Teoría de los números

Manuel Murillo Tsijli
José Fabio González Argüello

2ª edición

Editorial Tecnológica de Costa Rica

Teoría de los números

Teoría de los números

Manuel Murillo Tsijli
José Fabio González Argüello

Editorial Tecnológica de Costa Rica

Primera edición
Editorial Tecnológica de Costa Rica, 2006

Segunda edición
Editorial Tecnológica de Costa Rica, 2012

510
M977t Murillo Tsijli, Manuel

Teoría de los números / Manuel Murillo Tsijli,
José Fabio González Argüello.

Cartago, Costa Rica: Editorial Tecnológica de Costa Rica, 2012.

424 páginas.

ISBN 978-9977-66-252-7

1. Aritmética 2. Divisibilidad 3. Fracciones

I. González Argüello, José Fabio

Instituto Tecnológico de Costa Rica
Correo electrónico: editorial@itcr.ac.cr
www.editorialtecnologica.tec.ac.cr
Apdo. 159-7050, Cartago
Tel: (506) 2550-2297 / 2550-2336 / 2550-2392
Fax: (506) 2552-5354
Hecho el depósito de ley.

A mis padres, aunque ausentes,
han sido siempre la fuente de
inspiración en los proyectos de mi vida.
José Fabio González Argüello

A Florizul, Héctor y Felipe,
por quienes, en ocasiones sin saberlo,
he cruzado ríos, atravesado valles,
escalado montañas y domado volcanes.
Manuel Murillo Tsijli

Agradecemos profundamente a los colegas y amigos
Félix Núñez Vanegas y Teodora Tsijli Angelaki,
por sus oportunos comentarios y valiosas sugerencias.
Su interés y apoyo contribuyeron a
publicar esta nueva edición.

Contenido

Presentación **13**

Prólogo **17**

Simbología **23**

Capítulo 1. Sistemas de numeración **27**

1.1 Introducción 29

1.2 Sistemas de numeración 52

1.3 Conjuntos numéricos 60

1.4 Representación en bases enteras 66

1.5 Aritmética en distintas bases 73

1.6 Representación en bases fraccionarias 77

1.7 Representación en bases complejas 81

Capítulo 2. Principio de inducción y conteo **83**

2.1 Notación Σ y Π 85

2.2 Inducción matemática 92

2.3 Principios de conteo 106

Capítulo 3. Divisibilidad . . . 113

3.1 Definiciones básicas . . . 115
3.2 Máximo común divisor . . . 124
3.3 Ecuaciones diofánticas (primer método) . . . 135
3.4 Números especiales . . . 144
3.5 Criterios de divisibilidad . . . 161
3.6 Principio del palomar . . . 169

Capítulo 4. Fracciones continuas . . . 173

4.1 Fracciones continuas . . . 175
4.2 Ecuaciones diofánticas (segundo método) . . . 191
4.3 Más sobre criterios de divisibilidad . . . 194

Capítulo 5. Funciones especiales . . . 197

5.1 Función parte entera . . . 199
5.2 Funciones aritméticas y multiplicativas . . . 208
5.3 Funciones τ y σ . . . 211
5.4 Función de Euler . . . 220
5.5 Función de Möbius . . . 224
5.6 Fórmula de inversión de Möbius . . . 229
5.7 Funciones completamente multiplicativas . . . 231
5.8 Solución de la ecuación $\varphi(x) = m$ . . . 234

Capítulo 6. Congruencias numéricas . . . 237

6.1 Congruencias numéricas . . . 239
6.2 Sistemas de residuos . . . 249
6.3 Teoremas de Fermat, Euler y Wilson . . . 254
6.4 Congruencias lineales . . . 263
6.5 Ecuaciones diofánticas (tercer método) . . . 267

6.6 Teorema chino del residuo 269
6.7 Reciprocidad cuadrática 275

Apéndice A. Temas afines 285

A.1 Del tiempo y calendarios 287
A.2 Juegos NIM 303
A.3 Números modulares 310
A.4 Conjuntos de Cantor 312
A.5 Criptografía 323
A.6 Proporciones, progresiones y diseño 330
A.7 Números primos menores que 12000 356

Apéndice B. Solución de algunos ejercicios 359

Bibliografía 405

Índice temático 409

Sobre los autores 419

Presentación

Esta obra va dirigida a todas aquellas personas que encuentran en las matemáticas el lenguaje universal con el cual se pueden explicar los fenómenos en nuestro entorno y, por supuesto, a quienes ven en ella una puerta que los llevará hacia la búsqueda del conocimiento orientado al desarrollo científico y tecnológico.

Contiene los temas que habitualmente se imparten en cursos iniciales e intermedios de Teoría de Números a nivel universitario, como base para una formación académica sólida.

Su objetivo principal es presentar los contenidos de forma rigurosa y atractiva; para ello, se han escogido diversos ejemplos en los cuales se observan los métodos de demostración usuales en la matemática. Se ha tratado de que los temas se asimilen en forma paulatina; con ese propósito, se han incluido, al final de cada sección, ejercicios ilustrativos de los temas expuestos. De la mayoría se puede encontrar la solución, parcial o completa, en el apéndice B.

Asimismo, se presenta una buena cantidad de ejemplos que ayudarán al lector a comprender los conceptos que aquí se ofrecen. Estos son una guía para resolver los ejercicios propuestos; en la medida de lo posible debe observarse, en cada ejemplo desarrollado, el método expuesto; se ha intentado que éstos sean lo más explicativos posible.

El final de cada ejemplo se indica con el símbolo $\blacksquare$ y el final de cada demostración de las distintas proposiciones con $\square$. El procedimiento expuesto para resolver cada ejemplo o ejercicio no siempre es único. Debe intentarse, y quizá encuentre uno igualmente efectivo y eficiente.

Puede suceder que algunos de los contenidos de esta obra ya sean dominados por el lector; sin embargo, se quiere fortalecer aquellos que, por su importancia, se convierten en herramientas esenciales para la comprensión de los temas en cursos posteriores, así como para su formación académica integral y su desarrollo profesional.

En el capítulo 1 se presenta, a manera de motivación, una introducción al desarrollo histórico de la teoría de números y de los sistemas de numeración, sistemas posicionales y no posicionales, además de la aritmética en distintas bases.

