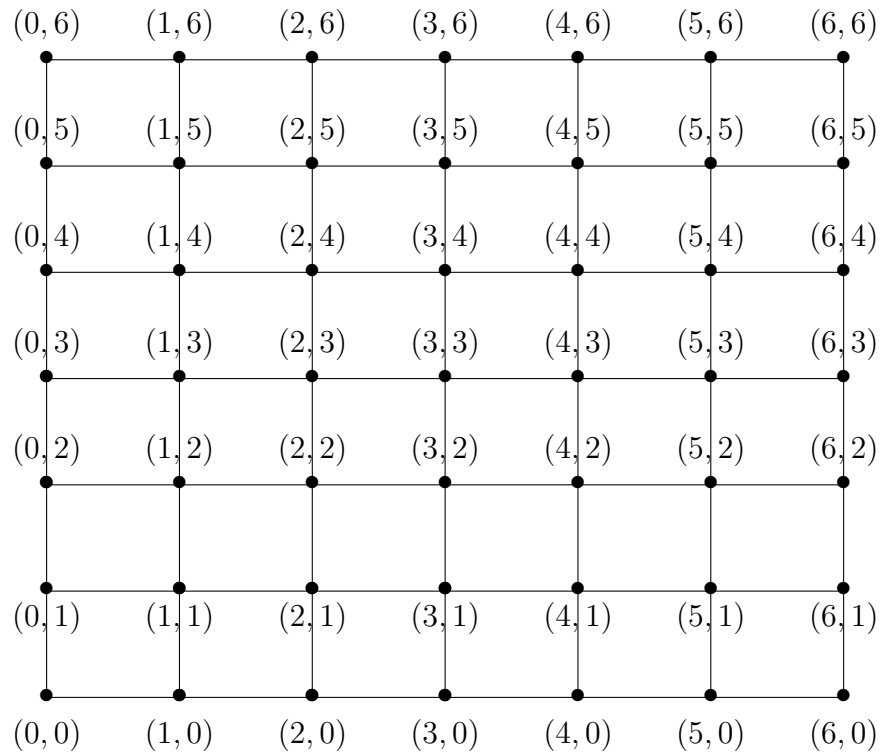


FIGURA 4.1. Números de Catalan - Diagrama n=6



El mensaje que actúa como recipiente para el mensaje oculto son los números en el triángulo de Pascal, los cuales se pueden obtener al calcular el número de trayectorias reticulares que conectan el punto  $(0, 0)$  con cada punto del diagrama  $D$ . Tales trayectorias se denominan reticulares ya que si  $T = (i, j), \dots, (0, 0)$  es una de tales trayectorias conectando los puntos  $(i, j)$  y  $(0, 0)$  entonces un punto  $(k, l) \in D$  con  $0 < k < i$ ,  $0 < l < j$  es un punto intermedio de  $T$  si además uno y solo uno de los puntos en el conjunto  $\{(k-1, l), (k, l-1)\}$  también pertenece a  $T$ . Por ejemplo, la siguiente es una trayectoria reticular conectando los puntos  $(0, 0)$  y  $(2, 2)$ :

$$(2, 2) \quad (2, 1) \quad (1, 1) \quad (0, 1) \quad (0, 0).$$

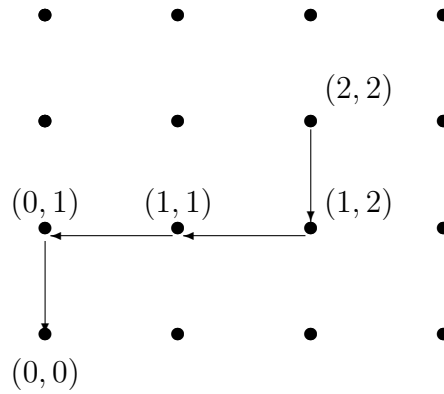


FIGURA 4.2. Trayectoria Reticular  $(0,0)$  y  $(2,2)$

$$(1, 1) \quad (0, 1) \quad (0, 0)$$

es una trayectoria reticular conectando  $(1, 1)$  y  $(0, 0)$ .

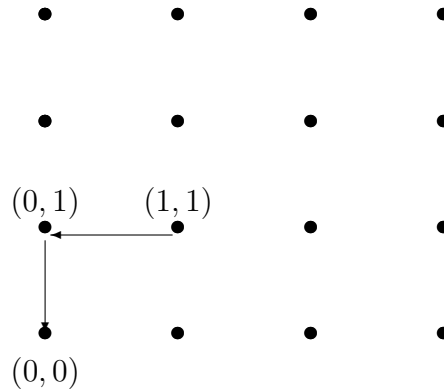


FIGURA 4.3. Trayectoria Reticular  $(1,1)$  y  $(0,0)$

En A. Moreno [5] se prueba que el número  $c(i, j)$  de trayectorias reticulares que conectan los puntos  $(0, 0)$  y  $(i, j)$  es:

$$c(i, j) = \binom{i+j}{j}$$

Para ello se considera que  $c(0, 0) = 1$ . El triángulo de Pascal se obtiene al asignar  $c(i, j)$  al punto  $(i, j)$  en  $D$ , como se ilustra en el siguiente diagrama para el caso  $n = 6$ .

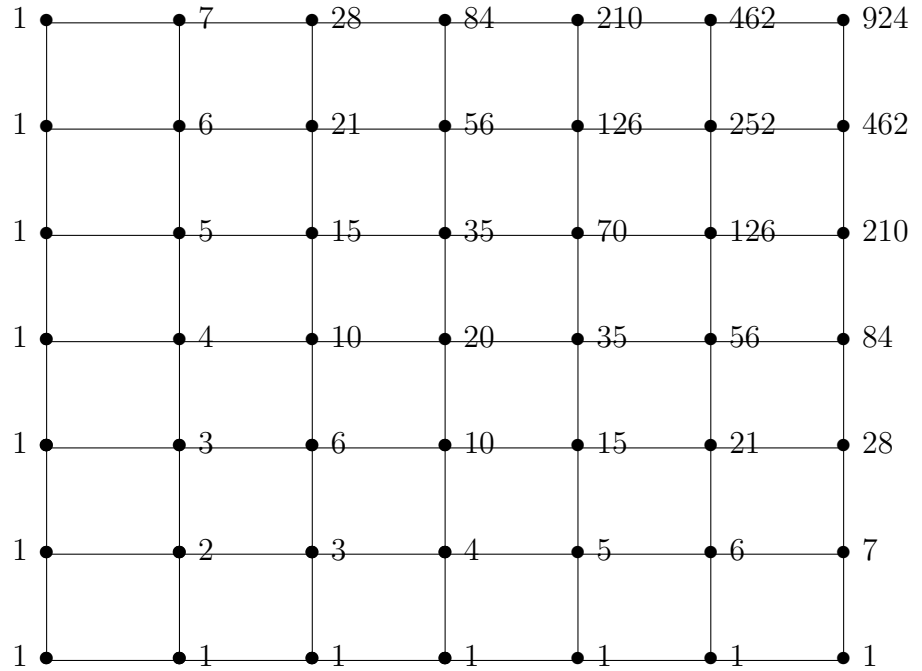


FIGURA 4.4. Triángulo de Pascal  $n=6$

En adelante,  $T$  denota el triángulo de Pascal, el cual es obtenido asociándole los números  $c(i, j) = \binom{i+j}{j}$  a los puntos del diagrama  $D$ .  $T_n$  se usará para denotar el arreglo finito que le corresponde a  $D_n$ . En este trabajo, se usará frecuentemente la notación  $c(i, j)$  para describir números combinatorios.

Una vez construido el recipiente se extrae un mensaje secreto oculto en él, para ello se emplea la siguiente clave esteganográfica:

$$K = k_{(ij)} = \begin{cases} 1, & i = j, \\ 0, & \text{en la alternativa.} \end{cases}$$

Si se superpone la clave  $K$  a  $D$  se observará la siguiente sucesión:

$$M = M_n \quad n \geq 0 = 1, 2, 6, 20, 70, 252, 924, \dots,$$

Si ahora contamos el número de trayectorias reticulares  $L_j$  conectando el punto  $(0, 0)$  con cada uno de los puntos  $(j, j) \in D$  encontramos la sucesión:

$$L = (L_n)_{n \geq 0} = (1, 1, 2, 5, 14, 42, 132, 429, 1430, 5852, \dots),$$

De donde, para cada  $k \geq 0$  se tiene:

$$L_k = \frac{M_k}{k+1} = \frac{c(k,k)}{k+1} = \frac{1}{k+1} \binom{2k}{k} = C_k; \text{ el } k\text{-ésimo número de Catalan.}$$

Se observa que el mensaje  $(C_1, C_2, \dots, C_n)$  se obtiene del recipiente  $T$  con la clave  $K = ((1, 0), (2, 0), (3, 0), \dots)$ .

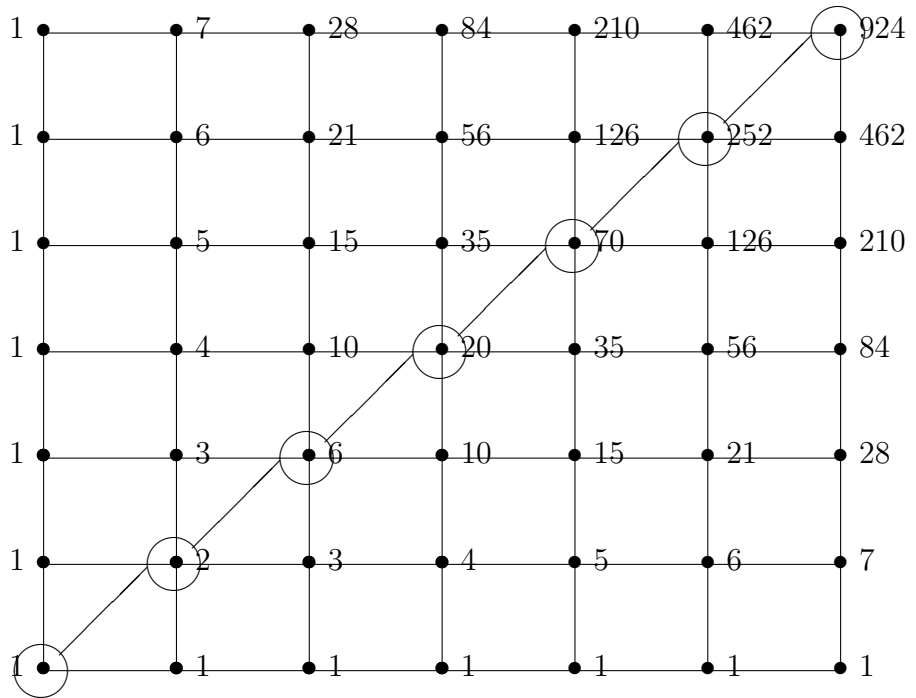


FIGURA 4.5. Triángulo de Pascal y Números de Catalan

El siguiente diagrama ilustra la relación entre las sucesiones  $M_n$  y  $L_n$ .

Las etiquetas en el diagrama muestran que el número de trayectorias reticulares coincide con el correspondiente número de Catalan:

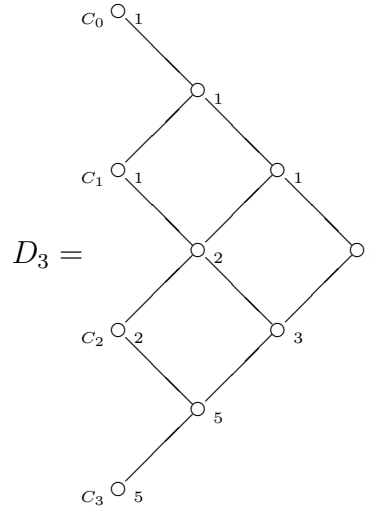


FIGURA 4.6. Trayectorias Reticulares y Números de Catalan

#### 4.1.1. Algunas Propiedades de los Números de Catalan

En esta sección se describen las soluciones dadas por Martin Erickson en [12] a algunos problemas combinatorios que conciernen números de Catalan. En ellas se usan las técnicas descritas en la sección anterior.

El siguiente resultado establece una relación entre números de Catalan.

**Teorema 4.1.** *el determinante de  $A_n = (A_{(i,j)})$  con  $A_{(i,j)} = (C_{i+j-2})$ ,  $(i, j \geq 1)$  denotado  $A_n$  es 1 para todo  $n$ .*

Por ejemplo si  $n = 3$ ;

$$A_3 = \begin{vmatrix} 1 & 1 & 2 \\ 1 & 2 & 5 \\ 2 & 5 & 14 \end{vmatrix} = 1$$

**Demostración.** Se observa en primera instancia que  $A = \sum_{\sigma} sgn(\sigma) \prod_{i=1}^n a(i, \sigma(i))$ , en donde  $\sigma$  es una permutación del conjunto  $1, 2, \dots, n$  y  $sgn(\sigma)$  es el signo de la permutación  $\sigma$ . ( $sgn(\sigma) = 1$  si se puede escribir como el producto de un número par de transposiciones o ciclos de longitud dos,  $sgn(\sigma) = -1$ , si ella puede escribirse como un producto de un número impar de transposiciones).

Observemos el caso  $n = 3$  en detalle:

Como el elemento  $A_{(i,j)} = C_{i+j-2}$ ,  $1 \leq i, j \leq 3$  entonces un sumando típico en el determinante de  $A_3$  es el número de sistemas de tres trayectorias conectando los puntos  $-(i-1), -(i-1)$  a los puntos  $(\sigma(i)-1, \sigma(i)-1)$ ,  $1 \leq i \leq 3$  multiplicado por  $\text{sgn}(\sigma)$ .

Se afirma que si dos trayectorias en un sistema de este tipo tienen un punto en común entonces tal sistema no será considerado en la suma. En efecto, si una trayectoria que comienza en un punto  $a$  y finaliza en un punto  $a'$  tiene un punto en común  $c$  con otra trayectoria con puntos terminales  $b$  y  $b'$  entonces si se invierten los puntos de las trayectorias después del punto  $c$ , se obtienen una trayectoria comenzando en  $a$  y finalizando en  $b'$  y otra trayectoria comenzando en  $b$  y finalizando en  $a'$  que también tienen el punto  $c$  en común. Cuando el determinante es calculado, los correspondientes sumandos tienen signos opuestos, ya que la transposición que cambia los puntos  $a'$  y  $b'$  cambia el signo de la permutación. De donde la contribución de estos sistemas al determinante es nula. Por lo que solo deben considerarse sistemas de tres trayectorias que no tengan puntos en común. Lo cual hace el cálculo mas simple.

Ahora se observará que la identidad es la única permutación con un sistema de tres trayectorias sin puntos en común. Para ello, se considera que cualquier trayectoria que empiece en  $(-2, -2)$  y finalice en  $(2, 2)$  no puede contener los puntos  $(0, 0)$  o  $(1, 1)$ , ya que de otra forma, el sistema de trayectorias que la contenga tendría un punto en común. Por lo que se puede asumir que una trayectoria comenzando en  $(-2, -2)$  finaliza en  $(2, 2)$ , la trayectoria que empieza en  $(-1, -1)$  finaliza en  $(1, 1)$  y que la trayectoria que empieza en  $(0, 0)$  finaliza en  $(0, 0)$ . Por lo que el único sistema de tres trayectorias  $(L_1 = (-2, -2), (-1, -2), (0, -2), (1, -2), (2, -2), (2, -1), (2, 0), (2, 1), (2, 2))$ ,  $L_2 = (-1, -1), (0, -1), (1, -1), (1, 0), (1, 1))$ ,  $L_3 = (0, 0)$  permitido en el cálculo del determinante está asociado a la permutación identidad con lo que el determinante de la matriz  $A_3$  es 1. El mismo argumento, puede usarse para todo  $n$ .  $\square$

Si se considera ahora que los números de Catalan ocultan un mensaje cifrado via el sistema criptográfico  $\mathcal{C}$  con clave  $K = ((2, 1), (2, 1), \dots)$ . Entonces dicho texto se puede recuperar al escribir los números de Catalan en una tabla o regla con una sola fila superponiendole una correspondiente clave esteganográfica, definida de la siguiente forma:

$$K = k_{1j} = \begin{cases} 1, & j = 2^k - 1 \text{ para algún } k \\ 0, & \text{en la alternativa.} \end{cases}$$

El siguiente es el mensaje que se observa al hacer la superposición mencionada:

$$C_0, C_1, C_3, C_7, C_{15}, \dots$$

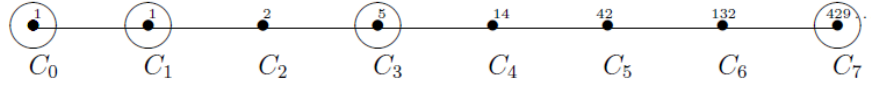


FIGURA 4.7. Clave Esteganográfica - Números de Catalan

El siguiente resultado permite verificar que la clave  $K = ((2, 1), (2, 1), (2, 1), (2, 1), \dots)$  ha sido usada para obtener el cifrado  $C = C_0, C_1, C_3, C_7, \dots$ , con el texto en claro  $P = 0, 0, 2, 214, \dots$ .

**Teorema 4.2.**  $C_n$  es impar si y solo si  $n = 2^k - 1$  para algún  $k$ .

**Demostración.** Se hará la prueba por inducción teniendo en cuenta que para todo  $n \geq 1$ ,  $C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}$  (lo cual se puede probar fácilmente al identificar los números de Catalan con el número de trayectorias reticulares, observe la Figura 4).

La afirmación de la proposición es válida si  $n = 0$ , ya que  $C_0 = 1$  y  $0 = 2^0 - 1$ . Consideremos entonces que la proposición es cierta para todo  $k$ ,  $0 \leq k \leq n$  y probemos que por tanto ella es cierta para  $C_{n+1}$ . Si  $n + 1$  es par entonces de la relación de recurrencia se tiene que:

$$C_{n+1} = 2 \sum_{i=0}^{(n-1)/2} C_i C_{n-i}$$

el cual es par.

