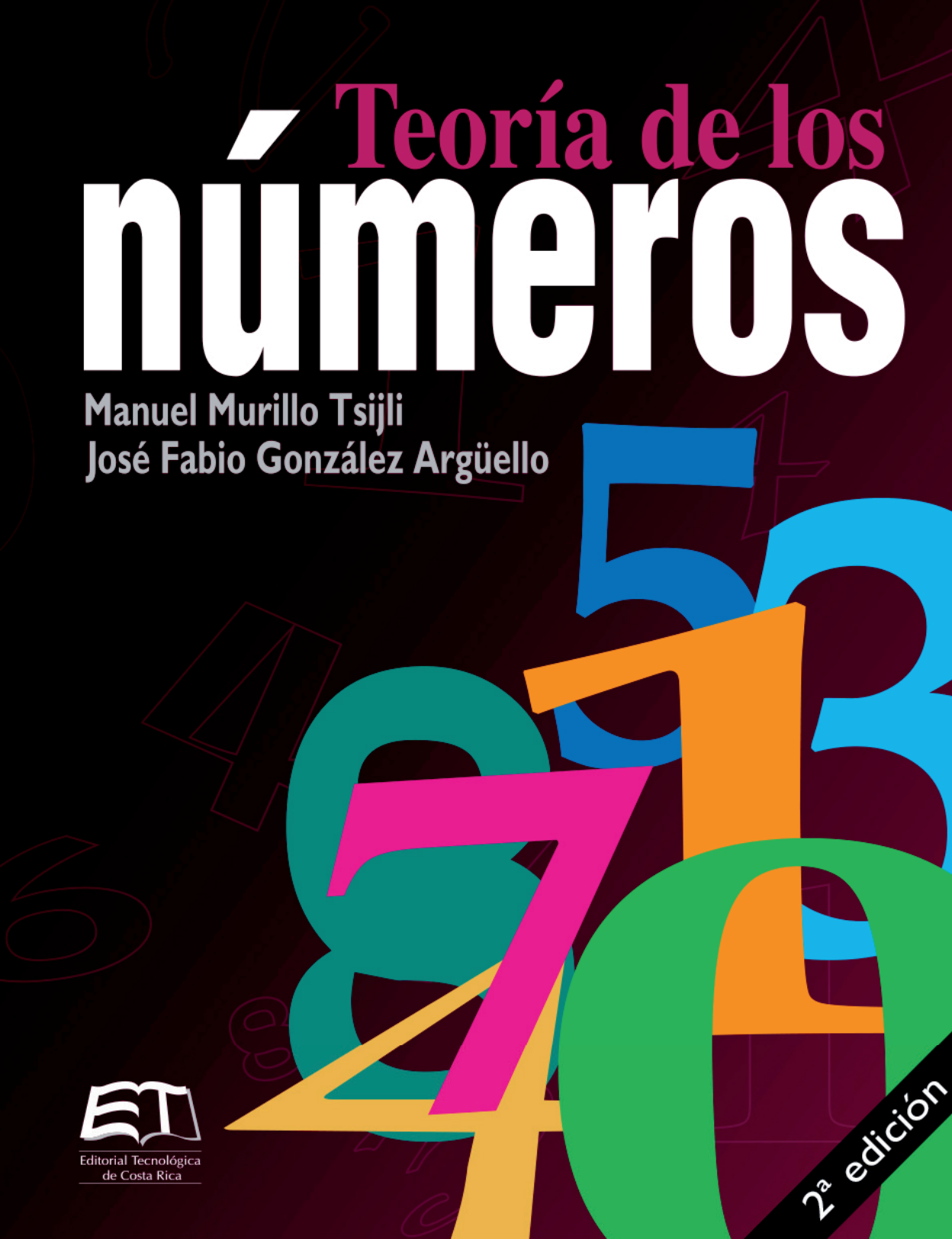
Teoría de los números

Manuel Murillo Tsijli
José Fabio González Argüello



Editorial Tecnológica de Costa Rica

2ª edición

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

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 ■ y el final de cada demostración de las distintas proposiciones con □. 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
$\dot{a}$ 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
$(a_k a_{k-1} \dots a_0)_b$	representación de n en base b
$[a_1, a_2, a_3, \dots, a_n]$	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