

Curvas Elípticas

Base criptográfica de las monedas
electrónicas

Curvas Elípticas

Base criptográfica de las monedas
electrónicas

Rommel J. Contreras G.

RJCG, Editor

Rommel Contreras: Caripiteño. Cursó estudios en la Escuela Técnica de la Fuerza Aérea Venezolana formándose como electrónico y navegante. Se especializa en el área de comunicación de datos, seguridad de computadoras, administración de recursos informáticos y materias afines. Recibió entrenamiento en tecnología geofísica, oceanográfica y procesamiento de imágenes de satelitales. Licenciado en Física (UDO/Venezuela). Su tesis de grado la dedica al estudio del Perfil Cortical de la Cuenca del Golfo de Cariaco, área donde participa en diversas investigaciones teóricas y de campo; tiene varias publicaciones científicas. Entre otros, ha sido docente en la Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana, jefe del departamento de Redes de la Coordinación de Teleinformática de la Universidad de Oriente (Administrador jefe de Tecnología de Información y Comunicación), Director de la Oficina de Catastro de la Ciudad de Cumaná y miembro fundador de la Academia de Geo Historia del Estado Sucre.

Editor Productor: RJCG

Diseño de la Portada: Jaws Web Solutions

Edición: 2^{da} 2024

Sitio Web: [CE](#)

© Hecho el Depósito de Ley: SU2023000007

© ISBN: 978-980-18-3962-0

*A Carmen Teodorina Gaspar, mi madre: cultivó
un mundo humanizado, colmó de amor verdadero
mi existencia y la de otros; un mundo —aún
abstracto— que he intentado desentrañar y legar
por herencia.*

Agradecimientos

Es justo agradecer este libro a mis seres queridos, a:

- *mi Fidia* (compañera y esposa querida).
- *Stephanie, Jhon y Rommel*² (mis cuatro hijos; cero nietos).
- *mi padre Aser A. Contreras, fuente luminosa de constancia e inspiración; me enseñó: disciplina, ciencias, justicia y humanidad.*
- *mis seis hermanas e hijos (mis diez sobrinos).*
- mis maestros y profesores.
- y otros ... familiares y amigos.

Igualmente quisiera mucho agradecer a todos aquellos que disponen material de estudios en la Internet, en forma gratuita y desinteresada.

Prefacio

“El miedo es la principal fuente de superstición y una de las principales fuentes de crueldad. Vencer al miedo es el principio de la sabiduría, tanto en la búsqueda de la verdad como en la búsqueda de una vida digna.”

—Beltrand Russell

Este libro pretende explicar un tópico de la Matemática, propio del Álgebra Abstracta y de la Teoría de Números; que normalmente queda fuera del alcance de las grandes mayorías (incluyendo al autor).

Para los matemáticos, las Curvas Elípticas y sus colaterales (formas modulares, representaciones de Galois, etc.) son temas de investigación de frontera; donde muchos rompen sus lanzas y pocos conquistan laureles. Sin embargo, es posible un leve entendimiento de las Curvas Elípticas; sin comprometer la propiedad y el monopolio que de ellas pretenden y ostentan los matemáticos. Intentaremos buscar interpretaciones más o menos tangibles de estas “nuevas” entidades, que de este modo extenderán su derecho de ciudadanía dentro de la matemática para adquirirlo dentro de la sociedad.

Para leer este material, no se requieren pre requisitos mayores a saber leer y saber contar (sobre todo saber leer). Cualquiera con un dominio medio de la matemática de bachillerato pudiera entender la esencia de lo que se plantea. Sin embargo, un poco de más matemática permitirá visualizar el problema general con mayor profundidad; lo que ayudaría a sopesar la utilidad presente y futura de la Curvas elípticas en distintas áreas de la cotidianidad humana.

Si usted solo aspira conocer la esencia de lo que se plantea: me permito sugerirle que lea con cuidado e interés solo el capítulo sobre las Curvas Elípticas; [Capítulo 3](#). Luego, si requiere más detalles, puede decidir leer el resto de los capítulos; centrándose minuciosamente en el segundo de ellos (La Nueva Álgebra, [Capítulo 2](#)). Si usted solo quiere presumir de que leyó algo referido a “elípticas”, entonces por lo menos lea el [Capítulo 4](#); u observe sonriente las *figuritas* de todo el libro ... detalladamente. Pero si usted quiere aprender algo sustancial sobre las Curvas Elípticas, entonces, además de este libro, consulte la bibliografía y lecturas recomendadas; y expanda sus conocimientos hasta la fronteras actuales de la investigación matemática al respecto.