Si  $n + 1$  es impar entonces:

$$C_{n+1} = 2 \sum_{i=0}^{(n-2)/2} C_i C_{n-i} + C_{n/2}^2$$

el cual es impar si y solo si  $C_{n/2}$  es impar. Por lo tanto,  $C_{n+1}$  es impar si y solo si  $C_{n/2}$  es impar, por hipótesis de inducción tal hecho ocurre si y solo si  $n/2 = 2^k - 1$ , para algún  $k$  y por lo tanto  $n + 1 = 2^{k+1} - 1$ .  $\square$

La siguiente es otra relación de recurrencia satisfecha por los números de Catalan:

$$C_n = \frac{4n-2}{n+1} C_{n-1}, \quad n \geq 1 \quad (4.1.2)$$

La fórmula (4.1.2) puede ser usada para probar el siguiente resultado.

**Teorema 4.3.**  $C_{3k-1} \equiv C_{3k} \equiv C_{3k+1} \pmod{3}$ .

**Demostración.** Como  $C_n = \frac{1}{n+1} \binom{2n}{n}$  entonces al multiplicar la igualdad en (4.1.2) por  $n+1$  se tiene:

$$(n+1)C_n = (4n-2)C_{n-1},$$

luego  $(n+1)C_n \equiv (n+1)C_{n-1} \pmod{3}$ , de donde si  $n = 3k$  entonces  $C_{3k} \equiv C_{3k-1} \pmod{3}$  y si  $n = 3k+1$  entonces  $C_{3k+1} \equiv C_{3k} \pmod{3}$ , de donde se tiene el resultado.  $\square$

### 4.1.2. Números de Delannoy

En esta sección se introduce un sistema criptográfico con el que se puede obtener una fórmula para los números de Delannoy. Los cuales se definen como el número de trayectorias  $d(i, j)$  que conectan puntos  $(i, j)$  del diagrama  $D$  con el origen. En este caso, los puntos en las trayectorias toman las direcciones  $(1, 0)$ ,  $(1, 1)$  y  $(0, 1)$ . Note que en una trayectoria reticular los puntos toman las direcciones  $(1, 0)$  y  $(0, 1)$ .

El siguiente diagrama muestra el número de trayectorias del nuevo tipo (que en adelante llamaremos trayectorias de Delannoy) conectando puntos  $(i, j)$ ,  $1 \leq i, j \leq 6$  con  $(0, 0)$  en  $D_n$  con  $n = 6$ :

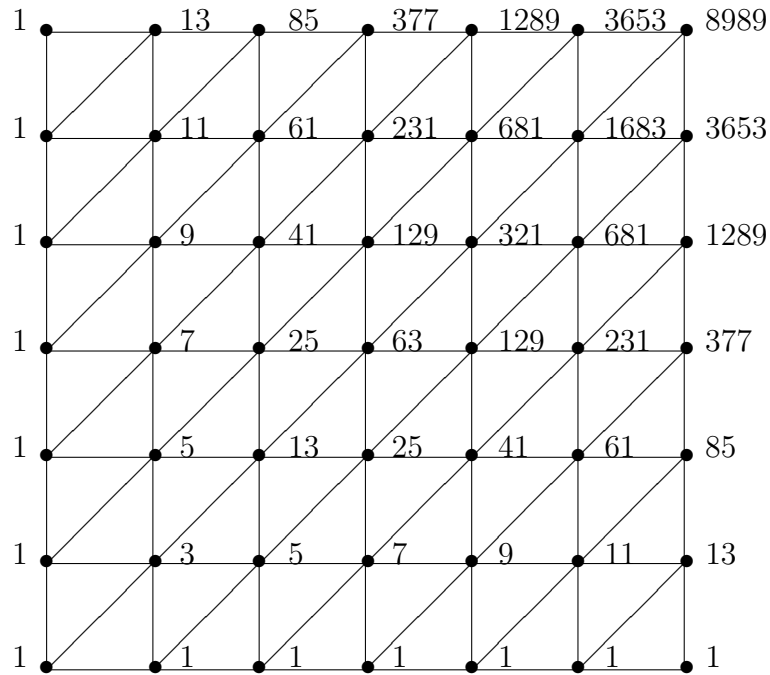


FIGURA 4.8. Trayectorias Números de Delannoy

En adelante  $T^i$  denota el conjunto que consta de sucesiones  $S$  de números en  $T$  tales que  $S = ((c(i-h, h), (c(i+r-h, h))) \quad i, r \geq 0, 0 \leq h \leq i$ .

Se define el sistema criptográfico  $\mathcal{D}$  de forma tal que para  $i \geq 0$  fijo y secreto:

$$\begin{aligned}
P &= K = T^i \\
C &= \mathbb{N} \\
e_k(x) &= \sum_{h=0}^i 2^h c(i-h, h) c(i+r-h, h) \\
d_k(y) &= ((c(i-h, h), c(i+r-h, h)) \quad 0 \leq h \leq i
\end{aligned} \tag{4.1.3}$$

En donde  $k = (c(i-h, h)) \quad 0 \leq h \leq i$  y  $d_k(y)$  es solución de la ecuación:

$$y = 2^0 c(i, 0) x_0 + 2^1 c(i-1, 1) x_1 + \cdots + 2^i c(0, i) x_i. \tag{4.1.4}$$

Por ejemplo, el cifrado del texto en claro:

$$x = c(3, 0), c(2, 1) \text{ .}$$

es 7 con  $k = c(1, 0), c(0, 1) \text{ .}$

La siguiente Figura 4.9 muestra los puntos en el diagrama  $D$  asociados al texto en claro:

$$x = c(3, 0), c(2, 1), c(1, 2)$$

y su correspondiente clave. En este caso,  $k = c(2, 0), c(1, 1), c(0, 2)$  y  $e_k(X) = 25$ .

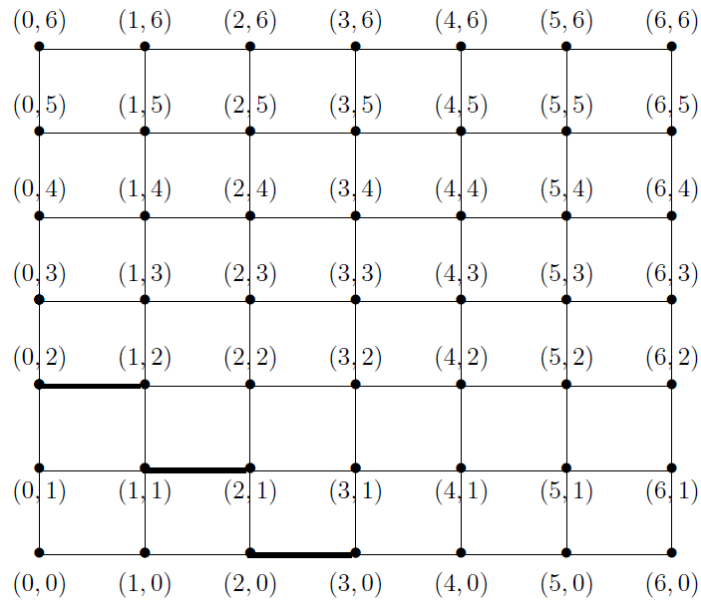


FIGURA 4.9. Diagrama  $D$  asociados al texto claro



Note que para  $k_i$ ,  $1 \leq i \leq 3$  convenientemente elegido:

$$\begin{aligned} d_{k_1}(7) &= c(3, 0), c(2, 1) \\ d_{k_2}(25) &= c(3, 0), c(2, 1), c(1, 2) \\ d_{k_3}(3) &= c(1, 0), c(0, 1) . \end{aligned} \quad (4.1.5)$$

El siguiente resultado, permite establecer la unicidad de  $d_k(y)$  en  $\mathcal{D}$ , para una clave fija  $k$  y un texto cifrado  $y$ . Además provee una fórmula para los números de Delannoy.

**Teorema 4.4.**  $d(i, j) = \sum_{h=0}^j 2^h \binom{i}{h} \binom{j}{h}$

**Demostración.** Por inducción aplicando la recurrencia,  $d(i, j) = d(i-1, j) + d(i, j-1) + d(i-1, j-1)$ .  $\square$

**Corolario 4.5.** La ecuación  $d(2, j) = x^2 + y^2$  tiene solución en los enteros positivos para todo  $j > 1$ .

**Demostración.** Note que  $d(2, 1) = 5 = 1^2 + 2^2$ ,  $d(2, 2) = 13 = 2^2 + 3^2$ . Si se supone que para todo  $k$ ,  $1 \leq k \leq j$  se cumple el corolario. Entonces  $d(2, j+1) = d(2, j) + d(1, j+1) + d(1, j) = j^2 + (j+1)^2 + 2j+1 + 2j+3 = (j+2)^2 + (j+1)^2$ .  $\square$

El Corolario (4.5) permite concluir que si  $\alpha$  es la potencia de un divisor primo  $q$  de un número  $d(2, j)$  con  $q \equiv 3 \pmod{4}$  entonces  $\alpha = 2j$ , en donde  $j$  es un entero no negativo.

**Nota 4.6..** La siguiente es la solución a la ecuación Diofántica:

$$A_1 x_1 + A_2 x_2 + \cdots + A_n x_n = A, A_1 = 0 \quad (4.1.6)$$

del tipo (4.1.4) desarrollada por K. Weihrauch y descrita por Dickson en [10].

Sean  $E(M : N)$  y  $R(M : N)$  la parte entera y el residuo que resultan de dividir el entero  $M$  por el entero  $N$ , respectivamente. Entonces se definen

$$\begin{aligned} x_1 &= E(A : A_1) - x_2 E(A_2 : A_1) - \cdots - x_n E(A_n : A_1) + t_1 \\ t_1 &= \frac{1}{A_1} R(A : A_1) - x_2 R(A_2 : A_1) - \cdots - x_n R(A_n : A_1) . \end{aligned} \quad (4.1.7)$$

El mismo proceso puede hacerse para obtener  $x_2$ . Por lo que se puede lograr una relación entre  $x_{n-1}$  y  $x_n$ , cuya solución involucra un término  $t_{n-1}$ . Luego

$$x_i = M_i + a_{i1} t_1 + \cdots + a_{i(n-1)} t_{n-1} \quad (i = 1, 2, \dots, n) \quad (4.1.8)$$

en donde  $M_1, \dots, M_n$  es un conjunto de soluciones de (4.1.6) y

$$A_1 a_{1j} + A_2 a_{2j} + \dots + A_n a_{nj} = 0, (j = 1, \dots, (n-1))$$

(4.1.8) genera todas las soluciones de (4.1.6) dado que:

$$\frac{1}{A_1} a_{ij} = \pm 1 (i = 2, \dots, n; j = 1, \dots, (n-1)).$$

**Nota 4.7..** Si  $i$  es conocido en el sistema criptográfico  $\mathcal{D}$  entonces  $\mathcal{D}$  es vulnerable a un ataque de texto claro conocido, ya que si se conocen una colección suficiente de esquemas texto en claro-texto cifrado entonces la clave  $k$  se puede obtener al resolver un sistema de ecuaciones lineales en  $\mathbb{Z}$ . Esto es,  $k = (k_1, k_2, \dots, k_i)$  se puede obtener al resolver un sistema de ecuaciones lineales del tipo:

$$\begin{bmatrix} x_{11} & x_{12} & \dots & x_{1i} \\ x_{21} & x_{22} & \dots & x_{2i} \\ \vdots & \vdots & \vdots & \vdots \\ x_{i1} & x_{i2} & \dots & x_{ii} \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_i \end{bmatrix} = \begin{bmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{i1} \end{bmatrix} \quad (4.1.9)$$

Esto es, si se escribe (4.1.9) en la forma  $Xk = y$  con  $X \neq 0$  entonces  $k = X^{-1}y$ , lo cual se puede expresar de la siguiente forma:

$$\begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_i \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1i} \\ x_{21} & x_{22} & \dots & x_{2i} \\ \vdots & \vdots & \vdots & \vdots \\ x_{i1} & x_{i2} & \dots & x_{ii} \end{bmatrix}^{-1} \begin{bmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{i1} \end{bmatrix} \quad (4.1.10)$$

## 4.2. Números Poligonales y Criptografía

En esta sección se usan técnicas esteganográficas y criptográficas para definir y deducir propiedades de los números triangulares, cuadrados y pentagonales.

Los pitagóricos solían representar los números mediante punto en la arena o piedrecillas, clasificándolos según las formas de estas distribuciones de puntos o piedras. Así, los números 1, 3, 6, 10, etc. recibían el nombre de triangulares porque los puntos correspondientes podían distribuirse en forma de triángulo equilátero. El cuarto número triangular, el 10, ejerció una fascinación especial sobre los pitagóricos, siendo para ellos una especie de número sagrado, que tiene cuatro puntos en cada lado; el 4 era otro de sus números favoritos. Los pitagóricos comprobaron que las sumas 1,  $1 + 2$ ,  $1 + 3$ , y así sucesivamente, daban lugar a los números triangulares y que  $1 + 2 + \dots + n = n \cdot (n + 1)/2$ . Los números 1, 4, 9, 16, ... recibieron el nombre de

números cuadrados debido a que sus puntos pueden distribuirse formando cuadrados. Los números compuestos (o no primos) que no eran cuadrados perfectos recibían el nombre de oblongos, como se observa en la siguiente figura.

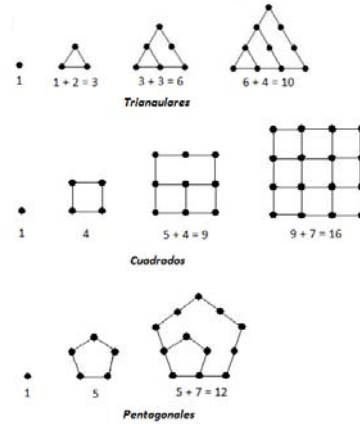


FIGURA 4.10. Números Poligonales

A partir de las distribuciones geométricas de los puntos aparecían como evidentes ciertas propiedades de los números enteros: por ejemplo, trazando la recta diagonal se descubre que la suma de dos triangulares consecutivos es un número cuadrado, como lo expone Kline[23].

$$\frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} = (n+1)^2$$

*Todo número cuadrado es suma de dos números triangulares*

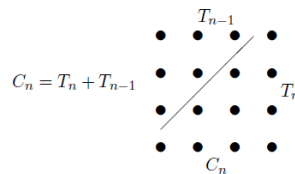


FIGURA 4.11. Propiedad de los Números Cuadrados

Podemos observar geométricamente otra propiedad: *la suma de los números impares es un cuadrado*

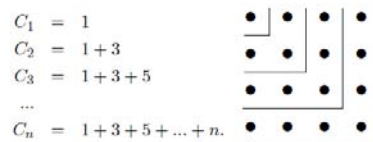


FIGURA 4.12. Propiedad Suma de Números Impares

Diofanto de Alejandría (s. III d.C) además de su famosa Aritmética, escribió otro libro, del que por desgracia sólo se conservan fragmentos, sobre los números poligonales, en el que la idea de su construcción se extiende al espacio, haciendo su aparición los números piramidales, que se obtienen apilando en capas los sucesivos números poligonales de un mismo orden.

La curiosidad sobre estos números va a llegar a la Edad Media gracias a las obras de Nicómaco de Gerasa (s. I d.C.) que llegó a descubrir resultados generales de interés como el hecho de que *el cubo de todo número entero  $n$ , es la suma de  $n$  números impares consecutivos*. En muchos de los manuscritos medievales inspirados en las obras de Boecio se puede encontrar referencias gráficas de los números poligonales que intentan describir de manera general estos números.

Es en siglo XVII, Pierre de Fermat, que va a dirigir su atención sobre los números poligonales, pero esta vez para lanzar uno de sus retos en forma de conjetura:

*“Todo número entero puede expresarse mediante suma de, a lo sumo,  $n$  números  $n$ -gonales”*. Se sabe los matemáticos Lagrange y Gauss aceptaron el reto, y fue este último quien publicó que: “Todo número entero es suma de, a lo sumo, tres números triangulares”. [39]

Estos maravillosos números han fomentado diversa curiosidades, es así que los números poligonales y especialmente los números triangulares se utilizaron como una forma de cifrar datos en papiros, éstos pudieron ser descifrados miles de años después. El triángulo de Pascal puede ser tratado como un texto cifrado por transposición

para que una vez obtenida una clave geométrica se puedan obtener resultados que tienen que ver con familias de números que son sumas de ciertas clases de números  $n$ -agonales. Por lo que la solución a estos problemas se reduce a hallar las claves de transposición empleadas para obtener este arreglo en particular.

A continuación se puede ver un ejemplo de este método, dadas las investigaciones de A. Moreno (2006) [3]

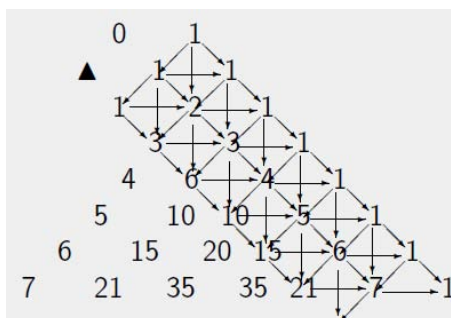


FIGURA 4.13. Claves con el Triángulo de Pascal

Los números que representan conjuntos, cuyos elementos se pueden situar en forma de figura geométrica regular se llaman *números figurados*. Los números figurados cuyo arreglo forma un polígono regular se denominan *números poligonales* (triangulares, cuadrados, pentagonales, hexagonales, etc). El  $k$ -ésimo número  $n$ -gonal deno-

tado  $p_k^n$ , se obtiene con la formula

$$p_k^n = \frac{1}{2}[(n-2)k^2 - (n-4)k] \quad (4.2.11)$$

en donde con  $n = 3$  se producen los números triangulares, con  $n = 4$  los cuadrados, etc.

Es importante resaltar que alrededor del año 1638, Fermat hizo la siguiente afirmación (probada por Cauchy en 1830), la cual tal vez describe el hecho mas relevante que concierne este tipo de números:

*Todo número puede ser expresado como una suma de a lo mas tres números triangulares, a lo mas cuatro números cuadrados, a lo mas cinco números pentagonales y asi sucesivamente hasta infinito.*

Matemáticos como Gauss en 1796, Legendre en 1798 también encontraron resultados excelentes sobre estos números. La demostración definitiva fue dada por Carl Friedrich Gauss en 1801 en sus *Disquisitiones*. Existe una hermosa prueba del teorema de Cauchy dada por Nathanson en 1987 [31]

Luego de realizar esta introducción histórica sobre los Números Poligonales, se continuará con el objetivo de de usar la esteganografía y criptografía para identificar las propiedades de éstos números.