En el capítulo 2 se introduce la notación para las sumas y productos; asimismo, se presenta el método de demostración, conocido como inducción matemática. Se aplica este método para probar, principalmente, proposiciones que involucran igualdades y divisibilidad. Además, se hace una breve explicación de los principios del conteo, básicamente para combinaciones y permutaciones.

En el capítulo 3 se introducen los conceptos de divisibilidad, criterios de divisibilidad y se presenta el principio del palomar. Se incluyen las definiciones de algunos números especiales utilizados a lo largo de la obra; también se presenta el tema de las ecuaciones diofánticas y se proporciona el primer método de solución utilizando el algoritmo de la división.

En el capítulo 4 se presentan las fracciones continuas y su aplicación para resolver las ecuaciones diofánticas y determinar algunos tipos de criterios de divisibilidad.

En el capítulo 5 se hace un estudio de algunas funciones especiales en este campo, por ejemplo, la función parte entera o piso, además de las funciones aritméticas y multiplicativas, como fi, sigma, tau, miu, entre otras. Su cálculo estará relacionado con la descomposición prima de los números, a la cual se refiere el teorema fundamental de la aritmética.

En el capítulo 6 se hace una breve introducción al tema de las congruencias numéricas y su utilidad. Además, se muestran algunos teoremas importantes en la teoría de números, en el contexto de las congruencias, como son los teoremas de Wilson, Fermat, Euler y otros. Asimismo, se trabaja la ley de reciprocidad cuadrática y las congruencias cuadráticas.

En el apéndice A se presentan algunos temas relacionados con la teoría de los números, se proporciona una lista de los números primos menores que 12 000, algunos de ellos se utilizan a lo largo del texto. Se presentan, a manera de motivación, otros temas afines a la teoría de números, como son los números modulares, juegos NIM, calendarios, diseño, entre otros, que pueden servir para proyectos de profundización por parte de los lectores o estudiantes. Para algunas de las secciones aquí presentadas se contó con la valiosa colaboración de connotados académicos.

En el apéndice B se presenta la solución, parcial o completa, de algunos de los ejercicios propuestos en cada una de las secciones.

Intencionalmente, la bibliografía es extensa y los libros, artículos, así como los dominios en internet que se incluyen, les pueden servir a los lectores para profundizar en los temas relacionados con esta teoría.

Finalmente, como aportes importantes de esta nueva edición, están la inclusión de las secciones 1.3, 2.3, 3.3, 3.4, 4.3, 5.4, 5.5, 5.7, 6.4 y 6.5, así como la traducción al español de algunas citas o referencias, y una cantidad considerable de ejemplos, ejercicios y soluciones que sin duda harán más clara la exposición de los temas aquí tratados.

Manuel Murillo Tsijli
José Fabio González Argüello

Prólogo

Decía el gran Carl Gauss que la teoría de los números era la “reina de las matemáticas”, disciplina que él a su vez pensaba era la “reina de las ciencias” (“reina y sirviente de las ciencias”, añadiría Eric Temple Bell). Para el “príncipe de los matemáticos”, esta no era una afirmación meramente retórica: durante toda su vida usó los métodos y conceptos de la teoría de números en otras partes de las matemáticas. Y esa primera consideración no deja de tener significado y plena justificación cuando uno se sumerge en este apasionante mundo de los números.

A manera de ejemplo: uno de los asuntos de la teoría de los números que provoca más fascinación y un desafío impenetrable para tantos y tantos cerebros durante varios siglos fue la última conjetura de Fermat, que afirma que la relación:

$$x^n = y^n + z^n$$

no se cumple para cuatro enteros no nulos n, x, y y z con $n \gneqq 2$. No han transcurrido todavía muchos años desde que se demostró. Se ofrecieron muchos premios para quien hiciera la prueba, y nadie pudo lograrlo desde 1630 (cuando Fermat escribió aquella famosa nota marginal en la *Arithmetica* de Diofanto). De hecho, curiosamente, es el resultado matemático que más pruebas falsas ha generado. Finalmente, la prueba fue realizada por el británico Andrew Wiles en 1995 en definitiva (porque había sido anunciada por él mismo el 23 de junio de 1993, y aún contenía algunos errores).

Me es muy grato hacer el prólogo de esta obra sobre la teoría de los números de mis apreciados colegas Fabio González y Manuel Murillo, de la Universidad Nacional y el Instituto Tecnológico de Costa Rica, con el sello de la Editorial Tecnológica de Costa Rica.

Lo primero que debe decirse es que se trata de un libro que reúne muchas virtudes. En primer lugar, llena un vacío en la literatura nacional sobre esta temática. En segundo lugar, lo hace con un elevado rigor matemático y una gran calidad intelectual en el tratamiento de los temas que, aunque con un propósito introductorio, no deja de plantear perspectivas profundas.

Solo estas virtudes que he mencionado serían suficientes para felicitar entusiastamente a estos brillantes académicos por su obra. Pero, además, el libro tiene una exquisita vocación pedagógica: busca cautivar al lector, motivar al estudiante, apreciar el estudio de la teoría de los números. Los autores incluyen introducciones históricas, anécdotas, colocan muchos de los temas en contextos socioculturales y siempre buscan entretener y agudizar la mente. Manifiestamente, el libro posee una voluntad didáctica, incluso lúdica en ciertos pasajes. Sin duda, se convertirá en una obra de gran utilidad para los estudiantes de matemáticas del país y para todo aquel que quiera introducirse en el mundo de los números.

Digamos un par de palabras sobre la historia de este campo de las matemáticas. Podemos empezar señalando, con André Weyl, que: "Fermat, Euler, Legendre y Lagrange... son los fundadores de la moderna teoría de números".

A manera de ilustración, aparte de la famosa conjetura mencionada anteriormente, Fermat planteó otras que tuvieron destinos interesantes en las matemáticas posteriores. Por ejemplo, aquella que afirma que los números de la forma $2^{2^n}+1$ eran aparentemente siempre primos. Euler demostró, cuando no existían las calculadoras, que:

$$2^{2^5}+1 = 4\,294\,967\,297 = 6\,700\,417 \times 641$$

¡Un contraejemplo! La conjetura parece no ser cierta para ningún primo mayor que $n = 4$. Los colegas Murillo y González también mencionan este interesante resultado.