En el [Apéndice A](#), se presenta una herramienta para aquellos que requieran profundizar en la comprensión de lo que se plantea, mediante la ayuda del programa matemático [Sage](#); una biblioteca de código abierto de rutinas computacionales para matemáticas simbólicas, exactas y numéricas. [Sage](#) está diseñado para ser una “alternativa viable y gratuita de código abierto a: [Magma](#), [Maple](#), [Mathematica](#) y [Matlab](#)”. Un poco de más matemáticas, de teoría de números (casi sin número) será benéfica para entender la importancia de las Curvas Elípticas; y de su enraizamiento a las teorías modernas.

Es posible que se tenga la opinión de que las Curvas Elípticas son una abstracción, propia de matemáticos y afines, que en nada afecta la vida cotidiana de los seres humanos del inicio del primer cuarto del siglo XXI. Pero, la cotidianidad de la moneda electrónica, de las criptomonedas y los contratos inteligentes, imponen la necesidad de saber de qué se trata y de cómo intervienen dichas curvas, en la seguridad del mundo digitalizado. Además, si tienes un teléfono, un juego de consola o simplemente usas las redes bancarias, redes sociales u otros servicios sobre la Internet, entonces, con plena seguridad, utilizas frecuentemente un cúmulo de logros matemáticos de más de dos siglos referidos a las Curvas Elípticas. Básicamente asociado a la criptografía de la información: la seguridad de los datos y de los protocolos utilizados en las redes de comunicación entre computadoras. Todo esto ha sido posible, gracias a cientos de años de investigación en lo que antes se llegó a pensar que era una rama de la Matemática inútil: la Teoría de Números y el Álgebra Abstracta. Ahora se pueden encontrar curvas elípticas en casi todos los equipos de alta tecnología que actualmente utilizamos. No podemos predecir con absoluta certeza hacia donde nos

conducirá ésta importante tecnología fundamental en nuestra era de la información.

Solo resta decir, que por costumbre, escribir sobre matemáticas ha sido siempre el reto de tratar de comunicar ideas complejas con precisión y concisión en un lenguaje «formalista» y «axiomático». Estaría muy contento si puedo comunicar esas ideas en lenguaje natural con referencias formales (a pesar de sus complejidades); en conciencia de que las entidades matemáticas al igual que las ideas, han sido solo abstracciones que divagan en nuestra mente; pero que ahora pueden representar o salvaguardar nuestro más privados y tangibles tesoros.

El autor

Cumaná - Venezuela

Índice

Agradecimientos	v
Prefacio	vi
I El Álgebra	
1 Preliminares	2
1.1 El lenguaje de los matemáticos	3
2 La Nueva Álgebra	15
2.1 Álgebra Moderna	16
2.2 Relaciones Binarias	22
2.3 Las estructuras matemáticas	34
II Praxis Moderna del Álgebra	
3 Curvas Elípticas	54
3.1 Generalidades.	55
3.2 El poder de la abstracción	59
3.3 Curvas Elípticas	61
3.4 El aspecto de la curva elíptica.	68

3.5	Más allá de lo no resuelto	77
4	Criptografía Elíptica	82
4.1	La criptografía con curvas elípticas.	83
4.2	El Algoritmo RSA.	86
4.3	Algoritmos de encriptación elíptica.	89
4.4	Las Monedas Electrónicas	91
4.5	Límites del “cálculo elíptico”	103

Apéndices

A	Tutorial SageMath	108
A.1	Introducción	108
A.2	Aritmética Básica	109
A.3	Aritmética modular	113
A.4	Ejemplos Varios.	114
A.5	Curvas Elípticas	116
B	Notación	121

Páginas finales

Referencias y lecturas recomendadas	123
Índice Alfabético	127

Parte I

El Álgebra

Capítulo 1

Preliminares

*Nada en la vida debe ser temido, solo debe ser entendido.
Ahora es el momento de entender más, para que podamos
temer menos.*

—Marie Curie

Se considera necesaria, una cierta madurez matemática para estudiar y comprender los planteamientos del álgebra abstracta. Se dice que, es aconsejable tener conocimiento básico de la teoría de conjuntos, la inducción matemática, las relaciones de equivalencia y de las matrices. Pero, lo verdaderamente importante es la capacidad de poder leer y comprender los planteamientos matemáticos.

Trataremos de solventar tan abrumadores requisitos “pasando por alto” un obligatorio curso de álgebra abstracta; esperamos aproximarnos a la idea . . . sin que un profundo dominio del lenguaje formal simbólico matemático, nos impida la comprensión de lo que se pretende.

El lenguaje matemático, opera utilizando un lenguaje formalizado, simbólico y artificial; realizando una abstracción de los contenidos conceptuales, de los conjuntos, sus elementos y de los espacios de trabajo. Tanto así, que el álgebra abstracta, no requiere trabajar con objetos numéricos; aunque estos son necesarios para enumerar los elementos de los conjuntos o los estados del objeto de su estudio. Por ello los números no son excluidos de su entorno; por el contrario, a todo objeto estudiado con la “lupa” del álgebra abstracta, se le llama **número**.