Se define una clave esteganográfica  $K$  para el recipiente  $D$ , de la siguiente forma:

$$K = K_{ij} = \begin{cases} 0, & i = 1, 0 \leq j \leq h, \\ 0, & i = 2, j = h \\ 1, & \text{en la alternativa.} \end{cases}$$

La Figura 4.14. muestra el conjunto de números que la clave deja observar si  $j = 4$ .

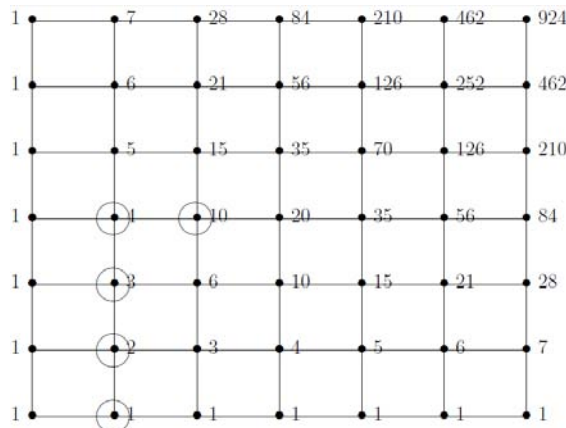


FIGURA 4.14. Conjunto de Números, si  $j = 4$

Por definición para cada  $j$  la clave deja ver el texto:

$$(c(1, t) \quad 0 \leq t \leq j, c(2, j))$$

tal que:

$$\sum_{t=0}^j c(1, t) = c(2, j) = \frac{(j+2)(j+1)}{2} \quad (4.2.12)$$

La identidad (4.2.12) permite establecer que para todo  $k \geq 0$ ,

$$p_{(k+1)}^3 = c(2, k). \quad (4.2.13)$$

Al usar el sistema criptográfico  $\mathcal{C}$  para cifrar el texto en claro:

$$x = (c(2, k) \quad 0 \leq k \leq j)$$

usando la clave:

$$k = (k_t \quad 1 \leq t \leq j+1, 0) = (k_t = c(2, t) \quad 1 \leq t \leq j, 0)$$

se obtiene el texto cifrado:

$$y = (y_k = c(2, k) + c(2, k+1) \quad 0 \leq k \leq j)$$

en donde para cada  $k$ :

$$y_k = p_k^3 + p_{k+1}^3 = p_k^4. \quad (4.2.14)$$

Si para  $j \geq 0$  fijo se descifra (en  $\mathcal{C}$ ) el texto:

$$y = (y_t = c(2, 2t) \quad 1 \leq t \leq j)$$

con la clave:

$$k = (k_t = c(2, t-1) \quad 1 \leq t \leq j, 0)$$

se obtiene el texto en claro:

$$x = (x_t = y_t - k_t \quad 1 \leq t \leq j)$$

se concluye que para  $k \geq 1$ :

$$c(2, 2k) - c(2, k - 1) = p_k^5. \quad (4.2.15)$$

Si la clave usada para obtener (4.2.15) se usa para cifrar el texto en claro:

$$x = (x_t = c(2, 2t) \quad 1 \leq t \leq j)$$

se obtiene el texto cifrado:

$$y = (y_t = c(2, 2t) + c(2, k - 1) \quad 1 \leq t \leq j)$$

en este caso se concluye:

$$c(2, 2k) + c(2, k - 1) = p_k^7. \quad (4.2.16)$$

Si en  $\mathcal{C}$  la clave:

$$k = (k_t = 2c(2, t - 1) \quad 1 \leq t \leq j, 0)$$

se usa para cifrar el texto en claro:

$$x = (x_t = c(2, 2t) \quad 1 \leq t \leq j)$$

se obtiene el texto cifrado:

$$y = (c(2, 2t) + 2c(2, t - 1) \quad 1 \leq t \leq j)$$

luego para todo  $k \geq 1$ :

$$c(2, 2k) + 2c(2, k - 1) = p_k^8 \quad (4.2.17)$$

Dado que al superponer la siguiente clave esteganográfica  $K$  a  $T$ :

$$K = K_{ij} = \begin{cases} 0, & i = 2, j = 2t, t \geq 0, \\ 1, & \text{en la alternativa.} \end{cases}$$

se obtiene la sucesión:

$$c(2, 2k) = p_k^6, k \geq 0. \quad (4.2.18)$$

Entonces se concluye el siguiente resultado como una consecuencia de las identidades (4.2.15), (4.2.16), (4.2.17) y (4.2.18):

**Teorema 4.6.** *Dados  $n$  y  $k$  fijos con  $5 \leq n \leq 8$  y  $k \geq 1$  entonces existen enteros  $a, b$  tales que  $ac(2, 2k) + bc(2, k - 1) = p_k^n$ .  $\square$*

Como los números de la forma  $2^n(32^{n+1} - 1)$  con  $n \geq 0$  son pentagonales de rango positivo. Entonces se concluye la siguiente consecuencia del Teorema 4.6:

**Corolario 4.7.** *Si  $n, m$  son números enteros tales que  $n = 2^{m-1}(2^m - 1)$  y  $m \geq 1$  entonces  $n$  puede escribirse como la suma de exactamente  $m$  números pentagonales de rango positivo.*

**Demostración.**  $n = 1 + \sum_{i=1}^{m-1} [2^{m-i}(2^{m-i+1} - 1) - 2^{m-i-1}(2^{m-i-2} - 1)]$ .  $\square$

Si  $\mathcal{F} = \{f_i \mid f_i \in \mathbb{N}\}$  es un conjunto de enteros positivos entonces se dice que  $\mathcal{F}$  genera al entero  $a$  o que  $a$  es una combinación lineal de los enteros  $f_i$  si existe un conjunto de enteros positivos  $\mathcal{A} = \{a_i \mid a_i \in \mathbb{N}\}$  tal que:

$$a = \sum_{a_i \in \mathcal{A}} a_i f_i. \quad (4.2.19)$$

Con esta notación se puede enunciar el siguiente resultado:

**Teorema 4.8.** *El conjunto  $\mathcal{G} = \{p_{2^k}^5 \mid k \geq 1\}$  genera los enteros de la forma  $S_n = \frac{32(4^{2n}-1)}{15}$ ,  $n \geq 0$ .*

**Demostración.** Si  $n$  es par y  $x$  denota el menor entero mayor o igual que  $x$  entonces:

$$S_n = p_{2^{2n+1}}^5 + p_{2^{2n}}^5 + 2(p_1^5 + p_{2^{2n-1}}^5 + p_{2^{2n-2}}^5) + 3(p_{2^{2n-3}}^5 + p_{2^{2n-4}}^5 + p_{2^1}^5 + p_{2^2}^5) + 4(p_{2^{2n-5}}^5 + p_{2^{2n-6}}^5 + p_{2^3}^5 + p_{2^4}^5) + \dots \left(\frac{n}{2} + 2\right)(p_{2^{n-1}}^5 + p_{2^n}^5).$$

Si  $n$  es impar entonces:

$$S_n = p_{2^{2n+1}}^5 + p_{2^{2n}}^5 + 2(p_1^5 + p_{2^{2n-1}}^5 + p_{2^{2n-2}}^5) + 3(p_{2^{2n-3}}^5 + p_{2^{2n-4}}^5 + p_{2^1}^5 + p_{2^2}^5) + 4(p_{2^{2n-5}}^5 + p_{2^{2n-6}}^5 + p_{2^3}^5 + p_{2^4}^5) + \dots \left(\frac{n}{2} + 2\right)(p_{2^n}^5).$$

Notese que cada sumando tiene la forma  $xa_x$  en donde  $a_x$  es la suma de a lo mas 4 elementos de  $\mathcal{G}$ . De hecho, si se nota  $H_{<}^i$  ( $H_{\geq}^i$ ) el conjunto de elementos de  $\mathcal{G}$  usados en la construcción del sumando  $a_i$  menores (mayores o iguales) que  $\bar{p} = p_{\lceil \frac{2n+1}{2} \rceil}^5$  entonces salvo para el primer y el último sumando se tiene que:

$$a_i = \sigma(a_i) + \sigma'(a_i) + \gamma(a_i) + \gamma'(a_i)$$



$$\sigma(a_i), \sigma'(a_i) \quad H_{<}^i, \sigma(a_i) = \sigma'(a_i).$$

$$\gamma(a_i), \gamma'(a_i) \quad H_{\geq}^i, \gamma(a_i) = \gamma'(a_i).$$

$$\sigma(a_1) = p_1^5, \sigma'(a_1) = 0, \gamma(a_1) = \gamma'(a_1) = 0.$$

$$\sigma(a_i) = \begin{cases} p_{2^{i-1}}^5, & i - 1 < \frac{2n+1}{2}, \\ 0, & \text{de otro modo.} \end{cases}$$

$$\sigma'(a_i) = \begin{cases} p_{2^i}^5, & i < \frac{2n+1}{2}, \\ 0, & \text{de otro modo.} \end{cases}$$

$$\gamma(a_i) = \begin{cases} p_{2^{2n-2i+1}}^5, & i \geq \frac{2n+1}{2}, \\ 0, & \text{de otro modo.} \end{cases}$$

$$\gamma'(a_i) = \begin{cases} p_{2^{2n-2i}}^5, & i \geq \frac{2n+1}{2}, \\ 0, & \text{de otro modo.} \end{cases} \quad \square$$

## CAPÍTULO 5

---

---

# ASPECTOS PEGADÓGICOS Y DIDÁCTICOS

---

---

*Un gran descubrimiento resuelve un gran problema, pero hay una pizca de descubrimiento en la solución de cualquier problema. Tu problema puede ser modesto, pero si es un reto a tu curiosidad y trae a juego tus facultades inventivas, y si lo resuelves por tus propios métodos, puedes experimentar la tensión y disfrutar del triunfo del descubrimiento*

*George Polya*

### 5.1. Acerca de Aprendizaje Significativo

Este tipo de aprendizaje para Ausubel, hace referencia la forma en que se incorpora la nueva información. En este sentido plantea que el aprendizaje significativo se da cuando la nueva información se ofrece de manera no arbitraria, sino en estrecha relación con el conocimiento previo del que aprende. Así, en el momento en que aquello que se aprende se pone en relación y se integra a los conocimientos que ya se poseen es posible integrarlo a las estructuras del conocimiento actuales.

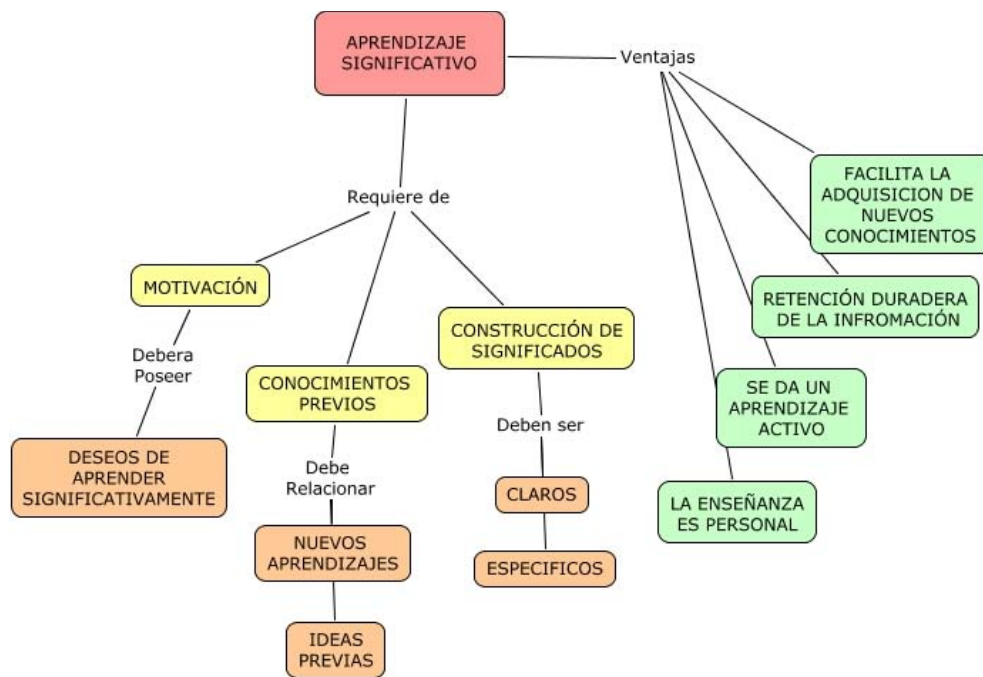
Esta teoría elaborada por David Ausubel, Joseph Novak, Helen Hanesian, Edmun Sullivan; conforme a H. Moreno [25] presenta algunas características:

- **Escuela:** La escuela para favorecer un aprendizaje significativo debe propiciar una selección y organización lógica de los contenidos a aprender en cada uno de los grados, es decir que el material a aprender tenga coherencia y significado.
- **Aprendizaje:** El contenido del aprendizaje debe ser potencialmente significativo, es decir, debe permitir ser aprendido de manera contextualizada. El

estudiante debe poseer en su estructura cognitiva los conceptos utilizados previamente formados, de manera que el nuevo pueda vincularse con el anterior. De igual forma, debe existir, disponibilidad, intención e interés por aprender.

- **Evaluación:** Se observa la estructura cognitiva altamente jerárquica y organizada con la presencia de conceptos diferenciados, estables y claros permitirá realizar un aprendizaje significativo.

El mapa que se muestra en la Figura 5.1. evidencia los aspectos importantes para el aprendizaje significativo según Ausubel.



Fuente: <http://aprendizajesignificativogm.blogspot.com/>

FIGURA 5.1. Aprendizaje Significativo

## 5.2. Metodología de Resolución de Problemas

La resolución de problemas se constituye en una herramienta fundamental para favorecer la articulación entre los saberes previos y los nuevos saberes y con ello la construcción de un aprendizaje significativo.

En el amplio campo que abarca la resolución de problemas se han hecho diversos estudios desde diferentes líneas de investigación tales como: la psicología, las matemáticas, la lingüística, etc., a fin de aplicarlo como un modelo educativo eficiente para ser trabajado en la escuela.

Una de las primeras investigaciones fue la realizada por el psicólogo Dewey en 1938. En su modelo planteó seis fases para la resolución de problemas las cuales fue-

ron: identificación de la situación problemática, Definición precisa del problema, Análisis medios-fines plan de solución, Ejecución del plan, Asunción de las consecuencias, Evaluación de la solución-supervisión-generalización ; de igual manera otros psicólogos siguieron trabajando con este modelo como lo fueron Mason, Burton, Stacey, Bransford, Stein. En la rama de las matemáticas se destacaron los trabajos de Polya, Schoenfeld, Goldin, Miguel de Guzmán, Puig, Cerdan entre otros.[41]

En la escuela se han tratado de introducir algunas de estas propuestas, con el fin de crear un enfoque metodológico de la resolución de problemas para la enseñanza de la matemática escolar, el cual tiene como objetivo desarrollar las capacidades investigativas del estudiante, por medio de situaciones que lo lleven a construir un saber firme nacido de su proceso investigativo, a fin de solucionar un problema.

Por otra parte, en este tipo de modelos, el maestro tiene como objetivo coordinar el proceso constructivo, de tal manera que el estudiante no pierda el rumbo de su investigación; también debe buscar el problema adecuado junto con él para que lo motive a adquirir el conocimiento relacionado con éste.

No se debe olvidar que el problema debe estar bien enfocado hacia los saberes a desarrollar en el grado, el lenguaje a utilizar con el estudiante sea el adecuado teniendo en cuenta el contexto en el que se encuentre, y su formulación debe dar a entender al alumno que no es una forma convencional de educación, pero que tampoco es una actividad momentánea.

En el modelo de Resolución de Problemas se puede encontrar aspectos favorables como lo son: el incentivar el espíritu investigativo en el estudiante, motivarlo a un cuestionamiento y reflexión constante sobre el trabajo a realizar, y el favorecimiento de intereses que busquen ampliar la visión del estudiante. Pero como todo modelo, este presenta algunas falencias como la falta de preparación por parte de los docentes para ponerlo en práctica en la escuela. Si no se tiene una buena guía se corre el riesgo que el estudiante pierda el rumbo a la solución.

Con base a las diversas propuestas que se conocen sobre resolución de problemas para este trabajo se considera que el modelo propuesto por Josefa Hernández y Martín Socas [41] es el más completo porque reúne aspectos trabajados por Polya y lo complementa con el sistema de representación de Goldin; su modelo propone fases como: la lectura del enunciado; comprensión; representación, ejecución y solución visual geométrica; representación, ejecución y solución formal; soluciones y finalmente la comprobación. En su modelo aclaran que estas fases no son lineales sino que el estudiante puede moverse de un tipo de representación a otra.

El enfoque metodológico de la resolución de problemas permite que la evaluación sea vista como el proceso global de cada uno de los individuos, donde su único referente no es sólo el estudiante, sino también el docente, la institución, la comunidad y en ella la familia.

**¿Qué es un problema?** Frente a esta pregunta se encuentran varias interpretaciones e investigaciones, Pero para este trabajo, se destaca la interpretación que hace Santos [38] , en la que se reconocen los siguientes componentes:

- a. La existencia de un interés.
- b. La no existencia de una solución inmediata.
- c. La presencia de varios caminos o métodos de solución (algebraico, geométrico, numérico).
- d. La atención por parte de una persona o grupo de individuos para llevar a cabo un conjunto de acciones tendientes a resolver esa situación

Como puede verse, en la solución de problemas, la vía para resolverlo es desconocida por el sujeto y éste quiere encontrar la solución. Esta es una de las consideraciones que deben tomarse en cuenta al plantear problemas, de tal forma que haga surgir la necesidad en el sujeto de resolverlo para que realmente quiera hacer las transformaciones convenientes.

En general, para que toda situación que se plantee al estudiante sea considerada un verdadero problema, éstas deben implicar la necesidad de un esfuerzo cognoscitivo por parte de quien los resuelve, en este caso el estudiante.