Otra conjetura de Fermat: que si p es primo y a es un entero divisible por p, entonces $a^p - 1$ es divisible por p. Esta segunda conjetura, que se suele llamar el "teorema menor" de Fermat, obtuvo una demostración de Euler (aunque Leibniz había dejado en manuscrito una prueba) que fue incluida en el *Commentarii* de San Petersburgo, en 1736.

Euler demostró un resultado más general por medio de la famosa "función de Euler". Si

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

con $p_1, p_2, \ldots, p_r$ los distintos factores primos de m (lo que se puede demostrar), Euler demostró que

$$a^{\varphi(m)} - 1$$

es divisible por m si a es primo relativo a m.

Legendre, otro gran matemático francés, publicó en 1797-1798 su libro *Essai sur la théorie des nombres*, el primer tratado dedicado a la teoría de números. Modernizó el teorema de la reciprocidad cuadrática y fue quien conjeturó que el número de primos menores que n, denotado por $\pi(n)$, tiende a

$$\frac{n}{\ln n - 1{,}08366}$$

cuando n crece indefinidamente; no sería sino hasta 1896 cuando se demostró que:

$$\pi(n) \to \frac{n}{\ln n}$$

cuando $n \to +\infty$ (en el sentido de que su razón tiende a 1). De hecho, esto último es un "campanazo" de lo que sería un desarrollo importantísimo en el siglo XIX: la teoría analítica de números (es decir, el uso de métodos y resultados analíticos para expresar y probar hechos acerca de los enteros).

A continuación otro ejemplo. La expresión $ax^2 + 2bxy + cy^2$, con a, b, c, enteros, es una forma binaria (tiene dos variables) y cuadrática (es de segundo grado). Si para valores específicos de a, b, c, x y y la expresión es igual a M, entonces M se dice estar representado por una forma o una clase de formas. Se pueden plantear dos problemas: ¿cuáles son los números M que son representables por una forma o una clase de formas?, y si se tiene el número M, y a, b, y c, entonces ¿cuáles son los x y y que representarían M? El último problema se ubica dentro de lo que se conoce como análisis diofántico, que es otro de los temas que específicamente también introduce este excelente libro de Manuel y Fabio. Lagrange descubrió que si un número se puede representar por una forma, entonces se puede representar con otras que son equivalentes (lo cual se hace por medio de un cambio adecuado de variables).

Sin embargo, fue con Gauss que la teoría de números empezó a adquirir una perspectiva moderna con métodos generales que englobaban casi todos los resultados anteriores. Por ejemplo, el resultado de Fermat que afirma que todo primo de la forma $4n + 1$ es la suma de dos cuadrados de manera única, Gauss lo hizo desprenderse de la teoría de las formas binarias cuadráticas que se desarrollan plenamente en las *Disquisitiones Arithmeticae*, de 1801. Con Weyl: "la grandeza de Gauss reside en que completó lo que sus predecesores habían iniciado, así como en haber inaugurado una nueva era en la historia de esta disciplina". En las *Disquisitiones* aparecen con gran desarrollo, originalidad y belleza la teoría de congruencias, la teoría de formas y también el inicio de los números algebraicos.

Los números algebraicos son realmente interesantes: empezaron con los "enteros complejos", que Kummer, el discípulo de Gauss y Dirichlet, definiría como de la forma $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{p-2}\alpha^{p-2}$ donde α es una p-ésima raíz imaginaria.

Dedekind (el de las famosas "cortaduras") extendería la definición en 1875 de la siguiente manera: Si $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$, con los a_i enteros racionales negativos o positivos, y de tal manera que r no es raíz de ninguna ecuación del mismo tipo y de grado menor a n, entonces r es un número algebraico de grado n. Si a_0 es 1, se llama entero algebraico de grado n. En esta dirección, Dedekind probó que los números algebraicos eran un campo, que los enteros algebraicos eran un anillo (noción que introdujo) y desarrolló la teoría de ideales, que puede verse como una generalización de los números enteros ordinarios. En 1887, Kronecker mostró, precisamente, que esta teoría era independiente de la teoría de los números reales.

Como se puede apreciar, análisis, álgebra (y también geometría) y la teoría de los números convergen y se benefician mútuamente, un rasgo típico de las matemáticas contemporáneas.

Varios de los temas de la teoría de los números serían condensados como retos dentro de los 23 problemas centrales que debían marcar el entonces nuevo siglo XX, señalados por David Hilbert en el famoso Congreso Internacional de Matemáticos de 1900 en París. Estos problemas se pueden encontrar en [48].

Pero volvamos al libro de Manuel y Fabio.

Los temas centrales en sistemas de numeración, congruencias, divisibilidad, inducción matemática y hasta incursiones en juegos como el ajedrez (que podrían "hacerse" con teoría de números) el lector puede encontrarlos en este libro. Hay tratamiento de muchos asuntos específicos, como por ejemplo las funciones de Möbius o de Liouville, el "teorema chino del residuo", los números figurados y los modulares, los conjuntos de Cantor y hasta la famosa "ley de reciprocidad cuadrática".

Un detalle sobre esta última "ley": Gauss la había demostrado primeramente en su *Disquisitiones Arithmeticae* en 1801, aunque el asunto había sido estudiado por Euler en su *Opuscula Analytica* de 1783 y por Legendre en 1785. Durante su vida Gauss hizo ocho demostraciones de esta ley, y posteriormente se han realizado más de cincuenta por otros matemáticos.

En Costa Rica, las matemáticas y su enseñanza-aprendizaje se encuentran en una coyuntura muy compleja. Los dramáticos rendimientos negativos en las pruebas nacionales y aquellos en los cursos de matemáticas de las universidades públicas conducen a la búsqueda de acciones en varias dimensiones para salir de la crisis. Una de las más importantes es la formación de formadores con calidad y rigor en las matemáticas y también en la pedagogía, en esa perspectiva dual se requiere de muchos instrumentos académicos y educativos. En especial libros de gran nivel y pertinencia educativa. Por eso, sin duda, este libro de Manuel y Fabio será un instrumento muy importante.