En matemáticas, la elección de la base numérica es crucial. Dos principios fundamentales guían esta selección: en primer lugar, la capaci-

dad de ser cardinal, lo que implica adoptar un signo o dígito estándar para las unidades y repetirlo según sea necesario; en segundo lugar, la capacidad de ser ordinal, donde cada número tiene sus propios dígitos distintivos. Sin embargo, estas consideraciones no son suficientes por sí solas; es esencial que el sistema minimice el conjunto de símbolos numéricos utilizados, como en el *sistema posicional*, en el cual los dígitos se disponen de derecha a izquierda, comenzando desde las unidades inferiores hasta las superiores, permitiendo una representación eficiente.

A lo largo de la historia, diversas culturas han empleado métodos numéricos distintos [19], marcando todos ellos el inicio de las abstracciones en el estudio de las matemáticas; utilizando signos propios y empleando bases numéricas adecuadas (principalmente las bases 5, 10, 12, 20 y 60); cada quién aprovecho las ventajas de su selección [16].

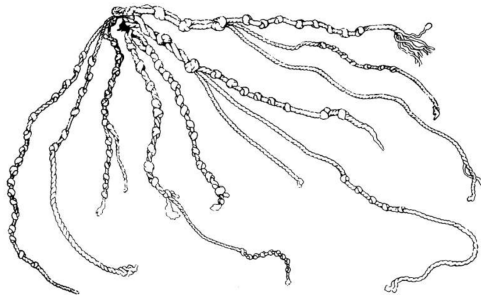


Figura 1.1 *Quipu de Cutusuma, Bolivia.* Los quipu de la civilización Inca, consisten en una serie de cuerdas o cordeles, generalmente de lana o algodón, atados a una cuerda principal. Los nudos en los cordeles y su posición codificaban información; se utilizaban para llevar registros numéricos y contables [Número 36.392 del Museo de Ciencia y Arte de la Universidad de Pennsylvania].

1.1 El lenguaje de los matemáticos

Uno de los principales objetos de las matemáticas superiores es demostrar teoremas. Los teoremas son los pilares donde se sustenta el gran edificio matemático: en general todas las ciencias. No se debe dejar a un lado la frase atribuida a Pitágoras de Samos “*Dios habla matemáticas*”.

Los teoremas matemáticos, sin embargo, no se expresan de forma oral, sino escrita. La mayor dificultad que presentan las matemáticas

para el profano es, precisamente, la lectura e interpretación de esos teoremas; no tanto la lógica de sus construcciones, sino más bien la semiótica y la abstracción que rodean sus signos. Los matemáticos delimitan: el contexto, los objetos, sus propiedades y las herramientas que aplican sobre ellos.

Es comprensible que la rigurosidad de sus planteamientos requiera de un lenguaje formal y de esquemas propios para representar su enfoque axiomático; pero igual comprensión debe permitirse (y suponerse) para que otro ser humano —indistintamente de su especialización o nivel académico— pueda aproximarse al entendimiento de lo que proponen. La estricta formalidad del lenguaje matemático, es el primer causante del alejamiento de las grandes mayorías a sus asuntos.

1.1.1 El Pretérito del Número; Mesopotamia

Los asiriólogos estudiosos de las civilizaciones mesopotámicas han determinado que durante el período llamado arcaico (3200 a 2800 a.C.), los signos numéricos se organizaron en una docena de sistemas metrológicos diferentes, los cuales designaban cantidades discretas, unidades de superficie y volumen. En ese período, los signos utilizados adquieren valor dependiendo del sistema metrológico en el que se empleen. El siguiente nivel se alcanza en el llamado período protodinástico (2800-2350 a.C.), «la escritura se desarrolla y permite la reproducción del lenguaje hablado». Se minimiza el plural de sistemas metrológicos, al poder escribirse las unidades correspondientes de manera explícita. Cuando el imperio se centraliza (alrededor del principio del *segundo milenio*), esa diversidad se unifica hacia un sistema de escritura contable: la escritura cuneiforme [6]; que evoluciona al final del ese período hacia un sistema único de base 60 semejante al utilizado anteriormente para las unidades discretas (sistema S).

Por ejemplo, el número decimal 14646, equivaldría en base 60 a: 446; ya que $4 \times 60^2 + 4 \times 60^1 + 6 \times 60^0 = 14646$ [Nota A.4.1]; se requiere de otros caracteres o signos para expresar cualquier número en la base 60. Para la base decimal, sólo requerimos de diez; y para la binaria de dos. El número 214646, se puede escribir en base 60, como: **xbq**; completando con letras los dígitos más allá del décimo.