Desde el punto de vista didáctico, esa caracterización tiene algunas implicaciones, entre ellas:

1. *La no-consideración de problemas tipos.* Es decir, que esta actividad no debe realizarse de manera mecánica ni memorística.
2. *La necesidad de la motivación para lograr despertar el interés en al alumno.* Es un aspecto importante en el proceso de solución a problemas, ya que si el estudiante no está motivado para resolverlo, aunque la situación planteada sea un problema, este no estará interesado en realizar las etapas necesarias.

Todo problema tiene su fundamento en una situación percibida como tal por el sujeto, y es por tanto un hecho individual, que tiene lugar sólo cuando un sujeto determinado experimenta la necesidad de buscar o encontrar algo sobre lo cual sus conocimientos no son suficientes. Además, mientras para un sujeto, determinada situación puede ser percibida como un problema, para otro puede no serlo, ya que depende de sus conocimientos previos, lo que expresa el carácter relativo.

### ***Resolución de problemas***

Se presentan algunas definiciones según Juidías y Rodriguez, citada por Gracia [18] sobre resolución de problemas:

1. “Una cuestión que causa perplejidad o que presenta dificultad”(Webster, 1979).

2. “Una situación que exige la aplicación de un plan de acción con objeto de transformarla” (McDermott, 1978).
3. “Una tarea que plantea al individuo la necesidad de resolverla y ante la cual no tiene un procedimiento fácilmente accesible para hallar la solución” (Lester, 1983).
4. “Para Schoenfeld (1989), una actividad de aprendizaje es un verdadero problema si el alumno se interesa en ella y no tiene medios matemáticos de fácil acceso para alcanzar la solución”.

A continuación se presenta un cuadro analizado por [18] en relación a la investigación hecha por Gazcón (2001), donde se muestra los modelos de los docentes derivados de asumir ciertas teorías epistemológicas de la matemática, haciendo énfasis en el papel que cumple la resolución de problemas en cada uno de ellos.

		MODELOS DOCENTES	CARACTERÍSTICAS PRINCIPALES	PAPEL DE LA RESOLUCIÓN DE PROBLEMAS
TEORÍAS EPISTEMOLÓGICAS	<b>Euclidianismo</b> El conocimiento matemático se deduce de un conjunto finito de proposiciones trivialmente verdaderas (axiomas) que constan de términos perfectamente conocidos (términos primitivos).	Teoricismo	Pone el acento en los conocimientos acabados y cristalizados en ‘teorías’ no considerando la actividad matemática, sólo el fruto final de ésta.	Actividad auxiliar en el aprendizaje de las teorías, no constitutiva del pensamiento matemático. Usados para aplicar, ejemplificar, consolidar teorías, introducir conceptos, motivar o justificarlos.
		Tecnicismo	Identifica implícitamente “enseñar y aprender matemática” con “enseñar y aprender técnicas algorítmicas”	Trivializados por su fijación en las técnicas, especialmente algorítmicas. Consideran problemas no rutinarios y fuera del contexto en el que se originan.
	<b>Cuasi-empirismo</b> El origen y el método de la matemática, e incluso su propia justificación, ha de provenir de la experiencia... en un sentido más sofisticado de experiencia matemática	Modernismo	Identifica “enseñar y aprender matemáticas” con enseñar y aprender esta actividad exploratoria, libre y creativa, de problemas no triviales.	Hacer ensayos, conjeturas, formular planes de resolución, establecer contra ejemplos. El enunciado no indica el procedimiento para su solución, y el dominio conceptual en el que se encuentran es familiar al estudiante.
		Procedimentalismo	El fin principal del proceso de enseñanza y aprendizaje de las matemáticas el dominio de técnicas no algorítmicas (heurísticas).	Se centra en el desarrollo, utilización y dominio de “estrategias complejas” para resolver problemas.
	<b>Constructivismo</b> Los mecanismos e instrumentos que establecen la transición de un período de la matemática a otro se corresponden con los que establecen el paso de un “tránsito psicogenético” al siguiente.	Constructivismo psicológico	El conocimiento matemático se obtiene a través de un proceso exclusivamente psicológico. No se refieren explícitamente la naturaleza matemática, la construcción del conocimiento, ni el contexto en el que ésta se realiza.	Instrumento para la construcción de conocimientos nuevos. En los problemas propuestos el conocimiento que se pretende que el estudiante construya debe constituir el insumo más conveniente para su resolución.
		Constructivismo matemático	El estudiante construye el conocimiento a través de la formulación de un modelo matemático, de un sistema intra o extra-matemático.	Tiene como objetivo primordial la obtención de conocimientos sobre el sistema modelizado.

De lo anterior expuesto, se podría decir que el último modelo permite que a través de contextos cercanos a los estudiantes se puede lograr un aprendizaje más coherente y que surja de su propia necesidad.

### 5.3. Álgebra Escolar

En el álgebra escolar se evidencia fuertemente la existencia de una brecha cognitiva, cuando se inicia la transición del aritmética (trabajo con números) y el álgebra (trabajo más abstracto). En la dinámica escolar se reconoce la dificultad que tienen los estudiantes en aceptar el uso de las "letras." lenguaje simbólico en álgebra, más aún cuando no se dota de sus distintas interpretaciones y aceptar su uso conlleva a niveles de abstracción de representaciones mentales que generan dificultades que forman parte natural de un proceso de desarrollo, en el cual los conocimientos mínimos aritméticos se constituyen en obstáculos para el aprendizaje del álgebra

Los autores que más han investigado sobre el Álgebra escolar es el maestro Martín Socas [43] refenciando principalmente el trabajo de C. Kieran [14] y en Colombia Grupo Pretexto de la Universidad Distrital [35], quienes a través diferentes estudios han podido dedicarse a la revisión de las causas que más conllevan a las dificultades de enseñanza, aprendizaje, comunicación de los conceptos y procedimientos del álgebra escolar.

Ellos han podido determinar que las principales tareas del álgebra escolar se centran en identificar los aspectos del *lenguaje algebraico* como: las letras con significado algebraico (variables), las expresiones algebraicas, las ecuaciones lineales y cuadráticas, los procesos de pensamiento algebraico y la resolución de problemas, son ciertos aspectos del pensamiento numérico que establecen las pautas para la abstracción, es decir, los conocimientos que facilitan la transición del pensamiento numérico al algebraico y que tienen que ver con ideas acerca de los distintos tipos de números y de las relaciones numéricas, particularmente en algunos objetos matemáticos y procesos numéricos; como lo expresa como lo expresa Martín Socas (2011)[43]

Todas estas investigaciones, argumentan que es de suma importancia iniciar con este trabajo algebraico desde los primeros años de escolaridad, reorganizando el currículo dando una visión más amplia del contexto algebraico a través de secuencias, patrones, ecuaciones sencillas; para ir introducción paulatinamente los diferentes significados de las letras.

Autores como (Warner; Kieran, 1989; Bednarz; Kieran; Lee, 1996; Kieran, 2007; Filloy; Rojano; Puig, 2008) han evidenciado las dificultades de los jóvenes como se mencionó anteriormente en la transición de la aritmética al álgebra de la Educación Media se centra en que se inicia el trabajo con demasiado lenguaje simbólico sin permitir identificar diferentes contextos donde se emplean las "letras matemáticas", esto también es descrito por el grupo Pretexto, el cual apoya los estudios de Küchemann (1978) y sugieren revisar las interpretaciones de las letras como lo

son: *Letra evaluada, Letra no usada, Letra como objeto, Letra como incógnita, Letra como número generalizado y Letra como variable*. lo cual favorece los contextos algebraicos que requieren los estudiantes.

Es así, que el álgebra, entendida no como un lenguaje restringido a lo simbólico y orientada hacia la resolución de problemas que involucren diferentes situaciones, evitará que las con conceptos matemáticos que requieran de ecuaciones, polinomios, algoritmos, entre otros aparezcan de manera forzada en la educación media, sin continuidad con los temas de aritmética, medida y geometría estudiados en grados inferiores.

A modo de síntesis los diferentes autores, reiteran que las competencias algebraicas de carácter simbólico son el resultado de un proceso de maduración más general que se desarrolla a lo largo del tiempo, se justifica que su enseñanza se inicie desde la escuela primaria (Carpenter; Frankle; Levi, 2003), citados por Socas [43]. Esto con el fin de disminuir las dificultades que generalmente presentan en el aula de clase los estudiantes que no muestran continuidad y acercamiento a sus procesos algebraicos.

Es valioso rescatar que en Colombia cada día son más los maestros que se preocupan y cuestionan sobre sus practicas en el aula, dando posibilidad a la investigación y formación, validando las estructuras matemáticas como procesos que requieren de espacios de sistematización y aprendizaje graduales, que no es necesario llenar de teorías a los estudiantes sin un modelo que involucre el contexto social y participativo de los jóvenes.

### 5.3.1. Enseñanza de los Sistemas de Ecuaciones Lineales

Según los Lineamientos del Ministerio de Educación de Colombia, en el área de Matemáticas [11] de grado noveno los estudiantes deben tener las competencias necesarias para poder solucionar sistemas de ecuaciones lineales por diferentes métodos, esto en el aula generalmente se centra en enseñar y aprender memorísticamente los algoritmos de los métodos de sustitución, igualación, reducción, gráfico y en muy pocos casos el empleo de matrices y determinantes; estos procesos se limitan a ejercicios donde importa sólo la solución de un sistema sin un contexto que demarque esas letras con números.

En la enseñanza de los sistema de ecuaciones, describe M. Socas (1998) que:

*El tratamiento simbólico de las relaciones funcionales, el planteamiento y resolución de sistemas de ecuaciones suele ser el punto de llegada del álgebra escolar. Su manejo permite enfrentarse a una gama más amplia de situaciones, en contextos de todo tipo, relacionados con la vida cotidiana, con aplicaciones de las matemáticas a otros campos de conocimiento, o con el análisis y resolución de problemas planteados desde otras partes de las propias matemáticas. Pero, para que sea efectivo ese aumento en la capacidad de resolver problemas que proporcionan los sistemas, es preciso que el que los utiliza sepa qué es un sistema de ecuaciones y qué significa*



*su solución, así como que sea capaz de resolverlas con cierta garantía de éxito.*

Los sistemas de ecuaciones lineales se abordan con estudiantes de edades entre los 12 y 15 años, quienes evidencian en la mayoría de los casos dificultades con los conjuntos numéricos, especialmente el de los Números Enteros y Racionales, esto lleva a que el inicio de estas temáticas algebraicas sean para ellos sólo reglas que permiten encontrar una “solución”, obteniendo números sin sentido.

Esta concepción, como lo argumenta el grupo pretexto [35] de debe a que esas edades se tiene una mayor sensibilidad para captar cuestiones de carácter técnico que para comprender los problemas científicos. Las definiciones y las ideas no interesan en el mismo grado que los procedimientos y los automatismos. El «cómo se hace» prevalece sobre el «por qué se hace».

Cabe anotar, que también es importante que los estudiantes reconozcan la importancia de ejercitarse en estos procesos algebraicos, pues ellos permitiran llegar a la solución, así mismo, se requiere que tanto los maestros como los jóvenes se sensibilicen sobre las ventajas de este lenguaje matemático que debe ser enriquecido por situaciones problemas reales y actuales que contribuyen al avance de investigaciones tanto pedagógicas como científicas.

### 5.3.2. Obstáculos de Aprendizaje

La noción de obstáculo se puede constituir como la herramienta didáctica que permite explicar la existencia de errores y dificultades especiales, (Brousseau, 1983) define algunas características del obstáculo pero aquí se destacan: “Un obstáculo es un conocimiento, no una falta de conocimiento” y “El alumno no es consciente del obstáculo”.

Algunas dificultades experimentadas por los estudiantes se deben a una falta del conocimiento básico necesario para una comprensión correcta de un concepto o procedimiento dado. El propósito de la caracterización de concepciones y obstáculos es que ello permite delimitar los distintos componentes implicados en la comprensión de un concepto. Brousseau en sus investigaciones ha identificado tres tipos de obstáculos:

- **Obstáculos ontogénicos o psicogenéticos:** hacen referencia a las características del desarrollo del niño y cómo se evidencia los conocimientos contruidos a lo largo del proceso enseñanza aprendizaje.
- **Obstáculos didácticos:** se originan debido a las metodologías o modelos didácticos propios de su contexto y de quien lo orienta. Estos obstáculos deben identificarse a tiempo para evitar que los procesos inadecuados tengan demasiadas consecuencias.

- **Obstáculos epistemológicos:** Relacionados intimamente con el propio concepto, su naturaleza y conteniendo parte del significado del mismo.

En relación a la enseñanza del álgebra y como lo expone E. Castro (2012) [29] se pueden identificar estos obstáculos como se muestra en el siguiente diagrama.

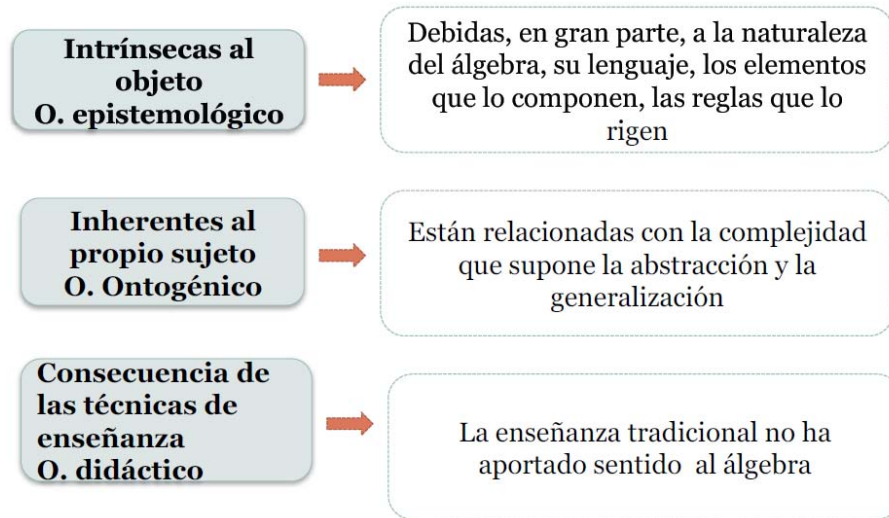


FIGURA 5.2. Tipos de Dificultades Algebraicas

En relación a los sistemas de ecuaciones lineales se podría identificar algunos de los siguientes obstáculos:

#### ***Epistemológicos:***

- Dificultades en la interpretación de la letra según investigaciones del grupo Pretexto [35]; Letra evaluada, Letra no usada, Letra como objeto, Letra como incógnita, Letra como número generalizado y Letra como variable.
- Poco manejo de las estructuras y conjuntos numéricos, especialmente de los Enteros y Racionales.
- Lenguaje básico para involucrar el lenguaje cotidiano con el lenguaje algebraico.

#### ***Ontogénicos:***

- Dificultad en el paso de situaciones particulares a su generalización.
- Escasa interpretación de las ecuaciones y su elementos.
- No identificar las fases de la generalización como los son: Ver: (la visión de la regularidad, la diferencia, la relación), Describir (su exposición verbal) y Escribir (su expresión escrita, de la manera más concisa posible); según (Masón y otros, 1985)

- Falta de abstracción en los conceptos concernientes a las ecuaciones lineales.

***Didácticos:***

- Explicaciones faltas de sentido y contextualización de los sistemas de ecuaciones lineales, sólo ejercicios con solución.
- La historia del surgimiento de las ecuaciones no hace parte de la rutina de aula.
- Las condiciones escolares y administrativas, como las sociales no permiten espacios ni políticas que favorezcan el aprendizaje de esta temática.
- Se continúa enseñanza las matemáticas del pasado, falta innovación en la aplicabilidad actual de los sistemas de ecuaciones y matrices.

## 5.4. La Criptografía en la Escuela

Año tras años se ha venido incrementando la investigación en el aula en relación al uso de la criptografía, especialmente en cursos iniciales universitarios, aunque algunos autores como P. Caballero y C. Bruno (2004) han dado paso a la posibilidad de iniciar estos conceptos en la educación media, así como el trabajo de F. Ibañez maestro colombiano quien realizó su investigación de maestría en este campo.

Se debe recordar y como lo expresa P. Caballero y C. Bruno [2] la criptografía es un pretexto excelente para orientar algunos conceptos matemáticos con los estudiantes mediante la resolución de problemas, pues esta ciencia posibilita la motivación del aprendizaje por su énfasis en descubrir lo secreto, en particular a este trabajo emplear métodos criptográficos contribuye al acceso de nuevos objetos matemáticos no tan cotidianos al currículo escolar.

Igualmente A. Rojas y A. Cano en su artículo “Motivando el aprendizaje del Álgebra Lineal a través de sus aplicaciones: la división de secretos” resaltan la importancia de motivar a los estudiantes realizando actividades académicas donde hagan uso de conceptos teóricos del Álgebra Lineal de una forma práctica, útil e interesante. Los autores diseñan actividades dedicadas a la división de secretos: allí un secreto no estará en manos de una sola persona sino que sólo cuando se junten un número determinado de personas se podrá recuperar completamente dicho secreto. Permitiendo no sólo el estudio de conceptos matemáticos sino contribuir a la sana convivencia entre los participantes.

El enriquecimiento del currículo escolar de matemáticas y el acercamiento a esta exclusiva aplicación de la aritmética modular como es la criptografía en el ámbito docente, puede realizarse a través de unidades didácticas sobre el tema y puede ser ampliado a proyectos institucionales donde se busque la interdisciplinariedad

Según J. Baena [37] la criptografía en la educación Media y su contextualización histórica conllevan a profundizar en situaciones sociales, económicas, científicas y de estrategias de guerra; que no son ajenas a las problemáticas actuales sensibilizando a los estudiantes sobre la importancia del conocimiento matemático.

Como lo describe P. Cabllero [2] en uno de sus artículos “Diseñar una clase de matemáticas a través de la criptografía tiene que responder a dos cuestiones principales: qué enseñar y cómo enseñarlo que posibiliten la profundización y el tipo de contenido (conceptual, procedimental o actitudinal) favoreciendo al aprendizaje de la matemáticas con un sentido actual y que responda al avance de la ciencia y tecnología de nuestros días”.