Potenciar el estudio de la teoría de los números, disciplina dotada de gran riqueza de métodos y enérgica provocación al razonamiento y a la aventura intelectual, una disciplina llena de belleza e ingeniosidad innatas, constituye un objetivo relevante de los esfuerzos por mejorar la formación matemática de nuestros estudiantes, de los profesores de matemáticas y de la población en general. En ese sentido tan medular, esta obra de los académicos costarricenses Fabio González Argüello y Manuel Murillo Tsijli constituye una contribución muy valiosa.

La Editorial Tecnológica de Costa Rica se pone una flor en el hojal con la publicación de este libro.

Ángel Ruiz Zúñiga
Director
Centro de Investigaciones Matemáticas y Meta-Matemáticas
Universidad de Costa Rica
Proyecto Apoyo a la Investigación AIEM, Universidad Nacional
Correo electrónico: angelruizz@racsa.co.cr
www.cimm.ucr.ac.cr/aruiz/ o www.angelruizz.com/
22 de noviembre del 2005

Simbología

$\Rightarrow\Leftarrow$	contradicción
$\exists$	cuantificador existencial
$\forall$	cuantificador universal
$\mathbb{N}$	$\{0, 1, 2, \dots\}$
$\mathbb{N}^*$	$\{1, 2, \dots\}$
$\mathbb{Z}$	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}^*$	$\mathbb{Z} - \{0\}$
$\mathbb{Q}$	conjunto de los números racionales
$\mathbb{R}$	conjunto de los números reales
$\varnothing$ o $\{\ \}$	conjunto vacío
$A \approx B$	conjuntos equipotentes
$a \mid b$	a divide a b
$a \nmid b$	a no divide a b
$\overset{\bullet}{a}$ o $\overline{a}$ o $[a]$	clase de equivalencia de a
$\sum$	suma
$\prod$	producto
$\mathrm{mcd}(a, b)$	máximo común divisor de a y b
$\mathrm{mcm}(a, b)$	mínimo común múltiplo de a y b
S_p	$1^p + 2^p + 3^p + \cdots + n^p$
$n!$	función factorial de n
$\lvert x \rvert$	función valor absoluto de x
$\lvert A \rvert$	cardinalidad del conjunto A

$\lfloor x \rfloor$	parte entera de x
$\vartheta(x)$	parte fraccionaria de x
$\varphi(n)$	función de Euler
$\pi(n)$	función pi
$\sigma(n)$	función sigma
$\mu(n)$	función de Möbius
$\tau(n)$	función tau
$\zeta(n)$	función zeta de Riemann
$\lambda(n)$	función de Liouville
$\nu(n)$	número de divisores primos de n
$\equiv$	equivalencia o congruencia
$\mathbb{Z}_n$	partición de $\mathbb{Z}$ módulo n
$Ta(n)$	enésimo número taxicab
$E_p(m)$	exponente de p en factorización prima de m
$(a_k a_{k-1} \ldots a_0)_b$	representación de n en base b
$[a_1, a_2, a_3, \ldots, a_n]$	fracción continua
c_k	k-ésimo convergente
$\left(\frac{a}{p}\right)$	símbolo de Legendre
M_p	números de Mersenne
ϕ	razón áurea
F_n	números de Fermat o de Fibonacci
L_n	números de Lucas
$\mathbf{1}_p$	primos de unidad repetida
$P(n,r)$	permutaciones
$C(n,r)$	combinaciones
$\mathfrak{C}$	conjunto de Cantor
$E^{(\omega)}$	espacio de los arreglos infinitos

Mayúscula	Minúscula	Nombre
A	α	alfa
B	β	beta
Γ	γ	gamma
Δ	δ	delta
E	ϵ, ε	epsilon
Z	ζ	zeta
H	η	eta
Θ	θ	theta
I	ι	iota
K	κ	kappa
Λ	λ	lambda
M	μ	miu
N	ν	niu
Ξ	ξ	xi
O	o	omicron
Π	π	pi
P	ρ	rho
Σ	σ	sigma
T	τ	tau
Y	υ	upsilon
Φ	ϕ, φ	phi
X	χ	chi
Ψ	ψ	psi
Ω	ω	omega

Alfabeto griego.

Capítulo 1
Sistemas de numeración

"En casi todas las ciencias, una generación destruye lo que otra ha construido, y lo que una ha establecido, otra lo deshace. Solo en la matemática cada generación añade un nuevo piso a la vieja estructura".

Hermann Hankel

Introducción
Conjuntos numéricos
Sistemas de numeración
Representación en bases enteras
Aritmética en distintas bases
Representación en bases fraccionarias
Representación en bases complejas

Este capítulo se inicia con una pequeña introducción a los distintos sistemas de numeración, posicionales y no posicionales, con una breve exposición de los que históricamente tuvieron alguna relevancia. Asimismo, se presenta la terminología propia de la teoría de números: sistema numérico, número primo, bases, divisibilidad, entre otros.

Para profundizar en los temas tratados en este capítulo, es recomendable consultar las referencias bibliográficas [29], [30] y [43].

1.1 Introducción

La aritmética y la geometría son las dos áreas de la matemática que, históricamente, se desarrollan primero. En general, se puede decir que la *teoría de números* estudia los números enteros y sus propiedades, se desarrolló desde la antigüedad bajo el nombre de aritmética, del griego $\alpha\rho\iota\theta\mu$ός (*arithmos*), número. Por un lado, tiene un atractivo relacionado a la solución de acertijos numéricos y problemas, y esto hace que los aficionados se recreen con esta teoría más que con cualquier otra rama de la matemática. Por otro lado, la dificultad derivada de la restricción propia de los enteros hace que muchos matemáticos se ocupen en la investigación de este campo.

A lo largo del tiempo, algunos números que satisfacen determinada propiedad han sido objeto de estudio y en algunos casos se les ha relacionado con la religión, la superstición, la suerte y hasta con la magia.

Las matemáticas son absolutamente necesarias para la magia, afirmaba Heinrich Cornelius Agrippa (1486-1535), famoso mago, filósofo, alquimista, cabalista, médico y nigromante alemán, quien escribió:

> "Pues todo cuanto se realiza por virtud natural está gobernado por el número, el peso y la medida. Cuando un mago obedece a la filosofía natural y a las matemáticas, y conoce las ciencias intermedias que de ella proceden −aritmética, música, geometría, óptica, astronomía, mecánica−, puede realizar cosas maravillosas".