Relictos de esa herencia —base 60— es evidente cuando medimos ángulos; también cuando expresamos coordenadas geográficas o nos referimos a la medida del tiempo (en horas, minutos y segundos); incluso cuando contamos en docenas, dado que 60 es divisible por 12, la docena es una forma natural de subdividir las unidades en el sistema sexagesimal. *A partir de ese momento, en Babilonia y su área de influencia, quedan establecidos los números abstractos; cuya escritura y manejo ya no dependen de los objetos que designan* (Babilonia se cita sólo como ciudad de referencia; otras grandes urbes le precedieron). La figura a la derecha, muestra la evolución de los numerales mesopotámicos; antes y después del eclipse de la civilización sumeria [19]. Ese fue un largo proceso de liberación del número de las unidades contables y metrológicas [12].

	Sistema Sumerio (base 60; con 10 y 6 como bases auxiliares)	Sistema ordinario Asirio-Babilonio (estrictamente en base decimal)
1	𒀭	𐎶
10	𒂵	𐎶𐎵
60	𒀭	𐎶𐎵𐎶𐎵
70	𒀭𒂵 60 10	𐎶𐎵𐎶
80	𒀭𒂵𐎶 60 20	𐎶𐎵𐎶𐎵
90	𒀭𒂵𐎶𐎵 60 30	𐎶𐎵𐎶𐎵𐎵
100	𒀭𒂵𐎶𐎶 60 40	𐎶𐎵𐎶𐎵𐎶
120	𒀭𐎶𐎶 60 60	𐎶𐎵𐎶𐎵𐎶𐎵
600	𒀭𐎶𐎶𐎶𐎶	𐎶𐎵𐎶𐎵𐎶𐎵𐎶
1000	𒀭𐎶𐎶𐎶𐎶𐎶 600 360 40	𐎶𐎵𐎶𐎵𐎶𐎵𐎶𐎵
3600	𒀭𐎶𐎶𐎶𐎶𐎶𐎶	𐎶𐎵𐎶𐎵𐎶𐎵𐎶𐎵𐎶

Figura 1.2

𒀭 1	𒂵 11	𒀭𒂵 21	𒀭𒂵𒂵 31	𒀭𒂵𐎶 41	𒀭𒂵𐎶𐎶 51
𒀭𐎶 2	𒂵𐎶 12	𒀭𒂵𐎶 22	𒀭𒂵𐎶𐎶 32	𒀭𒂵𐎶𐎶𐎶 42	𒀭𒂵𐎶𐎶𐎶𐎶 52
𒀭𐎶𐎶 3	𒂵𐎶𐎶 13	𒀭𒂵𐎶𐎶 23	𒀭𒂵𐎶𐎶𐎶 33	𒀭𒂵𐎶𐎶𐎶𐎶 43	𒀭𒂵𐎶𐎶𐎶𐎶𐎶 53
𒀭𐎶𐎶𐎶 4	𒂵𐎶𐎶𐎶 14	𒀭𒂵𐎶𐎶𐎶 24	𒀭𒂵𐎶𐎶𐎶𐎶 34	𒀭𒂵𐎶𐎶𐎶𐎶𐎶 44	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶 54
𒀭𐎶𐎶𐎶𐎶 5	𒂵𐎶𐎶𐎶𐎶 15	𒀭𒂵𐎶𐎶𐎶𐎶 25	𒀭𒂵𐎶𐎶𐎶𐎶𐎶 35	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶 45	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶 55
𒀭𐎶𐎶𐎶𐎶𐎶 6	𒂵𐎶𐎶𐎶𐎶𐎶 16	𒀭𒂵𐎶𐎶𐎶𐎶𐎶 26	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶 36	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶 46	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 56
𒀭𐎶𐎶𐎶𐎶𐎶𐎶 7	𒂵𐎶𐎶𐎶𐎶𐎶𐎶 17	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶 27	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶 37	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 47	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 57
𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶 8	𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶 18	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶 28	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 38	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 48	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 58
𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 9	𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 19	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 29	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 39	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 49	𒀭𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 59
𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 10	𒂵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 20	𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 30	𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 40	𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 50	𒀭𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶 60

Figura 1.3 Sistema tardío de numeración mesopotámico en escritura cuneiforme —estrictamente base 10—, utilizado por: sumerios, acadios y babilonios [Wikipedia].

1.1.2 Los Griegos

Los griegos, luego del período clásico, aún visualizan y conciben al número apegados a la geometría (¡un milenio después de que los números se pasearan libremente en la mente de maestros y estudiantes en Ba-

bilonia!).