## CAPÍTULO 6

---

---

# PROPUESTA DIDÁCTICA

---

---

*Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber*

*Albert Einstein*

En el diseño y aplicación de la secuencia didáctica se propone que cada actividad brinde al estudiante las herramientas matemáticas necesarias, que integren los conceptos matriciales con el uso de la criptografía clásica, en la solución de sistemas ecuaciones lineales u otros objetos matemáticos. Así mismo a lo largo de la propuesta se busca enfatizar en algunos estándares propuestos por el Ministerio de Educación Nacional en los Lineamientos Curriculares de Matemáticas; con el propósito de elevar los niveles de exigencia y potenciar los diferentes pensamientos matemáticos en los estudiantes de grado noveno.

### ***ESTANDARES A FORTALECER***

#### ***Pensamiento Numérico y Sistemas Numéricos.***

- Utilizo números reales en sus diferentes representaciones y en diversos contextos.
- Resuelvo problemas y simplifico cálculos usando propiedades y relaciones de los números reales y de las relaciones y operaciones entre ellos.

#### ***Pensamiento Espacial y Sistemas Geométricos.***

- Uso representaciones geométricas para resolver y formular problemas en las matemáticas y en otras disciplinas.

*Pensamiento Variacional y Sistemas Algebraicos y Analíticos.*

- Construyo expresiones algebraicas equivalentes a una expresión algebraica dada.
- Identifico diferentes métodos para solucionar sistemas de ecuaciones lineales.

**ACTIVIDADES A DESARROLLAR****6.1. Actividad 0: El Escarabajo de Oro**

- ✓ **Objetivo:** Propiciar en los estudiantes de grado noveno una lectura comprensiva del cuento El Escarabajo de Oro de Edgar Allan Poe, con el fin de motivar el acercamiento a la solución de acertijos a través de algunas técnicas criptográficas o esteganográficas.
- ✓ **Conceptos Previos:** Elementos de la lectura comprensiva, tablas estadísticas de frecuencia.
- ✓ **Conceptos a Estudiar:** Criptografía, análisis de frecuencia para descifrar mensajes, algunas técnicas de esteganografía.
- ✓ **Metodología - Desarrollo de la Actividad**

Para esta actividad se requieren de 2 sesiones que contemplen la lectura del cuento, desarrollo de la guía, construcción de nuevos mensajes, socialización e institucionalización de los conceptos aprendidos.

1. Lectura individual del cuento.
2. Entrega de la guía de lectura con preguntas que enmarquen el inicio del estudio de la criptografía.
3. Socialización de la respuestas de la guía de lectura para aclarar algunos conceptos, especialmente el de criptografía.
4. Construcción de nuevos mensajes según el método empleado en el cuento.
5. Exposición de dibujos y mensajes creados por los estudiantes.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos.
- Realiza inferencias partir de tablas, que presenten información relativa a situaciones del mundo real.

- Elabora hipótesis de lectura del texto, a partir de la revisión de sus características en la lectura comprensiva.

### ✓ Evaluación

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

El desarrollo de esta actividad valora la construcción y desciframiento de nuevos mensajes por parte de los estudiantes, empleando principalmente el análisis de frecuencias.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
 PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA

Más de **60** Años **Formando**  
*Maestros y maestras para la infancia*



## EL ESCARABAJO DE ORO

*"... realmente dudo que la inteligencia humana pueda concebir un enigma que la inteligencia de otro humano no sea capaz de resolver"* **EDGAR ALLAN POE**

Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_

- ✠ En El Escarabajo de Oro, el personaje explica, cómo logró hallar el tesoro, descríbelo

---



---



---



---

- ✠ En la lectura se encuentra la palabra **criptografía**, ¿Qué significado tiene?

---



---

✠ ¿Qué relación existe con las matemáticas?

---



---



---

✠ Ahora, ¡descifra este mensaje!



;48(86)\*;46\*39; (86\*;8(8);6\*31;(4?95\*););018[?^^08)

✠ Realiza un dibujo de lo que más te gusto de la lectura.

✠ Una buena tinta invisible se puede hacer con jugo de limón, usas un palillo para mojarlo con jugo de limón y escribes sobre el papel blanco, cuando se seca, es totalmente invisible. Para que aparezca la escritura, con una vela a una altura prudente colócalo sobre el fuego.





## 6.2. *Actividad 1: Te Reto a Descifrarlo*

- ✓ **Objetivo:** Identificar las habilidades de los estudiantes en la solución de acertijos clásicos, donde se involucre el uso de los números en diferentes situaciones para retomar algunos conceptos matemáticos.
- ✓ **Conceptos Previos:** Estructura Aditiva, Criterios de Divisibilidad, Lenguaje cotidiano - Lenguaje algebraico.
- ✓ **Conceptos a Estudiar:** Divisibilidad, Números primos, Números perfectos, Criptoaritmética, introducción métodos clásicos de ciframiento.
- ✓ **Metodología - Desarrollo de la Actividad**

En la actividad se podrán conformar grupos de trabajo de cuatro o tres estudiantes, que posibiliten la comunicación de estrategias de solución para cada uno de los acertijos, así como, compartir conceptos matemáticos requeridos en la guía; finalizando o iniciando la siguiente sesión se socializan las soluciones encontradas para institucionalizar los conceptos aprendidos.

1. Conformación de grupos y entrega de la guía.
2. Socialización de las estrategias empleadas para solucionar los acertijos.
3. Propuesta de nuevos retos por parte de los estudiantes.
4. Cierre y síntesis del trabajo realizado.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos.
- Identifica los criterios de divisibilidad para solucionar un problema.
- Emplea el lenguaje algebraico para describir situaciones cotidianas.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.

- ✓ **Evaluación**

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

Sistematizar las estrategias empleadas por los estudiantes al enfrentarse a situaciones problema, así como la iniciativa en la creación de nuevos retos.



- ✠ Sustituye las letras por números del 0 al 9, para que ésta sea correcta. (misma letras, mismos número)

**CRITOSUMA** ECUACION + ECUACION = ACERTIJO

¿Cuál es la solución?

$$\begin{array}{r}
 \square\square\square\square\square\square\square \\
 + \square\square\square\square\square\square\square \\
 \hline
 \square\square\square\square\square\square\square
 \end{array}$$

- ✠ Y éste es el último

**DESCUBRE LA PALABRA**

○ ○ ○ ○ ○ ○ ○

- Ⓐ Las palabras VESTIR Y DECIME no tienen ninguna letra en común con nuestra palabra.
- Ⓑ La palabra CELOSA tiene 3 letras en común pero no están en el lugar correcto.
- Ⓒ La palabra GRANDE tiene 3 letras en común pero no están en el lugar correcto.
- Ⓓ La palabra ARRUYO tiene 3 letras en común y están en el lugar correcto.
- Ⓔ La palabra INGLES tiene 3 letras en común, 2 en el lugar correcto y la otra no.
- Ⓕ La palabra LOGICA tiene 4 letras en común y sólo una en el lugar correcto.



- Ⓖ En total tienen 2 docenas de dulces
- Ⓗ Cada niño tiene un número diferente de dulces y por lo menos tiene 2 dulces.
- Ⓙ El número de dulces de los dos niños más grandes es media docena.
- Ⓚ El número de dulces del niño del centro es el doble de los dulces del niño más grande.
- Ⓛ El niño más chico tiene la mitad de los dulces que tienen juntos los 3 niños que tiene al lado.

**¿Cuántos dulces tiene cada uno?**

- ✠ Puedes encontrar éstos y más retos en la siguiente dirección electrónica: <http://retomania.blogspot.com/2009/07/criptoaritmetica.html>, además si conoces otros acertijos compártelos con tus compañeros.

### 6.3. *Actividad 2: ¿Cuál será el Camino?*

- ✓ **Objetivo:** Encontrar patrones numéricos en el Triángulo de Pascal, que permita a los estudiantes aprender sobre los Números Poligonales y con ellos generar claves para solucionar acertijos.
- ✓ **Conceptos Previos:** Secuencias Numéricas, Patrones Numéricos y Geométricos, Triángulo de Pascal.
- ✓ **Conceptos a Estudiar:** Números Poligonales, Patrones Numéricos y Geométricos .
- ✓ **Metodología - Desarrollo de la Actividad**

En la actividad se podrán conformar grupos de trabajo de cuatro o tres estudiantes, que posibiliten la comunicación de estrategias de solución para cada uno de los acertijos, así como, compartir conceptos matemáticos requeridos en la guía; finalizando o iniciando la siguiente sesión se socializan las soluciones encontradas para institucionalizar los conceptos aprendidos.

1. Conformación de grupos y entrega de la guía.
2. Socialización de las estrategias empleadas para solucionar los acertijos.
3. Propuesta de nuevos retos por parte de los estudiantes.
4. Cierre y síntesis del trabajo realizado.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos.
- Reconoce y describe regularidades y patrones en distintos contextos
- Identifica los Números Poligonales con sus características.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.

- ✓ **Evaluación**

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

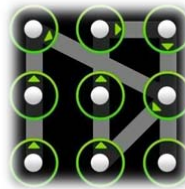
Sistematizar las estrategias empleadas por los estudiantes al enfrentarse a situaciones problema, así como la iniciativa en la creación de nuevos retos.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
**PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA**

Más de **60** años **Formando**  
Maestros y maestras para la infancia



## ¿CUÁL SERÁ EL CAMINO?



Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_



El celular de la profesora de matemáticas guarda todas las respuestas de los exámenes aplicados a los estudiantes de grado noveno, sin embargo, este celular tiene algunas claves en particular que sólo responden a curiosidades matemáticas.

Es así, que la profesora decide un día antes proporcionar las respuestas del examen final de periodo, a quien descubra cómo desbloquear su celular, las claves varían a medida que se van descubriendo las anteriores. El examen consta de 5 preguntas por lo tanto deberán descifrar el mismo número de claves.

Para obtener la primera respuesta deberás deslizar tus dedos de tal manera que al contar el número de círculos la clave que obtengas sea:

**1, 3, 6, 10, 15, 21**

✓ Si se pudiera extender la pantalla del celular ¿Cuáles serían los siguientes cinco números de la clave?

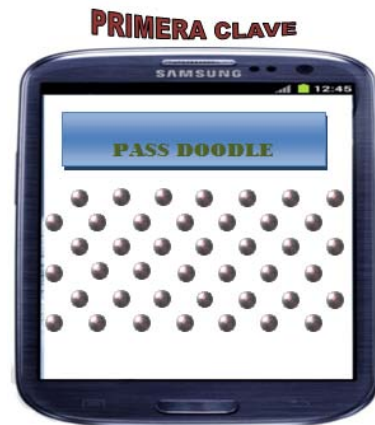
1   3   6   10   15   21                                                       

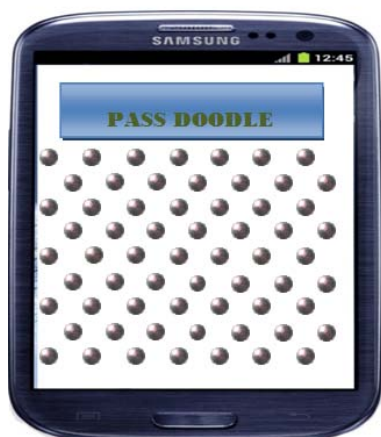
✓ Explica brevemente cómo descifraste el recorrido

---

---

---



**SEGUNDA CLAVE**

Para esta clave se tiene la siguiente secuencia

**1, 4, 9, 16, 25, 36**

De la misma manera se deben contar el número de círculos para encontrar la secuencia.

✓ ¿Qué forma tiene el desplazamiento para la segunda clave y para la primera?

---

✓ ¿Qué nombre le pondrías a cada una de las claves?

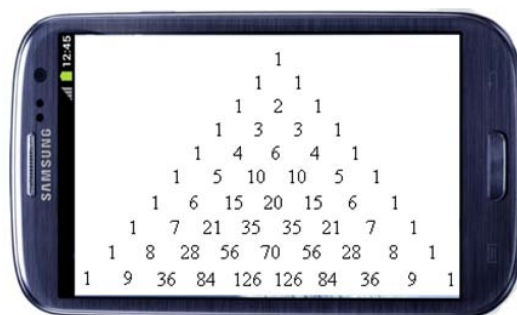
---

Al desbloquear el celular con la segunda clave, aparece en la pantalla una imagen muy famosa.

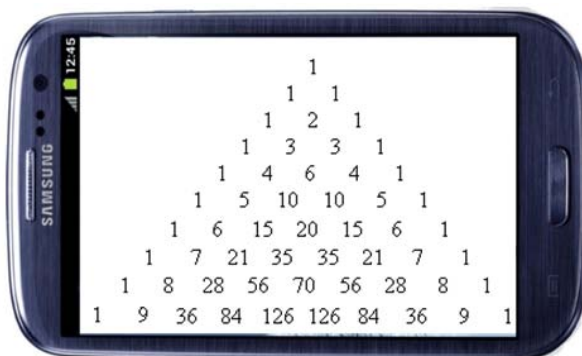
✓ ¿Cuál es el nombre que recibe esta imagen?

---

✓ En el triángulo se encuentra la primera clave, Señálala, ¿Cómo podrías obtener ésta columna, realizando desplazamientos en el triángulo? Tráza los

**TERCERA CLAVE**

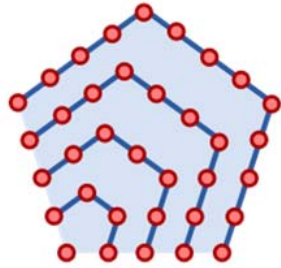
✓ Así mismo, empleando el triángulo, ¿Qué movimientos tendrías que hacer para hallar la segunda clave? Tráza los





**CUARTA CLAVE**

Existen unos números muy particulares que se obtienen de un arreglo geométrico como el siguiente:



1, 5, 12, 22, 35, ...

✓ ¿Qué nombre le asignarías a estos números? \_\_\_\_\_

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

✓ Descubre 2 maneras de desplazarte en el Triángulo de Pascal, para poder obtener estos entretenidos números. Luego, describe cómo lo hiciste

---



---



---

**QUINTA CLAVE**

N VIC SI LOEN ODBC OTEO UN EX X

Finalmente la profesora dejó escrito el anterior mensaje

*PISTA: CRIPTOGRAFÍA POR TRANSPOSICIÓN GEOMÉTRICA*



### 6.4. *Actividad 3: Ocultando Mensajes*

- ✓ **Objetivo:** Introducir a los estudiantes a algunos conceptos de criptografía, empleando los métodos Afín y de Vigère con el fin de motivar el aprendizaje de las congruencias.
- ✓ **Conceptos Previos:** Estructura Aditiva, Estructura Multiplicativa, Conjunto Numérico de los Enteros, Criterios de Divisibilidad.
- ✓ **Conceptos a Estudiar:** Divisibilidad, Congruencias, Método criptográfico Afín y Método de Vigenère,

#### ✓ **Metodología - Desarrollo de la Actividad**

Para el desarrollo de esta guía, llevará de 3 a 4 sesiones. Comenzará con una presentación formal de los conceptos necesarios para llevar a cabo el ciframiento y desciframiento de los mensajes según los métodos a emplear.

1. Establecer de manera individual los procesos o técnicas de cada método a estudiar.
2. Construcción de mensajes cifrados, dadas las indicaciones de las técnicas a usar.
3. Conformación de grupos para la elaboración de nuevos mensajes, los cuales serán descifrados por los demás compañeros.
4. Cierre y síntesis del trabajo realizado.

#### ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos.
- Identifica los criterios de divisibilidad para solucionar un problema.
- Emplea el lenguaje algebraico para describir situaciones cotidianas.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.



### ✓ Evaluación

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

En esta actividad se reconocerá principalmente la construcción de mensajes a partir de los métodos estudiados y la habilidad para cifrarlos y descifrarlos aplicando los conceptos matemáticos requeridos.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
 PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA

Más de **60** años **Formando**  
 Maestros y maestras para la infancia



Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_

A continuación encontrarás algunas indicaciones que servirán para cifrar mensajes, al estilo de un método clásico denominado Afín.

1. Seleccionar el texto en claro, es decir, un mensaje normal.
2. Se elabora un alfabeto al cual se le hace coincidir un valor numérico
3. El paso a seguir es adjudicar a cada letra del mensaje original su correspondiente con el alfabeto elaborado en el paso anterior.
4. Se asigna un clave para realizar una transformación del método Afín, la clave debe ser  $e_k(x) = ax + b \pmod{27}$
5. Finalmente se obtiene el mensaje.

Observa el ejemplo:

1. Mensaje en claro

*LAS MATEMATICAS SON SENCILLAS*

2. Alfabeto a emplear

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

3. Mensaje con el alfabeto anterior

L	A	S	M	A	T	E	M	A	T	I	C	A	S
11	0	19	12	0	20	4	12	0	20	8	2	0	19

S	O	N	S	E	N	C	I	L	L	A	S
19	15	13	19	4	13	2	8	11	11	0	19

Con el que se obtiene el texto con los siguientes números

11 0 19 12 0 20 4 12 0 20 8 2 0 19 19 15 13 19 4 13 2 8 11 11 0 19.

4. Se aplica una clave afín de la forma  $(7, 2)$ , es decir, una transformación  $7x + 2$ , para ello a cada número de la sucesión anterior se multiplica por 7 mód 27 y se adiciona 2 obteniendo la sucesión

25 2 0 5 2 7 3 5 2 7 4 16 2 0 0 26 12 0 3 12 16 4 25 25 2 0 .

5. Por lo que YCAFCHDFCHEPCAAMADMPEYYCA es el correspondiente texto cifrado.

**AHORA ES TU TURNO**

## CIFRA EL SIGUIENTE MENSAJE

ESTE MENSAJE SE AUTODESTRUIRA


Aplica la clave  $(5, 3)$  es decir la transformación  $5x + 3$

***EL TEXTO CIFRADO ES:***

Ahora, conozcamos otra forma de cifrar mensajes desarrollada por un criptógrafo francés llamado Vigenère. Sigue las indicaciones y el ejemplo!

1. Seleccionas una palabra clave para cifrar el mensaje.
2. Conviertes el mensaje y la palabra clave en dos sucesiones de números.
3. Debes sumar las dos sucesiones, recordando que son congruentes módulo 27
4. Finalmente se tiene el mensaje cifrado.