Al tercer día resucita Jesús, 3 conforman la Santísima Trinidad, son 5 los sentidos, 7 son los pecados capitales (soberbia, avaricia, lujuria, ira, gula, envidia y pereza), 7 las virtudes teologales que se contraponen respectivamente a los pecados capitales (humildad, largueza, castidad, paciencia, templanza, caridad y diligencia), 7 los sacramentos, 7 las vidas del gato y los días de la semana, 7 los arcángeles, 7 los sabios de la antigüedad y 7 las maravillas del mundo; son 7 las notas musicales y 7 los colores del arco iris (rojo, naranja, amarillo, verde, azul, añil y violeta); en la religión islámica hay 7 estadios o cielos, y para el hinduismo existen 7 *chakras* en el cuerpo humano. En la mitología griega, al minotauro que encerró Minos en el laberinto que construyó Dédalo se le ofrecían cada año 7 muchachos y 7 doncellas de Atenas. Claro que de los bailes más famosos se tiene la *Danza de los* 7 *velos*, y los marineros más exitosos, como *Simbad*, son los que han cruzado los 7 mares.

Por otro lado, en La Biblia se presentan muchos pasajes en donde el número escogido no es al azar, por ejemplo, en Génesis 41:15-29 se habla de 7 vacas flacas y 7 vacas gordas; en Juan 21:11 se menciona 153 peces en una red, número con muchas propiedades, entre ellas el ser de 3 dígitos que incluye a 3 y el ser tricúbico (véase página 150). Son 7 los dones del Espíritu Santo (Is 11:2): sabiduría, inteligencia, consejo, fortaleza, ciencia, piedad y temor de Dios. En Apocalipsis 13:18 se da al 666 el número de *La Bestia*; en el capítulo 6 son 7 los sellos que se rompen antes de que se desate la ira de Dios, y serán 7 también los ángeles que hagan sonar las 7 trompetas para enviar los 7 castigos sobre los injustos, en los 7 cuernos. En Apocalipsis 15:1 se escribe: "*Vi en el cielo otra señal, grande y admirable: 7 ángeles que tenían las 7 plagas postreras; porque en ellas se consumaba la ira de Dios*", por supuesto que no se deben confundir estas 7 plagas con las 10 que azotaron a Egipto en el Éxodo. Aun cuando efectivamente fueron diez los males con que fue advertido el Faraón, en algunas referencias se afirma que a partir de la cuarta fueron padecidas únicamente por los egipcios y no por los israelitas, aunque en la fuente primaria, el Éxodo, no hay indicios de que hubiera sido así; en cualquier caso, se escucha el dicho popular de que a una persona *le cayeron las* 7 *plagas de Egipto* cuando le sale todo mal en un tiempo prolongado. Otros ejemplos se pueden ver en Génesis 2:3, en Mateo 18:21-22 y en Job 1:2-3 y 2:13, o consultar las centenas de referencias en [50].

Para muchos, el número 7 es mágico, es la unión de lo divino y lo terrenal, pues es la suma del 3 y el 4, conocidos como el número *divino* y el número terrestre, respectivamente.

En los cuentos infantiles, los números primos son utilizados con bastante frecuencia: 3 cochinitos, los 7 enanos de *Blancanieves*, los 3 mosqueteros de Dumas, la banda de 41 ladrones de Alí Babá, 101 dálmatas, el *Sastrecillo Valiente* que mata a 7 moscas, y no gigantes, de un solo golpe, entre muchos otros cuentos. Además, autores como Isaac Asimov, escritor en temas de ciencia ficción y divulgación científica, véase entre muchos [2] o [3] iniciando con *Yo robot*, *Fundación* y *El hombre bicentenario*; Martin Gardner, gran exponente en la divulgación de las matemáticas recreativas, en muchos problemas y relatos utiliza las propiedades de los números primos y capicúas, por ejemplo su *Circo Matemático* [18]; Carl Sagan, con su inmortal *Cosmos* y su majestuosa *Contacto* en donde se utilizan, por ejemplo, los números primos para enviar mensajes, números en base 11, números trascendentes; J.K. Rowling a lo largo de toda su saga de *Harry Potter*, que consta de 7 libros, por ejemplo en *El misterio del príncipe* [38, pág. 462], en donde se menciona la posibilidad de dividir el alma en 7 partes ya que "*... el siete es el número mágico más poderoso...*". Magnus Enzensberger con su libro *El Diablo de los Números* [14], hasta *La Quinta Montaña* de Paulo Coelho, *Cinco semanas en globo* de Julio Verne, entre muchos otros autores, han utilizado el carácter mágico de los números para hipnotizar y encantar a sus lectores.

En el cine, al que se conoce como el *séptimo arte*, se tienen, solo por citar siete películas: *Siete años en el Tibet*, *Blancanieves y los siete enanos*, *El quinto elemento*, *Seven*, *Siete novias para siete hermanos*, *Los siete samuráis*, de Akira Kurosawa, y la emblemática película de Bergman, *El séptimo sello*, en la que un caballero cruzado reta a la Muerte a una partida de ajedrez, mientras busca respuestas a las preguntas clave de la vida.

Algunos resultados de la teoría de los números son fáciles de enunciar y probar; otros son fáciles de enunciar, pero difíciles de probar, y algunas proposiciones son difíciles de comprender y difíciles de comprobar; todo esto hace que la teoría de números ocupe una posición peculiar con respecto de las distintas ramas de la matemática, por su reputación de ser difícil y estar revestida de un aura de cierto misterio, que a la vez la hace ser más interesante.

La teoría de números es fundamental para el entrenamiento inicial de todo matemático; desde el comienzo su esquema es coherente, riguroso y de extrema profundidad, las ideas fluyen y la imaginación se potencia a partir de pocas definiciones y teoremas.