El gran matemático griego Euclides (ca. 300 a.C.), retoma lo pretérito y define al número como una *multiplicidad de unidades*; siendo la unidad un concepto primitivo no necesario de definir, “*que ya está ahí*”. En su imponente libro “Los Elementos”, Euclides razona sobre números que no especifica: ni siquiera dice si las representaciones numéricas que utiliza mediante segmentos, equivalen a 1, 2 o 3, etc.; así que podemos definirlos como: «representaciones de números abstractos». Simplemente cuando quiere expresar un número, lo designa mediante un segmento; al cual le aplica razonamiento matemático mediante un enfoque axiomático [18].

Los estudios gramaticales se iniciaron en Grecia a partir del siglo V a.C.; estos estudios se vincularon con «el arte de escribir bien», dado que en ese tiempo se consideraba el lenguaje escrito más importante que el lenguaje oral. No es casual, que, a partir de ese momento en los textos griegos conocidos (principalmente de Euclides, Arquímedes y Apolonio), también quedara establecido el «canon» ideal para los textos matemáticos.

Los griegos hicieron de la geometría una herramienta que le permitía incursionar en la teoría de números, que expresaban como razones geométricas. Esta abstracción griega del número, perduró más de un milenio y medio.

1.1.3 Los Indios

En la literatura árabe y persa, aparecen referencias al respecto de que los indios tuvieron la gloria de grandes logros matemáticos¹; entre ellos:

- El sistema posicional decimal.
- El refinamiento del cálculo aritmético en la base decimal.

¹En la leyenda de *Sessa*; referida al juego del *Shaturanja* (ancestro del ajedrez). Queda reflejada la explicación que los calculistas le hacen al rey; al respecto del sistema de cálculo posicional utilizado en el reino: se requieren 9 símbolos para representar las unidades, que adquieren diferentes valores en relación a la posición de orden que tengan en la escritura de un número. Y la utilización de un décimo símbolo para representar al «cero» que tiene valor nulo y sólo se utiliza para rellenar el lugar de las unidades del orden que no están presentes. Dice finalmente el calculista “con este sistema podemos representar cualquier número sin importar el largo que pueda tener y esa misma simplicidad permite cualquier cálculo aritmético.” [19]

El cero y los números negativos², aparecen en la matemática india a partir de la alta Edad Media occidental. El cero, fue introducido primeramente sólo como símbolo de numeración antes de ser considerado como un número; pero tanto como símbolo de relleno o número, el cero fue un gran avance para las matemáticas. Pero no se puede desconocer que el “cero” ya era conocido por los babilonios de una manera menos precisa. Los que no asimilaron la existencia del cero y de los números negativos, fueron los griegos; probablemente su teoría axiomática de las razones de magnitudes, resultaba inadecuada para operar con esas abstracciones³.

Producto del estudio y del análisis, los «números» se diversifican. Aparecen «nuevos números» como resultado de operaciones y de manipulación algebraica; entidades numéricas que en principio fueron llamadas anti números «falsos», «ficticios», «absurdos», «imposibles», «imaginarios», etc.; e.g. formalmente, ateniéndose a la definición, no debe tener sentido la diferencia $a - b$ de dos enteros naturales cuando es $a < b$. Sin embargo, este “sin sentido”, no era tal para los indios; ellos eran conscientes de la interpretación de los números negativos en algunos casos, como las deudas comerciales⁴ (algo semejante ocurrió en el entorno babilonio). “Para los griegos de la época clásica, buscadores ante

²Los indios eran conscientes de la interpretación que se debía dar a los números negativos en algunos casos: por ejemplo, en problema comerciales (una deuda). Los negativos, junto con una mejora progresiva de la notación algebraica, es el único progreso notable del Álgebra al final de la Edad Media.

³El progreso hacia el rigor que bien expresa Euclides es sus escritos, genera también un estancamiento, e incluso un retroceso, respecto a las técnicas del cálculo algebraico. La teoría de las magnitudes fue concebida para la Geometría; lo que paraliza el desarrollo autónomo de la notación algebraica. Los elementos que aparecen en los cálculos deben siempre ser «representados» geoméricamente. Por otra parte, las dos leyes de composición que intervienen no están definidas sobre el mismo conjunto (la suma de dos razones no siempre está definida, y el producto de dos longitudes no es otra longitud sino un área), todo esto origina una complicación que hace casi imposible el manejo de relaciones algebraicas de grado superior al segundo[6].