1. Se elige la palabra clave ***carmen***, para cifrar el mensaje

todosobtendrancincoenmaticas

2. y 3. Se convierte el texto en claro y la clave en dos sucesiones de números, con lo que se tiene

*texto:* 20 15 3 15 19 15 1 20 4 13 3 18 0 13 2 8 13 2 15 4 13 12 0 20 4 12 0 20 8 2 0 19

*clave:* 2 0 18 12 4 13

4. Se obtiene

VOUAWBDTVYHECNTTQOQEEXEGGMOCS como el texto cifrado

Con el anterior ejemplo, Cifra dos mensajes y compártelos con tus compañeros

A	20	15	3	15	19	15	1	20	4	13	3	18	0	13	2	8
B	2	0	18	12	4	13	2	0	18	12	4	13	2	0	18	12
$A + B \equiv \text{mód } 27$	22	15	21	0	23	1	3	20	22	25	7	4	2	13	20	20

A	13	2	15	4	13	12	0	20	4	12	0	20	8	2	0	19
B	4	13	2	0	18	12	4	13	2	0	18	12	4	13	2	0
$A + B \equiv \text{mód } 27$	17	15	17	4	4	24	4	6	6	12	18	5	12	15	2	19



1. Escribe un mensaje

---



---

2. Selecciona una clave máximo de 6 letras

---

3. Empleando tablas como las del ejemplo, organiza las sucesiones numéricas y súmalas recordando el concepto de congruencia.

## Y AHORA ... ¿CÓMO SE PUEDE DESCIFRAR MENSAJES CON ESTE MÉTODO?



Es muy sencillo si se conoce la clave, lo único que debes hacer es restar del mensaje cifrado la clave y se obtendrás el texto en claro.

✓ Descifra el mensaje **RSRIBWEOFZQIXNIEV**, el cual fue encriptado usando la clave **FELIZ**

## 6.5. *Actividad 4: Matriz Recargado*

- ✓ **Objetivo:** Estudiar la aritmética de matrices a través del método de Hill, para que los estudiantes contruyan mensajes cifrados y fortalezcan el trabajo colaborativo descifrando mensajes.
- ✓ **Conceptos Previos:** Estructura Aditiva, Estructura multiplicativa de Números Enteros, Congruencias.
- ✓ **Conceptos a Estudiar:** Matriz, producto de matrices, inversa de una matriz, congruencias.
- ✓ **Metodología - Desarrollo de la Actividad**

Esta actividad requiere de una estudio previo de algunos procesos de la aritmética de matrices desde una mirada formal, pero que atraiga la atención de los estudiantes.

1. Conformación de grupos y entrega de la actividad.
2. Desarrollar la actividad según las indicaciones de la misma.
3. Intercambio de mensajes entra los grupos para descifrarlos en equipos de trabajo.
4. Cierre y síntesis del trabajo realizado.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos.
- Emplea las operaciones entre matrices en un contexto criptográfico
- Identifica cuando una matriz tiene inversa.
- Calcula el determinante y adjunta de una matriz.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.

- ✓ **Evaluación**

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

Un estudiante avanzará en su proceso, si demuestra la habilidad para cifrar y descifrar mensajes a través del método de Hill y el uso de la aritmética de matrices.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
 PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA

Más de **60** años **Formando**  
 Maestros y maestras para la infancia



Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_

SIGUIENDO  
 LOS PASOS



¡ESCRIBE MENSAJES SECRETOS!

Regla	Indicaciones
1	Asignar un valor numérico a cada letra del alfabeto a utilizar iniciando en cero
2	La clave a utilizar debe constar de 4 para formar una matriz 2x2
3	El Mensaje se divide en grupos de 2 letras para ser puestas en matrices de 2x1 y se hacen corresponder con sus equivalente numéricos



¡INICIEMOS!

## 1. Alfabeto

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

2. Clave 

--	--	--	--

 $C = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

## 3. Mensaje

## CRIPTOGRAFÍA

<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>					<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>					<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>					<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>					<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>					<table><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>				
$M_1$	$M_2$	$M_3$	$M_4$	$M_5$	$M_6$																								

## 4. Escribe las matrices

$M_1 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

$M_2 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

$M_3 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

$M_4 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

$M_5 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

$M_6 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$

¿Y ahora qué hacemos?... muy fácil multiplica la clave por cada una de las matrices.

$$C \cdot M_1 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$$

$$C \cdot M_2 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$$

$$C \cdot M_3 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$$

$$C \cdot M_4 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$$

$$C \cdot M_5 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix}$$

Ahora que ya sabes cómo ocultar un mensaje. ¿Qué debes hacer para descifrarlo?



Regla	Indicaciones
1	Calculamos la matriz inversa de C
2	Del mensaje cifrado tomamos grupos de 2 letras y hacemos equivalente con los números del alfabeto.
3	Realizamos el producto de la inversa de C con cada uno de los grupos obtenidos en el paso 2.
4	Los resultados obtenidos corresponden al texto original

## MANOS A LA OBRA

Recuerda que para calcular la inversa de una matriz  $2 \times 2$  puedes emplear:

$$C^{-1} = \frac{1}{\det C} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

$$C^{-1} \cdot N_1 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

$$C^{-1} \cdot N_2 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

$$C^{-1} \cdot N_3 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

$$C^{-1} \cdot N_4 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

$$C^{-1} \cdot N_5 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

$$C^{-1} \cdot N_6 = \begin{pmatrix} \square & \square \\ \square & \square \end{pmatrix} \cdot \begin{pmatrix} \square & \square \end{pmatrix} = \begin{pmatrix} \square \\ \square \end{pmatrix} \text{mód } 27 = \begin{pmatrix} \square \\ \square \end{pmatrix}$$

FINALMENTE, QUE YA IDENTIFICASTE Y CONOCES ESTE SISTEMA DENOMINADO HILL POR SU CREADOR LESTER HILL EN 1929; CONSTRUYE NUEVOS MENSAJES Y ENVÍALOS A LOS DEMÁS GRUPOS. GANA EL EQUIPO QUE PRIMERO LOS ENVÍE Y DESCIFRE





## 6.6. *Actividad 5: Compartiendo Secretos*

- ✓ **Objetivo:** Fortalecer el trabajo cooperativo y las competencias ciudadanas, mediante la aplicación del método de Shamir, que lleven a los estudiantes a solucionar sistemas de ecuaciones lineales.
- ✓ **Conceptos Previos:** Estructura aditiva, Estructura multiplicativa de Números Enteros y Racionales, polinomios algebraicos, ecuaciones lineales, lenguaje algebraico.
- ✓ **Conceptos a Estudiar:** Polinomios, Sistemas de Ecuaciones, determinante de Vandermonde.
- ✓ **Metodología - Desarrollo de la Actividad**

Para esta actividad es necesario la conformación de grupos donde exista o se fortalezca la confianza y seguridad, además que se establezcan alianzas como acuerdos que permitan lograr el objetivo de encontrar el mensaje.

Por otro lado, se debe haber realizado un ejemplo previo en relación a la interpolación de polinomios y cálculo del determinante Vandermonde.

1. Conformación de los grupos y repartición del secreto.
2. Aplicación del esquema shamir.
3. Reunión de los integrantes para conocer el mensaje oculto.
4. Cierre y síntesis del trabajo realizado.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos. a
- Resuelve problemas y simplifico cálculos usando propiedades y relaciones de los números reales y de las relaciones y operaciones entre ellos.
- Identifica diferentes métodos para solucionar sistemas de ecuaciones lineales.
- Identifica el proceso para calcular el determinante de Vandermonde.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.

- ✓ **Evaluación**

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

Sensibilizar a los estudiantes sobre la importancia de las competencias ciudadanas, vistas como componente esencial para lograr un objetivo en común.

Desarrollar habilidades en la solución de sistemas de ecuaciones e identificación de las propiedades de los determinantes.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA

Más de **60** Años **Formando**  
Maestros y maestras para la infancia



Nombres (grupo): \_\_\_\_\_ Curso: \_\_\_\_\_

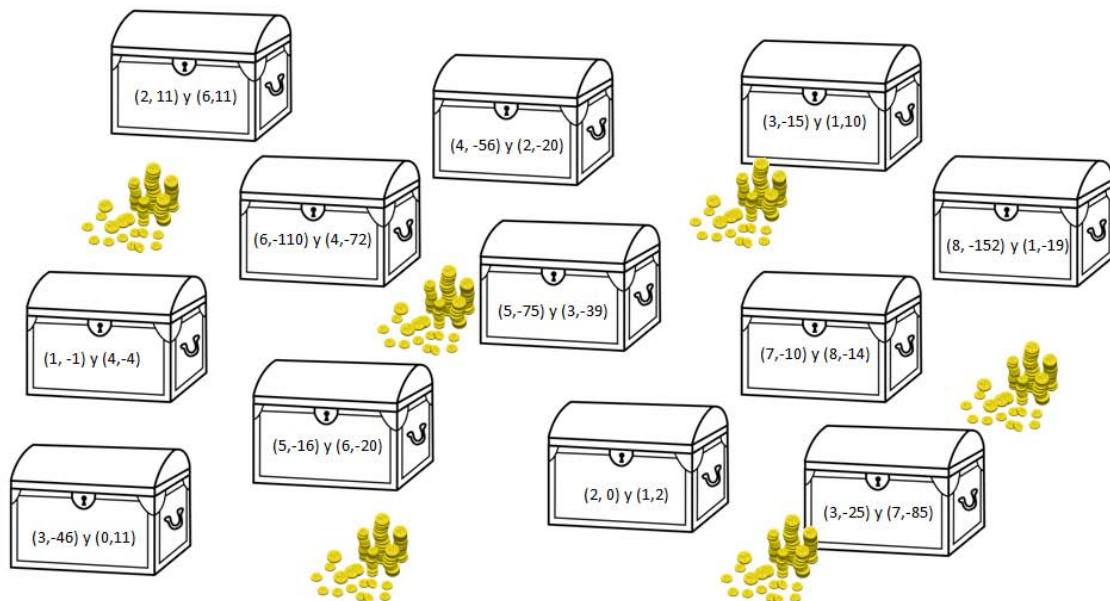


## COMPARTIENDO SECRETOS

COMPARTIENDO SECRETOS



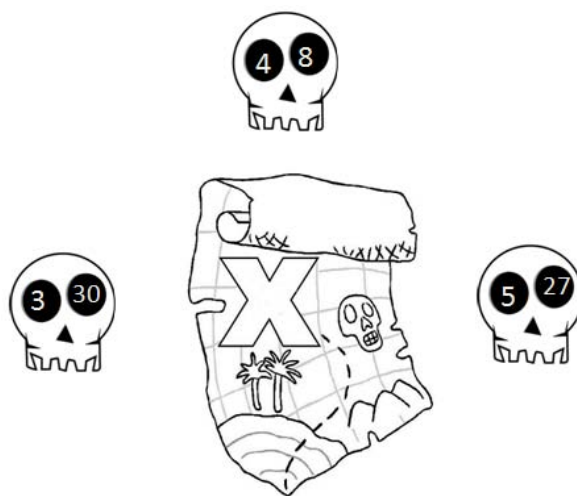
✠ La profesora de Matemáticas para la última clase de Álgebra decide eximir del examen final al grupo de estudiantes que primero logre reunir las partes del secreto que se presenta a continuación.



Debes tener presente las siguientes indicaciones

1. Conformar grupos de 2 estudiantes.

2. Organizar la pista asignada en un sistema de ecuaciones para encontrar parte del secreto.
  3. Proponer una estrategia para reunir todas las partes del secreto.
- ✠ Si eres uno de los grupo que descubrió el mensaje, obtendrás un bono extra en clase de matemáticas si descifras el siguiente enigma.



Puedes emplear el siguiente polinomio y el Determinante de Vandermonde

$$P(x) = s + s_1x + s_2x^2$$

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (b-a)(c-a)(c-b)$$

**buena suerte**

## 6.7. *Actividad 6: DESCUBRE EL ENIGMA*

- ✓ **Objetivo:** Institucionalizar los conceptos aprendidos por los estudiantes de grado noveno durante el desarrollo de la propuesta didáctica, permitiendo la sistematización y análisis de la misma.
- ✓ **Conceptos Previos:** Estructura aditiva, Estructura multiplicativa de Números Enteros y Racionales, aritmética de matrices, determinantes, polinomios algebraicos, ecuaciones lineales, lenguaje algebraico.
- ✓ **Conceptos a Estudiar:** Retomar algunos de los métodos criptográficos desarrollados en la propuesta especialmente método de Hill y esquema Shamir, enfocados hacia la aritmética de matrices y sistemas de ecuaciones lineales.
- ✓ **Metodología - Desarrollo de la Actividad**

1. Asignación de pistas.
2. Trabajo individual y/o grupal para identificar habilidades y dificultades.
3. Aplicación de sistemas criptográficos.
4. Cierre y síntesis del trabajo realizado.

- ✓ **Indicadores**

- Reconoce y usa los números en diferentes contextos. a
- Resuelve problemas y simplifico cálculos usando propiedades y relaciones de los números reales y de las relaciones y operaciones entre ellos.
- Identifica diferentes métodos para solucionar sistemas de ecuaciones lineales.
- Estable distintas estrategias para cifrar mensajes o hallar la solución de mensajes cifrados.
- Promueve en sus compañeros la formulación de preguntas que movilicen la comprensión de los conceptos matemáticos abordados.

- ✓ **Evaluación**

La evaluación en cada una de las actividades será vista como el proceso que facilita la identificación y análisis del estado del aprendizaje de los estudiantes, por ello será continua (seguimiento permanente), sistemática (organizada según los objetivos de la propuesta), interpretativa (da sentido a los resultados y procesos) y formativa (orienta para el mejoramiento).

Aplicación y propuesta de nuevos retos o problemas, por parte de los estudiantes evidenciando los aprendizajes logrados a lo largo de la propuesta, teniendo en cuenta la criptografía como recurso didáctico para acceder al conocimiento matemático o de otras disciplinas.

SECRETARÍA DE EDUCACIÓN DE BOGOTÁ D. C.  
**ESCUELA NORMAL SUPERIOR DISTRITAL MARÍA MONTESSORI**  
 PREESCOLAR, BÁSICA, MEDIA Y FORMACIÓN COMPLEMENTARIA

Más de **60** años **Formando**  
 Maestros y maestras para la infancia



Nombre: \_\_\_\_\_ Curso: \_\_\_\_\_



### ESTIMADO ESTUDIANTE

Para desarrollar la actividad deberás seguir las siguientes indicaciones:

- ✦ Con las pistas asignadas podrás encontrar los lugares del colegio donde recibirás el mensaje o enigma.
- ✦ Si requires de trabajo en equipo, establece alianzas y estrategias para poder encontrar la solución.
- ✦ Recuerda que el trabajo honesto conlleva a buenos aprendizajes y resultados.
- ✦ El primer estudiante o equipo obtendrá el premio mayor.

### *Pista No.1.*

EN ESTE LUGAR SIEMPRE SE APRENDE A TRAVÉS DE JUEGO Y SÓLO SE ESCUCHAN VOCES DE FELICIDAD

88	7	150	13	4	0	1	8	9	100	45	33	10
1	4	1	9	2	16	5	71	14	89	42	115	132
47	1	24	11	4	1	32	44	4	2	11	91	22
28	46	2	85	6	9	107	93	34	18	7	34	78
2	4	23	5	120	34	67	89	27	68	10	22	56
78	24	144	13	14	1	7	8	13	64	19	3	11
8	13	45	2	6	42	8	15	135	28	16	13	6
4	56	78	100	4	2	132	13	10	1	7	8	9
33	8	55	23	1	55	48	3	22	98	21	20	4

⇒ **1**



2  
↑

ENCUENTRA UNA SECUENCIA  
 NUMÉRICA DE MUCHO INTERÉS EN LA  
 TABLA No. 1, LUEGO RECÓRTALA Y  
 SUPERPÓNLA EN LA TABLA No. 2.  
 ENCONTRARÁS UN MENSAJE OCULTO



A	H	G	G	2	D	B	4	B	Ñ	L	M	B
N	Z	O	P	S	O	V	J	E	Z	M	X	O
Q	S	W	F	I	7	Y	S	B	J	Z	B	K
4	D	A	H	5	X	G	N	Z	A	D	Ñ	V
R	Z	Q	L	2	E	H	N	O	T	V	6	S
X	F	B	T	A	N	M	U	G	H	8	F	Z
F	C	Q	S	U	S	L	P	E	W	Y	W	E
G	C	H	G	K	O	3	D	K	S	Q	S	W
J	P	V	K	W	S	Ñ	R	L	I	H	A	Ñ

***Pista No.2.***

CUANDO NO ERES PUNTUAL AL INICIAR LA JORNADA ESCOLAR,  
ALLÍ DEBES ESPERAR

***Descubre!***

Descifra el siguiente mensaje sabiendo que se ha empleado el criptosistema de César con un desplazamiento de C cinco lugares:

“PFKPTYFXZGQFWNRFJXYFJRQFWIJPHTWFP”.

***Pista No.3.***

EN ESTE ESPACIO PUEDES UBICAR A LAS PERSONAS QUE HAN  
DIRIGIDO A LA ESCUELA LOS ÚLTIMOS 50 AÑOS

***Encripta!***

Empleando la siguiente transformación  $5x + 2$  cifra el mensaje:

NO HABRA CLASE MAÑANA

***Pista No.4.***

SÓLO ALLÍ SE ENCUENTRA EL SILENCIO Y TRANQUILIDAD PARA  
IMAGINAR, RECREAR Y TRANSPORTARSE A LUGARES E HISTORIA  
INOLVIDABLES.

***Cifra y descifra***

Con la ayuda de la aritmética de matrices y empleando la clave **AZUL**, cifra el mensaje

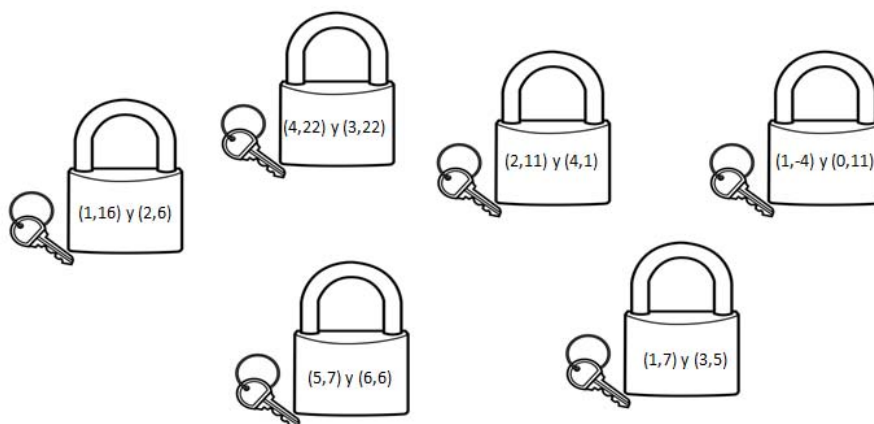
ACERTIJO

Luego crea otro mensaje, cífralo y envíalo a otro grupo o compañero.