Los enteros positivos constituyen, sin duda alguna, la primera creación matemática del hombre, es realmente difícil imaginar a los seres humanos sin la habilidad de contar, aunque esta se halle reducida a estrechos límites. La historia dice que ya en el 5700 a.C., los antiguos sumerios disponían de un calendario; por lo tanto, tuvieron que haber desarrollado alguna forma de aritmética. En el 2500 a.C. los sumerios desarrollaron un sistema de numeración utilizando 60 como base; este pasó a los babilonios, quienes desarrollaron una gran habilidad calculadora. La calculería era conocida por los griegos con el nombre de *logística*.

Cuando las antiguas civilizaciones alcanzaron un nivel que les dejaba tiempo libre para reflexionar sobre las cuestiones no cotidianas, algunos pueblos empezaron a especular acerca de la naturaleza y propiedades de los números. Esta curiosidad se desarrolló en un cierto misticismo numérico o *numerología*, y aún hoy números como 3, 7, 11 y 13 se consideran portadores de buena o mala suerte. Los números se utilizaron para fijar los recuerdos, celebraciones o para realizar transacciones comerciales unos 5 000 años antes de que se pensara en estudiarlos en sí mismos de forma sistemática.

El origen de la teoría de números se atribuye a los griegos, pues son los que dan la primera orientación científica al estudio de los enteros, más allá de la simple aritmética.

Pitágoras (572 – 497 a.C.), quien nació en la isla de Samos, Grecia, fue para algunos el primer matemático puro y se cree que fue discípulo de Tales. Es en esta isla donde fundó su primera escuela; luego, huyendo de la tiranía de Polícrates, estableció la segunda escuela en Crotona y la tercera en Tarento. Pitágoras y sus discípulos efectuaron un estudio bastante completo de los enteros, pues la filosofía de los pitagóricos se basaba en ellos y los consideraban pilares del conocimiento. Fueron los griegos los primeros en clasificar los enteros en números pares, impares, primos, compuestos, perfectos, amigos, entre otros (véase sección 3.4). Esta escuela aceptaba solamente los números enteros; para ellos, las fracciones no eran números.

Los pitagóricos relacionaron los números con la geometría; Pitágoras, por ejemplo, demuestró geométricamente muchas proposiciones de la teoría de números; además, introdujeron la idea de números poligonales: triangulares, cuadráticos, pentagonales, entre otros, dependiendo de una disposición geométrica muy particular (véase página 148).

A la escuela pitagórica se le atribuye la demostración del teorema de Pitágoras, resultado conocido, pero no demostrado formalmente muchos años antes por otros pueblos. Los pitagóricos estudiaron la diferencia de dos números cuadráticos consecutivos $C_{n+1} - C_n$, que llamaron *gnomon*, palabra que significa "una escuadra de carpintero". En ocasiones, el gnomon es un cuadrado perfecto, por ejemplo $C_5 - C_4 = 3^2$, consideraciones que ayudaron a formular el teorema de Pitágoras. Este teorema enuncia que en todo triángulo rectángulo, el cuadrado de la longitud de la hipotenusa es igual a la suma de los cuadrados de las longitudes de los catetos, establece una clara conexión con la geometría. Los pitagóricos se interesaron por los triángulos rectángulos cuyos lados son números enteros, llamados triángulos pitagóricos. La correspondiente terna de números (x, y, z), que representan las longitudes de los lados, se llama terna pitagórica.

Se ha encontrado una tablilla babilónica del 1700 a.C. aproximadamente, la cual contiene una lista extensa de ternas pitagóricas, algunos de sus números son bastante grandes. Los pitagóricos fueron los primeros en proporcionar un método para determinar infinidades de ternas. En notación moderna es posible describirlo como sigue: sea n un número impar mayor que 1, y sean:

$$x = n, \qquad y = \frac{n^2 - 1}{2}, \qquad z = \frac{n^2 + 1}{2}$$

la terna que resulta (x, y, z) siempre constituye una terna pitagórica en donde $z = y + 1$. He aquí algunos ejemplos:

x	3	5	7	9	11	13	15	17	19
y	4	12	24	40	60	84	112	144	180
z	5	13	25	41	61	85	113	145	181

Posteriormente, Platón (430-349 a.C.) justificó un método para determinar las ternas pitagóricas por las fórmulas $x = 4n$, $y = 4n^2 - 1$, $z = 4n^2 + 1$. Como ejemplo, considere:

x	8	12	16	20
y	15	35	63	99
z	17	37	65	101

en estos, se tiene que $z = y + 2$.

"Todo es número", como afirmó Pitágoras. Con esta frase, de alguna manera se encierra místicamente la filosofía de que el universo y todos sus secretos, misterios y milagros están regidos por el número y sus propiedades, el simple hecho que los alfabetos clásicos del latín, griego y hebreo tuvieran equivalentes numéricos (véase cuadro 1.1 página 56 para el caso del griego, para los otros consulte [46]), hace que se desarrolle una pseudociencia conocida como *gematría*.

En su forma más sencilla, la gematría iguala las palabras con números equivalentes e interpreta los equivalentes verbales. Un ejemplo es la palabra *amén*, que según la escritura griega corresponde a los números 1, 40, 8 y 50, al sumarlos se obtiene 99 y por este motivo el 99 aparece al final de muchos escritos antiguos, plegarias o tumbas.

Es importante señalar que los griegos fueron los primeros en plantear distintos tipos de paradojas, muchas de ellas relacionadas con la teoría de números. Zenón de Elea (490 – 430 a.C.), discípulo de Parménides, formuló cuatro paradojas: la de la *Dicotomía*, la de *Aquiles*, la de la *Flecha* y la del *Estadio*.

La idea de la paradoja de la Dicotomía (véase [39]), es la siguiente: un corredor debe recorrer una distancia d. Para lograrlo debe recorrer la mitad de esa distancia $\frac{d}{2}$ y también la mitad de esa mitad, que es $\frac{d}{4}$, luego, la siguiente distancia $\frac{d}{8}$, $\frac{d}{16}$ y así sucesivamente. La conclusión es que el corredor debe recorrer un número infinito de distancias y el problema es que lo debe hacer en un tiempo finito. Por lo tanto, nunca podrá recorrer esa distancia; entonces, no hay movimiento. El problema es el concepto de infinito, en particular, realizar una división de manera infinita. En nuestros tiempos, todo se reduce a calcular la suma de la serie infinita:

$$\frac{d}{2}+\frac{d}{4}+\frac{d}{8}+\frac{d}{16}+\cdots \quad = \quad d\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots\right)=d\cdot 1=d$$

o, con un argumento geométrico, se puede pensar que $\frac{1}{2}$ representa la mitad de un cuadrado de lado 1, $\frac{1}{4}$ la cuarta parte, $\frac{1}{8}$ la octava parte y así sucesivamente, de forma que $\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots$ es igual al área de todo el cuadrado, que se sabe es 1.