⁴Los hindúes establecieron su propia codificación algebraica: La adición fue indicada por yuxtaposición; la sustracción por un punto sobre el sustraendo; la multiplicación por las letras *bha* (primera sílaba de la palabra *bhavita*; “el producto”); la división poniendo el divisor debajo del dividendo; la raíz cuadrada por la sílaba *ka* (de la palabra *karana*; “irracional”) antes de la cantidad. *Brahmagupta* (628) indica las incógnitas por *yā*, los enteros conocidos por *rū* y una segunda incógnita por *kā*. e.g. en su notación, $5xy + \sqrt{13} - 4$ escribiría como: *yā kā 5 bha ka 13 rū 4* [9].

todo de la claridad, estas extensiones hubieran sido inconcebibles; solo podían venir de calculadores más dispuestos que ellos a depositar una confianza un poco mística en el poder de sus métodos y a dejarse llevar por el mecanismo de sus cálculos sin pararse a comprobar lo lícito de cada paso, confianza en general justificada a posteriori por los resultados exactos a que conducía la extensión a estos nuevos entes matemáticos de las reglas de cálculo únicamente validas, en rigor, para los números conocidos anteriormente” [6].

1.1.4 Diofanto de Alejandría

No todos los griegos fueron atrapados por el rigor de la teoría de magnitudes, Diofanto⁵ hace grandes esfuerzos y rescata de las tradiciones pasadas, las reglas heredadas de los egipcios y de los babilonios; que aún sobrevivían sin modificaciones entre los calculistas profesionales (llamados «logísticos»). Diofanto, no se complica con las representaciones geométricas e inventa la suya propia: desarrolla de modo natural reglas para el cálculo algebraico abstracto. Actúa con libertad, sin preocuparse mucho por las ideas generales que imperaban; como la concepción axiomática de las leyes de composición⁶. Entre otras, Diofanto enuncia la «regla de los signos», y realiza cálculos con número negativo; relacionado con el cálculo de polinomios, permitiendo desarrollar productos tales como: $(a - b)(c - d)$; pero no llega a “conocer” o enunciar los número negativo como objetos numéricos independientes [6].

⁵Matemático griego, llamado “el padre del álgebra”, trabajó en la ciudad de Alejandría [fundada por Alejandro Magno al norte de África], el principal centro de intelectualismo científico en la antigüedad. [20]

⁶La influencia de Diofanto (y la de sus seguidores inmediatos) respecto a la concepción axiomática de las leyes de composición, hacen que éstas no vuelvan a aparecer en el Álgebra hasta principios del siglo XIX.

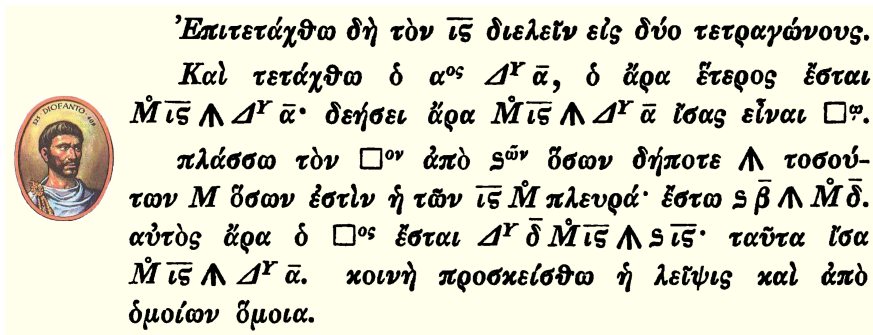


Figura 1.4 El africano Diofanto de Alejandría, según Baldor [3], y muestra de su escritura matemática altamente simbolizada (*Aritmética* 2.8) [31].

Diofanto rompe con el «canon» ideal griego para los textos matemáticos. En su *Aritmética*, opta por un estilo completamente diferente al establecido; muy alejado al de Euclides. A pesar de que evita la teoría axiomática de las razones de magnitudes, cada problema es seguido por el razonamiento que conduce a la determinación de una solución. Utiliza regularmente símbolos para formular los problemas y el tipo de prueba que les sigue, los cuales involucran enunciados relacionados con números e incógnitas; por primera vez usa un símbolo literal para representar una incógnita; otro para identificar a los números desconocidos “ ς ”⁷, otro para los ángulos rectos, etc. [Cuadro 1.5]; sin embargo, estos símbolos difieren en el fondo de la manera como se utilizan actualmente (en un entorno puramente simbólicos). Al parecer ayudaron a formar el significado de las declaraciones; como los símbolos en una abreviatura. Pero sin duda alguna, sus símbolos ayudaron a mejorar la capacidad de reconocimiento de las expresiones, de la misma manera como lo hace una escritura técnica especializada [9]; en ese sentido, facilitaron la abstracción y comprensión de elementos matemáticos complejos; por sus méritos, Diofanto es considerado uno de los padres del álgebra [20].

⁷Diofanto utilizó ς (variación de sigma minúscula) de manera especial para denotar un número desconocido en general; el simbolismo fue el elemento más importante de su legado [9].

Cuadro 1.5 Algunos Símbolos de Diofanto.