***Pista No.5.***

ES EL LUGAR MÁS VISITADO POR EL GRUPO AMBIENTAL

Escribe los sistemas de ecuaciones lineales  $2 \times 2$  necesarios para descifrar el mensaje



## CAPÍTULO 7

---

# APLICACIÓN Y ANÁLISIS DE RESULTADOS

---

La propuesta se desarrollará en La Escuela Normal Superior Distrital María Montessori, institución formadora de maestros, la cual atiende una población de 3.350 estudiantes, entre niños y niñas provenientes de diferentes localidades especialmente de Antonio Nariño, Barrios Unidos, San Cristóbal, Ciudad Bolívar, Rafael Uribe Uribe, Kennedy y Santa Fe.

La secuencia fue orientada a estudiantes de grado Noveno durante el segundo semestre del año 2013 la institución contó con 6 grupos de 40 estudiantes aproximadamente en cada uno de ellos; la gran mayoría de ésta población cuenta con hogares conformados por padre y madre con condiciones económicas favorables, su estrato socioeconómico se ubica principalmente en estrato 3 representado en un 48,8 %; estrato 2 el 30,4 %; se cuenta con familias en estrato 1 con un 1,8 %; el 0,6 % en estrato 4 y en estrato 5 el 0,3 % según el informe de caracterización realizado por el comité de convivencia de la Escuela.

Estos datos se pueden corroborar con el reporte entregado por el ICFES para describir a la Escuela Normal



Establecimiento educativo: ESC. NORMAL SUPERIOR DISTRITAL MARIA  
Código DANE: 111001011908  
Fecha de actualización de datos: viernes 16 de agosto 2013

Ficha técnica de evaluados

Establecimiento	ESC. NORMAL SUPERIOR DISTRITAL MARIA
Código DANE	111001011908
Dirección	CL 14 SUR 14 36
Municipio -	Bogotá, D.C.-Bogotá, D.C.
Sector	Oficial
Zona	Urbana
Nivel socioeconómico	4

Ficha técnica de evaluados\* de noveno grado:

TABLA 7.1. Ficha Técnica ICFES



Históricamente una de las áreas que ha presentado mayor dificultad en su enseñanza-aprendizaje, es el área de matemáticas, convirtiéndose en un fenómeno social que afecta nuestro sistema educativo, y para el caso la Escuela Normal; los factores asociados a estos altos índices de reprobación en matemáticas; inician desde el núcleo familiar pues son quienes orientan las pautas iniciales en los hábitos de estudios, en la lectura comprensiva diaria, organización de tiempo, la influencia que hoy en día tienen las tic, las dinámicas escolares, el sistema de evaluación que en ocasiones no favorece un seguimiento para los estudiantes con dificultad en el área, igualmente las metodologías de algunos docentes no demuestran las aplicaciones para la vida que las matemáticas tiene y es normal que muchos estudiantes reprueben por creer que el área es exclusiva para algunas personas con ciertas aptitudes.

Anualmente en la Escuela Normal se lleva a cabo el plan de mejoramiento a la luz de las pruebas institucionales y externas que visualicen qué estrategias implementar para elevar los niveles de exigencia y calidad en la formación de maestros para la infancia, en particular se focaliza en matemáticas por presentar los más altos índices de reprobación.

Frente a las pruebas externa, el ICFES reportó los siguientes niveles de desempeño que evidencian las dificultades y habilidades de los estudiantes de la institución en el área de matemáticas.

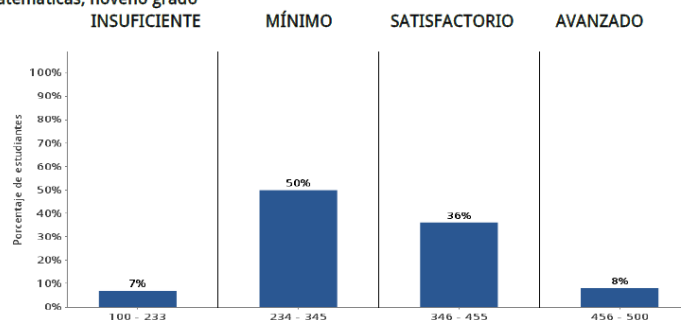
Establecimiento educativo: ESC. NORMAL SUPERIOR DISTRITAL MARIA

Código DANE: 111001011908

Fecha de actualización de datos: viernes 16 de agosto 2013

#### Resultados de noveno grado en el área de matemáticas

##### 1 Distribución porcentual de los estudiantes según niveles de desempeño en matemáticas, noveno grado



#### Resultados de noveno grado en el área de matemáticas

en el área y grado, su establecimiento es, relativamente:

- Fuerte en Razonamiento y argumentación
- Fuerte en Comunicación, representación y modelación
- Débil en Planteamiento y resolución de problemas

FIGURA 7.1. Desempeño estudiantes grado Noveno según Prueba Saber 2012

Dada esta situación se busca privilegiar la resolución de problemas y la aplicación de conceptos a la realidad de los estudiantes para que sea más visible su utilidad e importancia en su formación; es por ello que la secuencia didáctica diseñada para los jóvenes de grado noveno involucró la pregunta orientadora sobre ¿Qué tipos de problemas desarrollan el pensamiento algebraico de los educandos para que atraigan su atención y motivación?. Con ese fin se empleó la criptografía como un recurso que favorece la adquisición de algunos conceptos matemáticos a través de problemas y trabajo colaborativo en especial para la enseñanza de la aritmética de matrices y solución de sistemas de ecuaciones lineales.

Este trabajo se desarrolló con dos grupos de 40 estudiantes cada uno, de noveno grado; el **grupo experimental** con quien se implementó la propuesta didáctica y el **grupo control** donde no se aplicó las actividades de criptografía y se mantuvo una enseñanza tradicional de las temáticas para las matrices y sistemas de ecuaciones.

La implementación y evaluación de la propuesta se llevó a cabo con una metodología cuantitativa, para verificar la validez de la hipótesis sobre el uso de la criptografía como pretexto para el aprendizaje de estructuras matemáticas acordes al grado y el mejoramiento en los resultados de aprobación del área.

Se inició con una encuesta que identificaba algunas de las disposiciones de los estudiantes frente al área de matemáticas; se puede consultar las preguntas y resultados en [30]. A continuación se muestran los resultados de alguna de ellas.

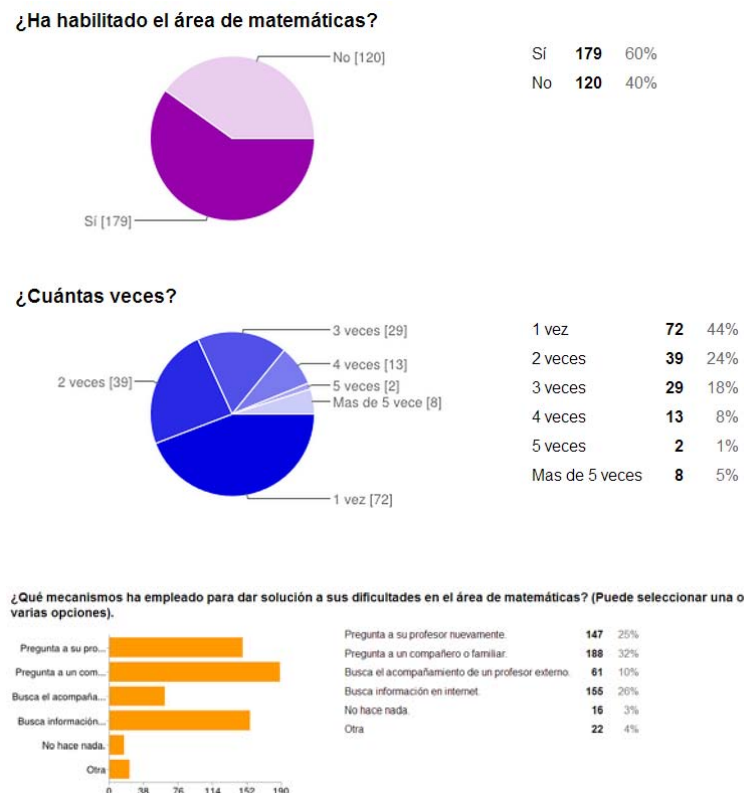


FIGURA 7.2. Resultados Encuesta

Así mismo las respuestas más frecuentes en la pregunta de ¿Cuáles han sido las dificultades que se les ha presentado en el área de matemáticas?, los estudiantes expresan sobre su falta de hábitos de estudio, poca dedicación de estudio extracurricular, dificultad en los números enteros, la solución de problemas y lo molesto que es aprenderse procesos de memoria.

Para la aplicación de la propuesta se focalizó a los grupos según los desempeños para el segundo periodo académico según la escala valorativa de evaluación en la Escuela Normal, que se presenta a continuación

Desempeño	Rango
Superior	$4.5 \leq x \leq 5.0$
Alto	$4.0 \leq x < 4.5$
Básico	$3.0 \leq x < 4.0$
Bajo	$1.0 \leq x < 3.0$

TABLA 7.2. Escala de Valoración ENSDMM

Los resultados obtenidos por los grupos para el periodo mencionado se muestran en la Fig. 7.3. en el cual se identifica que más del 50 % de los estudiantes no cumple con los requerimientos básicos para aprobar el área y sólo uno de ellos acredita desempeños superiores.

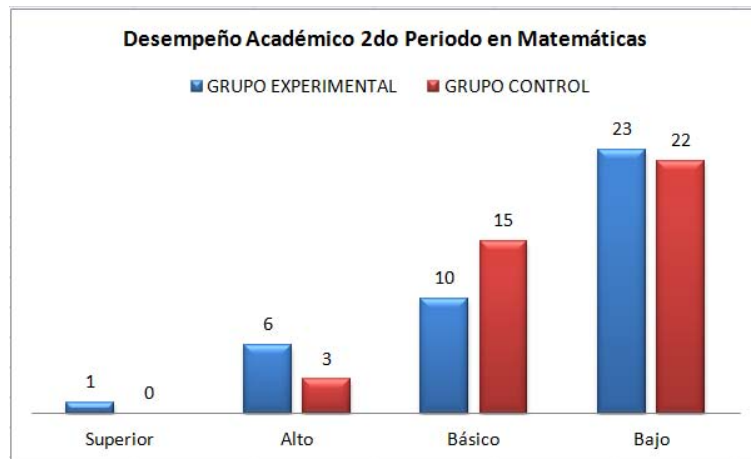


FIGURA 7.3. Desempeño de los estudiantes del Grupo control y Experimental

Frente a la aplicación de la propuesta didáctica se valoraron las diferentes instancias y procesos teniendo en cuenta los objetivos e indicadores diseñados en las actividades; a medida que se avanzó en el tiempo los demás grupos donde no se había

proyectado desarrollar las actividades sugirieron la equidad de los grupos y poder aprender lo que era novedoso para ellos.

Dada la situación presentada y la exigencia de los estudiantes, se puede decir que el 80 % de los estudiantes de grado noveno, es decir, 5 grupos tuvo la oportunidad de conocer y aprender sobre criptografía y su utilidad en el aprendizaje de algunos conceptos matemáticos no tan familiares para ellos.

Culminado el proceso y manteniendo mayor énfasis en los dos primeros grupos seleccionados, al finalizar el año 2013, los desempeños logrados fueron:

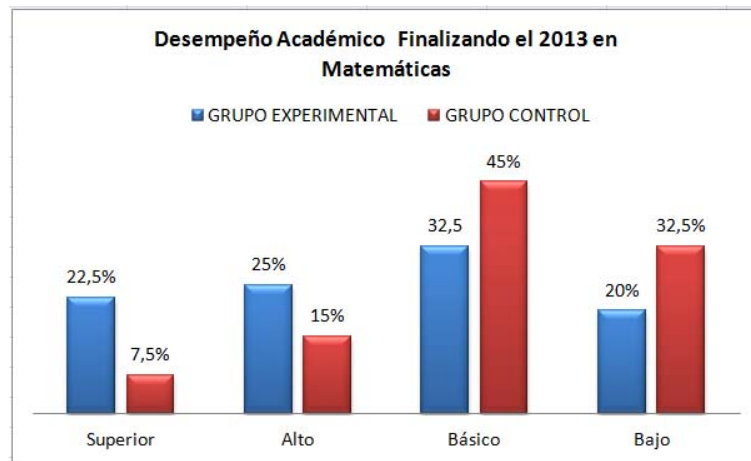


FIGURA 7.4. Desempeño de los estudiantes del Grupo control y Experimental Finalizado el 2013

Los resultados que se identifican de la información presentada en la Fig. 7.4., comparando los dos grupos, muestra que existe mayor apropiación por parte del grupo experimental de las temáticas propuestas en las actividades como lo fueron la aritmética de matrices y la solución de sistemas de ecuaciones; con un porcentaje de 22,5 % en superior y un 25 % en Alto comparado con un 7,5 % Superior y 15 % Alto del grupo control. La tendencia para el desempeño básico, mostró dismución tanto en el grupo control y experimental teniendo como referencia la Fig. 7.3. lo que sugiere que los estudiantes a los que no se les plaicó la propuesta, obtuvieron menor dominio del tema solución de sistemas de ecuaciones lineales.

Asi mismo, a nivel convivencial el trabajo con algunos sistemas critográficos favoreció la sana convivencia y la posibilidad de encontrar en el otro habilidades que no sobresalen en la cotidianidad escolar, igualmente la criptografía como agente motivador conllevó a la investigación por parte de los estudiantes pues requerian conocer más sobre esta ciencia para idear nuevas “técnicas” para mantener segura su información.

También es de rescatar que teniendo como referencia la prueba externa aplicada por el ICFES en el 2013 y según el informe presentado por ellos, el cual se muestra en la Fig. 7.5; que un 53 % de los estudiantes del grado noveno superó el nivel mínimo. Dadas las preguntas allí formuladas un estudiante promedio del nivel satisfactorio

utiliza las propiedades de la potenciación, radicación y/o logaritmación para solucionar un problema, utiliza expresiones algebraicas y representaciones gráficas para modelar situaciones sencillas de variación, entre otros.



MinEducación  
Ministerio de Educación Nacional

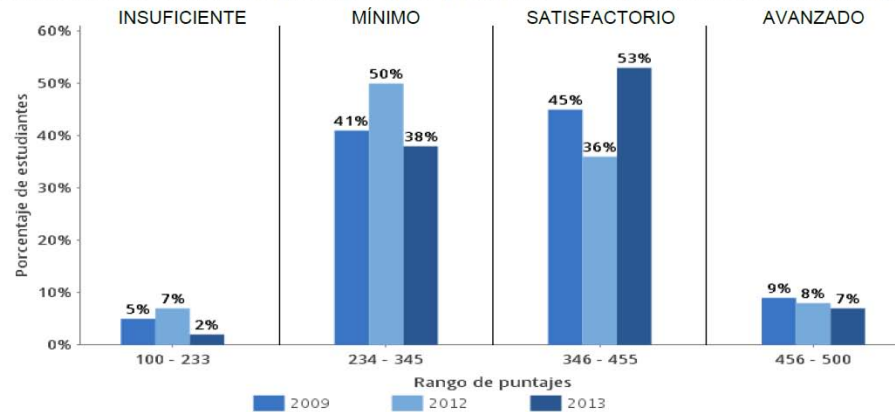
PROSPERIDAD  
PARA TODOS

Establecimiento educativo: ESC NORMAL SUPERIOR DIST MARIA MONTESSOR||

Código DANE: 111001011908

Resultados de noveno grado en el área de matemáticas

Distribución de los estudiantes según rangos de puntaje y niveles de desempeño en matemáticas, noveno grado



Número de estudiantes

2009	2012	2013
144	92	147

FIGURA 7.5. Comparativo de Desempeños

En relación al componente de *razonamiento y argumentación* un estudiante promedio de la Escuela Normal

- Utiliza ecuaciones para solucionar situaciones problema.
- Encuentra relaciones o propiedades que determinan la formación de secuencias numéricas.
- Analiza situaciones modeladas a través de funciones lineales o cuadráticas.
- Establece conjeturas sobre propiedades y relaciones numéricas convencionales.

Para el componente de *comunicación, representación y modelación*:

- Utiliza el lenguaje verbal y la representación gráfica para modelar situaciones problema.
- Establece relaciones entre expresiones numéricas y expresiones algebraicas.

Finalmente en *formulación y solución de problemas*:

- Utiliza las propiedades de la potenciación, radicación y/o logaritmación para solucionar un problema.
- Da significado, en un contexto, a la solución de una ecuación.

Se puede concluir que la contextualización de las situaciones problema, y en este caso con la aplicación de la Criptografía como recurso didáctico favorecen los aprendizajes en los estudiantes principalmente en las estrategias de la solución de problemas y argumentación de las mismas, aún más conlleva a que los estudiantes conozcan nuevas investigaciones en el desarrollo de las matemáticas como ciencia que permite el avance tecnológico de la humanidad.

---

---

## Conclusiones

---

---

Abordar temáticas como solución de sistemas de ecuaciones lineales, aritmética de matrices y algunas técnicas criptográficas con sus aplicaciones en la enseñanza de las matemáticas escolares, permite generar habilidades en los estudiantes que los acercan y familiarizan con la actividad matemática, en cuanto exige a los jóvenes el desarrollo de la comunicación, el razonamiento, la resolución de problemas, la ejercitación de procedimientos y la modelación.

Uno de los objetivos de este trabajo consistió en presentar diferentes instancias históricas de la Criptografía que pueden ser usadas como recurso para la enseñanza de las matemáticas. Esta propuesta, desea resaltar que, a pesar de ser una disciplina con un enorme desarrollo en la actualidad, basa muchos de sus sistemas criptográficos en conceptos matemáticos al alcance del currículo de la educación Media.