Alrededor de 300 a.C. ocurrió un hecho realmente importante en la historia de la matemática: la aparición de los *Elementos* de Euclides (325-265 a.C.), una colección de 13 libros que transformaron las matemáticas de la numerología en una ciencia deductiva. Euclides fue el primero en presentar hechos matemáticos junto con sus rigurosas demostraciones.

Los primeros seis libros están dedicados a la geometría plana; los siguientes tres libros están dedicados a la teoría de números, el décimo sobre inconmensurables y los tres últimos sobre geometría de sólidos. En el libro IX, Euclides demostró que existe una infinidad de números primos; esta demostración todavía se enseña en nuestros cursos formales de matemática. El libro X dio un método para obtener todas las ternas pitagóricas, dado por las fórmulas

$$x=t(a^2-b^2), \qquad y=2tab, \qquad z=t(a^2+b^2)$$

donde t, a, b son enteros positivos arbitrarios tales que $a>b$, a y b carecen de factores primos comunes, y uno de ellos, a o b, es par y el otro es impar.

Por esta época, el matemático griego Eratóstenes (276-194 a.C.) desarrolló un método para determinar los números primos menores que n, conocido como la *criba*[1] *de Eratóstenes*, aunque su aporte más importante a la ciencia es obtener una aproximación de la circunferencia de la Tierra utilizando las medidas de los ángulos de elevación al Sol.

[1] Criba es un medio de seleccionar y, en particular, de distinguir lo verdadero o bueno de lo que no lo es. En este caso, es el procedimiento ideado por Eratóstenes para seleccionar los números primos.

Además, Euclides hizo una importante contribución al problema de buscar todos los números *perfectos* (véase página 145), planteado por los pitagóricos. En el libro IX, da la fórmula para todos los números perfectos pares; demuestra que un número par es un número perfecto si es de la forma

$$2^{p-1}(2^p - 1)$$

donde tanto p como $2^p - 1$ son números primos, resultado conocido como *teorema de Euclides*. Los primeros números perfectos son el 6 y el 28, conocidos desde la Grecia Antigua, y los siguientes son 496 y 8128, descubiertos en el siglo I d.C. por Nicómaco. Si $s(n)$ denota la suma de los divisores propios de n, se tiene que

$$\begin{aligned} s(6) &= 1+2+3=6 \\ s(28) &= 1+2+4+7+14=28 \end{aligned}$$

como $496 = 16 \cdot 31 = 2^4 \cdot 31$, se tiene que

$$\begin{aligned} s(496) &= 1+2+2^2+2^3+2^4+31+31\cdot 2+31\cdot 2^2+31\cdot 2^3+31\cdot 2^4 \\ &= 496 \end{aligned}$$

es decir, 496 es perfecto. Al observar la factorización prima de estos tres enteros perfectos, se nota que $6 = 2 \cdot 3$; $28 = 4 \cdot 7$ y $496 = 16 \cdot 31$ y son de la forma $2^p(2^{p+1} - 1)$, donde el último factor es primo.

Para p primo, los números de la forma $M_p = 2^p - 1$ se conocen como los *números de Mersenne*; en caso de que M_p sea primo, se le llama primo de Mersenne. Se puede demostrar que si $2^n - 1$ es primo, entonces n también lo es (véase ejercicio 24, página 123); además, note que el recíproco no es verdadero, pues a pesar de que 11 sí es primo, $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ es compuesto. Se les llama de esta forma en honor de Martín Mersenne (1588-1648), fraile franciscano que pasó la mayor parte de su vida en los monasterios de París. Fue el autor de *Cognitata Physico-Mathematica* y estudió estos números en 1644.

Aunque no se ha demostrado, se cree que hay un número infinito de primos de Mersenne, y curiosamente solo se han encontrado 47 de ellos (véase cuadro 3.2, página 154). El mayor, que además corresponde con el mayor número primo conocido, es el número 45 dado por:

$$M_{43112609} = 2^{43112609} - 1$$

de 12978189 dígitos, descubierto en agosto del 2008 por Edson Smith, de la UCLA, en Estados Unidos. En setiembre del 2008 Hans-Michael Elvenich, en Langenfeld, Alemania, encontró el primo de Mersenne número 46 dado por $M_{37156667} = 2^{37156667} - 1$, de 11185272 dígitos, que curiosamente es menor que el anterior. En Noruega, Odd Magnar Strindmo descubrió a $2^{42643801} - 1$ en abril del 2009, el primo número 47 que cuenta con 12837064 dígitos. Para mayores detalles consulte [47].

Es fácil probar que si $2^p - 1$ es primo, entonces el número n dado por $n = 2^{p-1}(2^p - 1)$ es perfecto (véase páginas 146 y 216). Euclides fue el primero en probarlo, en el siglo IV a.C, y dos mil años más tarde, Euler demostró el recíproco del teorema de Euclides, esto es: cada número perfecto par debe ser del tipo descrito por Euclides, por ejemplo $8128 = 2^6(2^7-1)$. Como consecuencia de ello, la escritura de un número perfecto par solo puede acabar por un 6 o un 8.

Los números perfectos son, realmente, muy raros; los cinco primeros números perfectos pares son 6, 28, 496, 81128 y 33550336. En el momento actual, solo se conocen 47 números perfectos (véase página 154). No se conoce ningún número perfecto impar, tampoco se sabe si existen, pero si es así, deben ser muy grandes, de hecho, mayores que 10^{50}. Sin embargo, existen algunos resultados parciales: si existe un número perfecto impar, debe ser mayor que 10^{300} y tener al menos 8 factores primos distintos, y al menos 11 si no es divisible por 3.

La historia de los números de Mersenne y números perfectos está estrechamente relacionada con el desarrollo de la informática; para verificar este hecho, puede consultar el dominio [47].