Signo	Significado	Origen-griego
ς	número desconocido	sigma minúscula
$\nmid$	signo negativo	una $\wedge$ con un $ $ central
Δ^{Υ}	incógnita cuadrática	delta superíndice epsilon
κ^{Υ}	numero cúbico	kappa superíndice epsilon
Δ^U	incógnita cúbica	delta superíndice'U'
$\square$	un número al cuadrado	
$\perp$	catetos de un Δ rectángulo	contexto pitagórico
$\overset{\circ}{M}$	las unidades	inic. de la palabra 'monades'

1.1.5 Los Árabes

Desde lejanas geografías, los árabes portaron en sus caravanas y en sus mentes, conocimiento de todo tipo y de todas las áreas del saber. Entre muchos: libros, instrumentos, técnicas, fórmulas y métodos de resolución de problemas matemáticos; con todo esmero se dedicaron a recopilar matemática y astronomía; de la India, de Grecia y de todo el mundo antiguo por donde circularon, drenando y absorbiendo sus saberes. Pero los árabes no se limitaron a ser simples transportes para las ciencias; las cultivaron, las mejoraron, las sistematizaron y las asentaron por escritos en libros y bibliotecas; ese sin duda fue su mayor aporte para la humanidad. Por ellos y de la mano de ellos, en su forma y con su grafía, el mundo occidental se entera del conocimiento pasado; «olvidado, perdido o extraviado»; gran parte de lo que se sabe del mundo antiguo, lo dice la obra árabes (lamentablemente no pudieron decirnos todo ... gran parte se perdió o continúa extraviado).

El impulso civilizatorio (con carácter de conquista) que Alejandro Magno impuso sobre los pueblos del cercano oriente y mediterráneos durante el llamado Período Heleno (323 a. C.-30 a. C.), no se agota y culmina con el derrumbe del Imperio Romano (entre los siglos V y VII); no se diluye en la Edad Media. Fue retomado por los árabes y cultivados en sus Escuelas y Universidades; en tinieblas fue esparcido por el mundo y también al cúmulo de reinos que se disputaban la península ibérica (donde aún no existía políticamente España). Los árabes asentaron en iberia al Estado Al Andaluz, al cual sembraron de jardines, y palacios; en ellos amasaron los conocimientos propios

y del mundo antiguo (babilonios, egipcios, indios, griegos, etc.). De los peninsulares castellanos, pero también de los moros africanos y de los árabes, es el mérito de que el conocimiento antiguo y “moderno” llegaran al mal llamado Nuevo Mundo; donde el helenismo aún prosigue conquistando espacio y alumbrando oscuridades.

Así como en su tiempo hicieron los griegos, los árabes fueron eficientes en organizar y axiomatizar los conocimientos matemáticos, tantos que hicieron propios, los provenientes de culturas anteriores, como los que alcanzaron en virtud del estudio, de la razón y de la constancia.

Los árabes, luego del siglo IX, introdujeron el concepto fundamental de *ecuación*; como una concatenación de argumentos lógicos (no simbolizados). Una relación que combinaba una magnitud desconocida (la incógnita), con otras magnitudes conocidas; todo ello en un contexto geométrico (frecuentemente relacionados con problemas de reparto de herencias de tierras). Luego razonaron, que, dependiendo del problema, la incógnita podía ser una magnitud geométrica o un número; se dieron cuenta que podían manipular las magnitudes geométricas, mediante un cálculo aritmético realizado mediante ecuaciones que relacionaban números; había nacido una nueva álgebra. Luego del siglo XII, con esta álgebra, realizaron cálculos aproximados en notación decimal (con cifras detrás de la coma); cálculos polinómicos muy elaborados de potencias –cuadráticas, cúbicas y cuartas– e incluso potencias negativas; y finalmente polinomios de raíces⁸ de orden cualquiera. *¡Europa aún ignoraba todo eso!*

Los árabes siguieron escribiendo frases y sentencias para tratar las ecuaciones en lenguaje ordinario, a pesar de los logros de los matemáticos indios y del heleno–africano Diofanto; sólo los coeficientes fueron indicados numéricamente.

⁸Se llama raíz (o cero) de un polinomio o de una función (definida sobre un cierto cuerpo algebraico $f(x)$) a todo elemento x perteneciente al dominio de dicha función de manera que se cumpla: $f(x) = 0$.

1.1.6 René Descartes

“Entonces apareció Descartes, e hizo lo contrario de lo que debía hacer; en vez de estudiar la naturaleza trató de imaginarla. Era el geómetra más grande de su siglo, pero la geometría deja al espíritu tal como lo encuentra. El de *Descartes se inclinaba demasiado a la invención*. Las obras del primero de los matemáticos casi no son otra cosa que novelas de filosofía. Un hombre que desdeñó las experiencias, que no citó jamás a Galileo, *que quería construir sin materiales, no podía levantar más que un edificio imaginario*. Lo que tenía de novelesco fue aceptado, y las pocas verdades mezcladas a sus quimeras fueron al principio combatidas”[35].