Así mismo, hoy en día el avance de las tecnologías de información y comunicación, impulsan a replantear qué y cómo se enseña en la educación escolar y universitaria, pues los conceptos que en ocasiones se plantean para estos grados de escolaridad no corresponden a las demandas y vivencias de la humanidad, es importante que la tendencia actual es ocultar y proteger la información en distintos contextos sociales.

Con el diseño e implementación de la secuencia didáctica para la enseñanza aritmética de las matrices y la solución de sistemas de ecuaciones lineales a través de la criptografía, se puede concluir que:

- Permitió desarrollar habilidades en los estudiantes como: razonamiento y argumentación, comunicación, representación y modelación, formulación y solución de problemas; además los estudiantes valoraron el lenguaje algebraico y numérico para los resolver las situaciones planteados, permitiéndoles alcanzar confianza y cercanía con algunas estructuras matemáticas como las de congruencias, matrices, ecuaciones lineales; definiendo las estrategias de solución para conseguir los resultados.
- Competencias ciudadanas Esquema Shamir: Este método en particular, en el cual los estudiantes requirieron aprender sobre polinomios y la solución de

ecuaciones y donde el objetivo principal fue descubrir un secreto, facilitó la cooperación y participación en un grupo a través de la comunicación y transparencia, involucrando conceptos matemáticos y relaciones interpersonales para alcanzar la meta de encontrar el enigma.

- Estrategías de solución de problemas como lo fueron: Entender el problema (lectura comprensiva), Configurar un plan (identificar conocimientos existentes y requeridos), Ejecutar el plan (No desfallecer ante la dificultad de la pronta solución, o revisión y formación de los conceptos necesarios en la solución ), Mirar hacia atrás (institucionalizar los conceptos aprendidos).
- Uso de la criptografía como recurso de motivación: para introducir algunos conceptos matemáticos fundamentales para los estudiantes a través de la resolución de problemas y promoción del trabajo colaborativo en el aula; la criptografía involucra situaciones de motivación debido a que mezcla la intriga, la curiosidad y astucia como estrategias para ocultar información así como, la habilidad para descubrir secretos.
- Elevar niveles de exigencia y aprobación: emplear esta estrategia de mejoramiento para evitar el alto índice de reprobación, aportó tanto a los estudiantes como a la autora, la posibilidad de cualificar el área disciplinar con otros elementos no tan frecuentes en el currículo escolar exigiendo la formación constante. Cabe anotar, que la propuesta fue innovadora atrajo la atención de los estudiantes lo que permitió que ellos tuvieran la necesidad de construir un conocimiento.

Finalmente, es importante resaltar que abordar algunas temáticas no fue sencillo debido a los obstáculos didácticos y epistemológicos que surgen de introducir la enseñanza de la criptografía en la educación media, esto afirma que se debe fortalecer en los conocimientos básicos desde los primeros años de escolaridad y que se requieren en los diferentes pensamientos establecidos por el Ministerio de Educación Nacional.

[11]



---

---

## Trabajo futuro

---

---

- Continuar diseñando y aplicando actividades que favorezcan el aprendizaje de conceptos matemáticos a través de criptografía como recurso didáctico, así mismo divulgar en la comunidad educativa la experiencia realizada en la Escuela Normal Superior Distrital María Montessori con el fin de crear un semillero de investigación en el área.
- Buscar espacios de socialización y discusión con docentes de otras áreas e instituciones para fortalecer la aplicación de la criptografía en la educación media, de manera interdisciplinar.
- Implementar talleres de criptografía para estudiantes y docentes, donde se emplee la tecnología y software propio de esta ciencia tales como: CrypTool, Criptored, TrueCrypt, entre otros; para motivar el aprendizaje y difusión de métodos criptográficos.
- Investigar sobre la criptografía visual y los primos de Mersenne como propuesta didáctica en grados superiores o grados iniciales en el trabajo de captchas y passdoodles, apoyándome en el trabajo de Investigación del profesor Agustín Moreno.

---

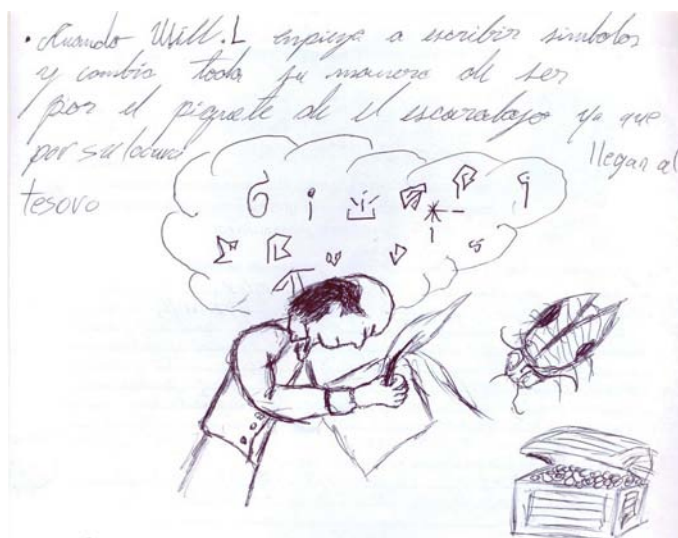
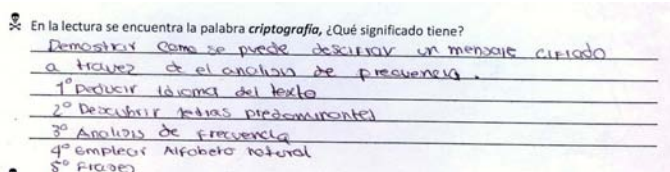
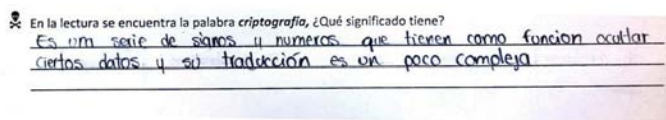
---

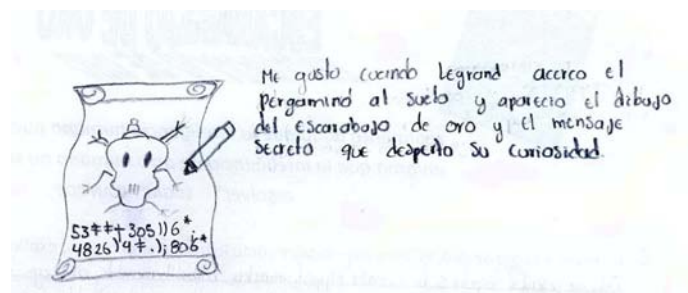
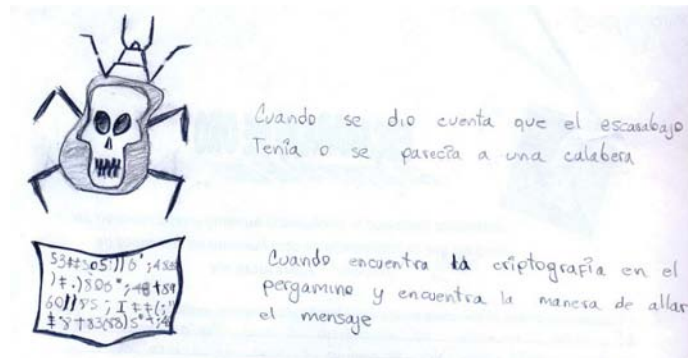
## Anexos

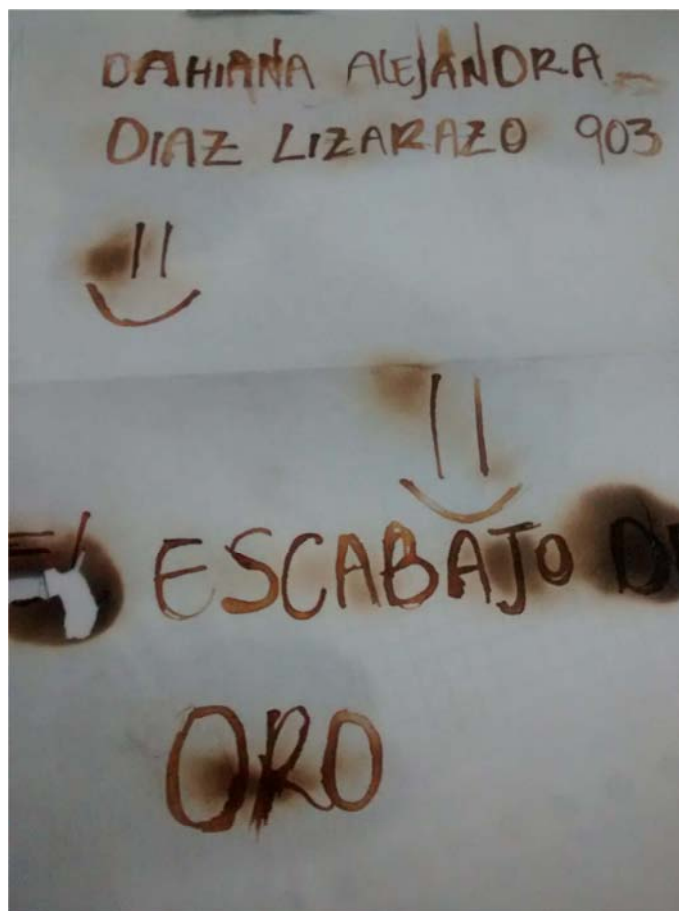
---

---

Se pueden observar estos y otros anexos de las actividades desarrolladas por los estudiantes en la página: <http://matematicasmontessoriprofeclau.blogspot.com/>








Nombre: Leidy Milena Asidillo Pajon curso: 902

**CRITOSUMA** ECUACION + ECUACION = ACERTIJO

			6
		1	6
	6	5	5
+	6	7	0
	2	2	3
	2	2	3

Número Perfecto.  
Primer número natural con 5 divisores.  
Número Primo.  
Suma digital: 16.  
Número múltiplo de 42.

16, 1, 2, 4, 8




✓ Si se pudiera extender la pantalla del celular ¿Cuáles serían los siguientes cinco números de la clave?

1 3 6 10 15 21 28 36 45 56 66

✓ Explica brevemente cómo descifraste el recorrido

Se partió del hecho de que la secuencia va aumentando y  
por lo tanto en cada uno los valores dados.

**SEGUNDA CLAVE**



Para esta clave se tiene la siguiente secuencia  
 1, 4, 9, 16, 25

De la misma manera se deben contar el número de círculos para encontrar la secuencia.

✓ ¿Qué forma tiene el desplazamiento para la segunda clave y para la primera?

Triangular

✓ ¿Qué nombre le pondrías a cada una de las claves?

Jorge Steven GARCIA

1. Alfabeto

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

2. Clave A M O R  $C = \begin{pmatrix} 10 & 13 \\ 20 & 25 \end{pmatrix}$

3. Mensaje

CRİPTOGRAFİA

C	R	I	P	T	O	G	R	A	F	J	A
2	18	9	16	20	15	6	18	0	5	8	0
$M_1$	$M_2$	$M_3$	$M_4$	$M_5$	$M_6$						

4. Escribe las matrices

$M_1 = \begin{pmatrix} 12 & 18 \end{pmatrix}$        $M_2 = \begin{pmatrix} 9 & 16 \end{pmatrix}$        $M_3 = \begin{pmatrix} 20 & 15 \end{pmatrix}$

$M_4 = \begin{pmatrix} 6 & 18 \end{pmatrix}$        $M_5 = \begin{pmatrix} 0 & 5 \end{pmatrix}$        $M_6 = \begin{pmatrix} 8 & 0 \end{pmatrix}$

---

---

## Bibliografía

---

---

- [1] E. Aparicio, *Fundamentos de la teoría de números*, Editorial Mir Moscu, 1977.
- [2] P. Caballero Gil; C. Bruno, *Educación matemática a través de la criptografía*, Revista Uno Didáctica de las Matemáticas (2004).
- [3] A. Moreno Cañadas, *Aplicaciones criptográficas*, ALTENCOA, 2006.
- [4] ———, *Descripción categórica de algunos algoritmos de diferenciación*, Ph.D. thesis, Universidad Nacional de Colombia, 2007.
- [5] ———, *Teorema del binomio y sus aplicaciones*, Temas de Aritmética y Álgebra. Notas de Clase. Universidad Nacional de Colombia (2010).
- [6] ———, *Congruencias y los números perfectos*, Temas de Aritmética y Álgebra, Universidad Nacional de Colombia (2011).
- [7] ———, *Criptografía-esteganografía, seminario avances de la ciencia*, Universidad Nacional de Colombia (2013).
- [8] A. Rojas; A. Cano, *Motivando el aprendizaje del Álgebra lineal a través de sus aplicaciones: la división de secretos*, Universidad de Córdoba (s.f.).
- [9] L. E. Dickson, *History of the theory of numbers*, vol. I, Carnegie Institution of Washington, 1919.
- [10] ———, *History of the theory of numbers*, vol. 2, Dover Publications, 2005.
- [11] Ministerio De Educación, *Estándares curriculares de matemáticas*, Ministerio de Educación Nacional de Colombia, 2003.
- [12] M. Erickson, *Aha! solutions*, Mathematical Association of America, 2009.
- [13] W. Mora F., *Introducción a la teoría de números*, Revista digital Matemática, Educación e Internet, 2010.
- [14] C. Kieran; Y. E. Filloy, *El aprendizaje del álgebra escolar desde una perspectiva psicológica*, Investigaciones y Experiencias Didácticas (1989).
- [15] J. Fraleigh, *Álgebra abstracta, primer curso*, ADDISON-WESLEY IBEROAMERICANA, 1988.
- [16] A. Moreno Cañadas; C. Gómez, *Números poligonales*, Universidad Nacional de Colombia.
- [17] L. Vásquez González, *Métodos computacionales para esquemas de compartición de secretos ideales*, Master's thesis, Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, 2004.
- [18] M. G. Gracia, *Formando docentes de matemática para la enseñanza del álgebra lineal*, Integra Educativa (2010).

- 
- [19] R. K. Guy, *Unsolved problems in numbers theory*, Springer Verlag, 2004.
- [20] J. H. Davenport, *The higher arithmetic, an introduction to the theory of numbers*, Cambridge University Press, 2010.
- [21] A. Cofré; H. Henao, *Conceptos básicos de Álgebra lineal y geometría multidimensional*, Ediciones UC (s.f.).
- [22] M. L. Iturralde, *Las matemáticas de los secretos*, Revista Numeros Didáctica de las Matemáticas **74** (2010).
- [23] M. Kline, *El pensamiento de la antigüedad a nuestros días*, vol. I, Alianza Editorial, S.A. Madrid, 1992.
- [24] A. Kurosh, *Higher algebra*, Mir Publishers, 1984.
- [25] H. Moreno; A. Losada, *Pedagogía y otros conceptos afines*, Ediciones S E M Ltda, 2004.
- [26] M. Stamp; R. Low, *Applied cryptanalysis, breaking cipher in the real world*, Wiley-Interscience a Jhon Wiley Sons, Inc., Publication, 2007.
- [27] J. Benítez López, *Breve historia del álgebra matricial*, Universidad Politécnica de Valencia (2007).
- [28] E. Malisani, *Los obstáculos epistemológicos en el desarrollo del pensamiento algebraico*, Revista IRICE, Instituto Rosario de Investigaciones en Ciencias de la Educación (1999).
- [29] E. Castro Martínez, *Dificultades en el aprendizaje del álgebra escolar*.
- [30] Escuela Normal Superior Distrital María Montessori, *Encuesta identificación de dificultades en el área de matemáticas*. <https://docs.google.com/forms/d/1tgbc-mbdvcp7qqy8zzqd5kwsirn5qfhe6dro80chei/viewform> (2013).
- [31] M.B. Nathanson, *A short proof of cauchy's polygonal number theorem*, Proceedings of The American Mathematical Society **99** (1987), no. 1.
- [32] N. Palma, *Un esquema de criptografía visual con un efecto cocktail party artificial*, Master's thesis, Universidad Nacional de Colombia, 2011.
- [33] D. Luzardo; A. Peña, *Historia del Álgebra lineal hasta los albores del siglo xx*, Divulgaciones Matemáticas **14** (2010), no. 2, 153–170.
- [34] B. D'Amore; J. Díaz Godino; M. Fandiño Pinilla, *Competencias y metemática*, Cooperativa Editorial Magisterio, 2011.
- [35] Grupo Pretexto, *La transición aritmética-Álgebra*, Grupo Editorial Gaia, 1999.
- [36] L. Jiménez; J. Gordillo; G. Rubiano, *Teoría de números (para principiantes)*, Pro-Offset Editorial Ltda, 2004.
- [37] J. B. Ruiz, *Códigos secretos: otra forma de aplicar las matrices en bachillerato*, Revista Suma (1994).
- [38] L. M. Santos, *Principios y métodos de la resolución de problemas en el aprendizaje de las matemáticas*, Grupo Editorial Iberoamerica, 1996.
- [39] A. Pérez Sanz, *Los números poligonales. una caja de sorpresas de mucha historia*, LA GACETA (s.f.).
- [40] S. Singh, *Los códigos secretos, el arte y la ciencia de la criptografía desde el antiguo egipto a la era internet*, DEBATES, 2000.
- [41] J.E. Hernández; M. Socas, *Modelos de competencia para la resolución de problemas basados en los sistemas de representación en matemáticas*, I Seminario Nacional sobre Lenguaje y Matemáticas (1994).
- [42] M. Socas, *Análisis didáctico del lenguaje algebraico en la enseñanza secundaria*, Revista Interuniversitaria de la formación del profesorado **32** (1998).

- 
- [43] ———, *La enseñanza del Álgebra en la educación obligatoria*, Revista Números Didáctica de las Matemáticas **77** (2011).
- [44] P. Xifré Solana, *Antecedentes y perspectivas de estudio en historia de la criptografía, proyecto final de carrera*, Universidad Carlos III de Madrid, 2009.
- [45] A. R. Zúñiga, *Disquisitiones arithmeticae*, Traducción Asociación Costarricense de Historia y Filosofía de la Ciencia, 1995.