Después de Euclides, no se efectuaron avances significativos en teoría de números hasta aproximadamente el 250 d.C., cuando otro matemático griego llamado Diofanto de Alejandría publicó su obra más importante, *Arithmetica*, compuesta por 13 libros, de los cuales se conservan solamente 6; esta es la primera obra griega en la que se realiza un uso sistemático de los símbolos algebraicos. Diofanto fue hábil para resolver ecuaciones algebraicas con dos o tres incógnitas, a pesar de que la notación que empleaba era un tanto incómoda.

Muchos de los problemas se originaron en la teoría de números y a él le pareció natural buscar soluciones enteras para las ecuaciones. Las que deben ser resueltas por medio de valores enteros de las incógnitas hoy se llaman ecuaciones diofánticas, y el estudio de tales ecuaciones recibe el nombre de *análisis diofántico*.

Un siglo después de la muerte de Diofanto se escribió la *Antología Palatina*, que contiene una serie de problemas griegos escritos en forma poética, en donde destaca uno, (véase ejercicio 3, página 142), cuya solución contiene toda la información acerca de la vida de Diofanto. Su enunciado es:

> "Aquí ves la tumba que contiene los restos de Diofanto. Se puede notar que ingeniosamente se cuenta la medida de su vida. La sexta parte de su vida, Dios se la concedió a su juventud. Después de un doceavo más, le creció la barba. Después de un séptimo adicional, encendió la luz del matrimonio, y en el quinto año fue padre. Elas, su hijo, un querido pero desafortunado niño, vivió la mitad de su padre, y esto fue también duración de un cruel destino dado, y el consoló su pena en los restantes cuatro años de su vida".

Tras Diofanto no se realizaron muchos progresos en teoría de números hasta el siglo XVII, si bien existe evidencia de que el tema empezó a crecer en el Lejano Oriente, especialmente en la India, en el periodo comprendido entre el 500 y el 1200 d.C. [39]. En esta época no se utilizaban los símbolos, los problemas se describían en su totalidad con base en palabras, al igual que el problema de la edad de Diofanto, conocida como la época *retórica*; luego vino la *sincopada*, en donde se empezaron a utilizar abreviaciones, y por último, luego de la formalización del álgebra, inició la época *simbólica*. Se recuerda la bella forma en que aparecen algunos de los problemas planteados en el libro *Lilavati*, del gran matemático hindú del siglo XII, Bhaskara (1114-1185 d.C.), véase [42]:

> "La quinta parte de un enjambre de abejas se posa sobre una flor de *kadamba*, la tercera parte en una flor de *silinda*, el triple de la diferencia entre estos dos números vuela sobre una flor de *krutja* y una abeja vuela indecisa de una flor de *pandanus* a un jazmín. Dime, hermosa niña, ¿cuál es el número de abejas?"

El más conocido de los matemáticos árabes es Mohammed ibn Musa Al-Khwarizmi (750-850) quien, en su obra *Aritmética*, explica con detalle el funcionamiento del sistema decimal de numeración y del cero que se utilizaba en la India; se cree que de ahí viene la confusión esparcida de que el sistema decimal que se utiliza sea de origen árabe y no hindú. De su nombre, que se pronunciaba en Europa como *algorismi*, proviene la palabra *guarismo*, que se utiliza para indicar las cifras de un número.

Posteriormente, Omar Khayyám (1040-1125), astrónomo, matemático y poeta árabe, quien fue director del Observatorio de Merv, actual Merí en Turkmenistán, emprendió y realizó en 1074 la reforma del calendario musulmán [45]. Como matemático, ideó un método para la extracción de raíces cuadradas y cúbicas, publicó un tratado sobre algunas dificultades de las definiciones de Euclides, entre otras. Como poeta, legó 170 cuartetos de gran belleza y sencillez, que bastaron para inmortalizarlo en su bella obra *Las Rubaiyat*.

En China se desarrollaron muchos de los conceptos de la teoría de números (en la sección 6.6 se verá el conocido teorema chino del residuo y se resolverá un problema planteado por Sun-Tsu en el siglo I d.C.). Además, hicieron grandes aportes en campos como la construcción de calendarios e incluso hasta cuadrados mágicos que fueron una interesante tradición entre los chinos, además del *Origami*.

Leonardo de Pisa (1170-1240), mejor conocido como Leonardo Fibonacci por su padre Bonacci (Fibonacci significa *figlio de Bonacci*, o sea, hijo de Bonacci) introdujo en su obra más conocida (*Liber Abaci*, 1202) la sucesión que lleva su nombre.

La sucesión de Fibonacci está dada por: 1, 1, 2, 3, 5, 8, 13, 21, ..., donde cada término de la sucesión es la suma de los dos anteriores, es la histórica solución dada por Leonardo de Pisa al "problema de los conejos", cuyo enunciado es: *Empezando con una pareja de conejos que acaba de nacer. Al cabo de dos meses, esta pareja está lista para reproducirse, generando, a partir de ahora, una nueva pareja de conejos cada mes. Esta nueva pareja que acaba de nacer, a su vez empezará a reproducirse a los dos meses, dando otra pareja cada mes. ¿Cuál es el número total de parejas de conejos en un número específico de meses?* La fórmula recursiva de esta sucesión es:

$$F_n = \begin{cases} 1 & \text{si } n = 1 \text{ o } n = 2 \\ F_{n-2} + F_{n-1} & \text{si } n \geq 3 \end{cases}$$

En el siglo XVII, el tema renació en Europa gracias a los esfuerzos, principalmente, del matemático francés Pierre de Fermat (1601-1665), conocido generalmente como el padre de la teoría moderna de números. Gran parte de la inspiración de Fermat deriva de los trabajos de Diofanto. Fue el primero en descubrir propiedades realmente profundas de los enteros y demostró los siguientes teoremas:

1. Todo número entero es un número triangular o una suma de dos o tres números triangulares. Todo número entero es cuadrático o una suma de dos, tres o cuatro cuadráticos. Todo número entero es pentagonal o una suma de dos, tres, cuatro o cinco números pentagonales, y así sucesivamente.

2. Ningún triángulo rectángulo tiene por área un cuadrado perfecto.

3. Ningún número de la forma $8k - 1$ es cuadrado o suma de dos o tres cuadrados.