Figura 1.6 René Descartes [F. Hals, 1650].

En Europa, a finales del siglo XV, El Renacimiento, permitió que la curiosidad humana emprendiera el rescate de sus valores perdidos, igualmente hizo posible la aceptación de nuevos cánones; empezó a diferenciarse una ciencia pura sin el predominio de la iglesia católica. Un logro que el mundo musulmán ya había alcanzado por lo menos cinco siglos antes. A inicios del siglo XVI, los matemáticos italianos comenzaron a trabajar con ecuaciones de tercer y cuarto grado; pronto se vieron obligados a aceptar nuevos entes y campos numéricos como había sucedido con los números negativos: los llamados imaginarios. El francés Viète en 1646, introdujo las letras para designar a todos los elementos en las ecuaciones algebraicas (datos e incógnita).

René Descartes en su Geometría (apéndice de El Discurso del Método; 1637 [14]), anuncia que una ecuación algebraica tiene tantas raíces como grados; pero explica que estas raíces no siempre eran reales; en su texto introdujo formalmente el viejo término «imaginario» (Albert Girard, ya los denominaba «imposibles» 1629). Sin embargo, ambos consideraban a esos extraños números como intermediarios para tratar problemas en forma general, no lo reconocieron como objetos numéricos propios (eso tardó un poco más)[18].

La notación algebraica fue perfeccionada por Viète y Descartes; a partir de este último, la notación algebraica ha sido (poco más o menos) la que empleamos hoy[6].

Uno de los legados más perdurables de René Descartes fue el desar-

rollo de la geometría analítica (llamada geometría cartesiana), donde utiliza un refinado lenguaje simbólico; lenguaje que se ha generalizado y enriquecido por los matemáticos luego de él, esta herencia se ha extendido a toda la matemática. Descartes inició la convención de representar con letras las incógnitas en las ecuaciones e.g., $[x, y, z]$; igual para los datos conocidos e.g., $[a, b, c]$. También fue pionero en la notación estándar que usa súper índices para mostrar las potencias o exponentes; e.g., los 2 utilizados en x^2 para indicar x al cuadrado [39].

El cero, los números negativos, las interpretaciones y abstracciones de carácter geométrico o cinemático; junto con las mejoras progresiva de la notación y la sintaxis algebraica iniciada por Diofanto: representan el único progreso notable del Álgebra al final de la Edad Media; antes de «El Renacimiento». En matemáticas, al renacimiento se le debería llamar racionalismo; siendo René Descartes el mejor representante de ese impulso que aún no culmina.

1.1.7 Diversidad numérica y las reglas del álgebra

La evolución de los números a lo largo de la historia ha sido testigo de la emergencia de nuevos conceptos numéricos, resultado tanto de operaciones matemáticas como de reflexiones sobre su significado. Estas nuevas entidades, inicialmente denominadas de diversas maneras: ‘anti números’, ‘falsos’, ‘ficticios’, ‘absurdos’, ‘imposibles’, ‘imaginarios’, etc.. Por ejemplo, la noción de números negativos, parecía carecer de sentido en ciertos contextos para algunas culturas antiguas; para los griegos de la época clásica, buscadores ante todo de la claridad, estas extensiones hubieran sido inconcebibles. Pero encontró justificación en situaciones como las deudas comerciales; reconocidas por civilizaciones como la india y la babilónica.

Formalmente, ateniéndose a las antiguas definiciones, no debe detener sentido la diferencia $a - b$ de dos enteros naturales cuando es $a < b$; pero los indios eran conscientes de la interpretación de los números negativos en algunos casos, como las deudas comerciales (algo semejante ocurrió en el entorno babilonio). A pesar de la resistencia inicial a estas extensiones numéricas, su adopción demostró ser esencial para la

evolución de las matemáticas, abriendo nuevas posibilidades y revelando la profundidad de su naturaleza. Confianza en general justificada a posteriori por los resultados exactos a que conducía la adopción de estos nuevos entes matemáticos, utilizando las reglas de cálculo únicamente validas, en rigor, para los números conocidos anteriormente” [6]; pero fue necesario adecuar la sintaxis matemática.

En álgebra elemental, se conocen estas expresiones y transformaciones fundamentales que imperan sobre la “sintaxis”, como reglas; reglas de supresión de paréntesis, reglas de signos, etc. Al aplicar estas reglas (combinaciones de transformaciones elementales), uno se puede olvidar que cada letra con que modernamente se trabajan las expresiones algebraicas, es sólo un símbolo que representa a un número; se puede proceder mecánicamente con independencia del significado de la transformación; atentos solamente a las reglas que rigen las transformaciones.