INTRODUCCIÓN A LA TEORÍA ANALÍTICA DE LOS NÚMEROS

T. M. APOSTOL

EDITORIAL REVERTÉ

INTRODUCCIÓN A LA TEORÍA ANALÍTICA DE LOS NÚMEROS

T. M. APOSTOL

EDITORIAL
REVERTÉ

Barcelona · Bogotá · Buenos Aires · México

Título de la obra original:
Introduction to Analytic
Number Theory

Edición original en lengua inglesa publicada por:
Springer-Verlag, New York-Heidelberg-Berlin

Edición en papel:
© Editorial Reverté, S. A., 1984
ISBN: 978-84-291-5006-3

Edición e-book (PDF):
© Editorial Reverté, S. A., 2020
ISBN: 978-84-291-9105-9

Versión española por:
Dr. José Plá Carrera
Doctor en Matemáticas, Profesor de la Facultad de Ciencias Matemáticas
de la Universidad de Barcelona

Revisada por:
Dr. Enrique Linés Escardó
Catedrático de la Facultad de Ciencias Matemáticas de la Univesidad de Madrid

#791

Prólogo

Éste constituye el primero de dos volúmenes de un libro de texto[1] *que deriva de un curso (Matemáticas 160) ofrecido en el California Institute of Technology durante los últimos 25 años. Proporciona una introducción a la Teoría analítica de números apropiada para estudiantes de Licenciatura con cierto conocimiento del Cálculo superior, pero que carecen de todo conocimiento de Teoría de números. En realidad, gran parte del libro no requiere Cálculo alguno y puede ser estudiado con provecho por los estudiantes de Escuelas superiores sofisticadas.*

La Teoría de números es tan basta y rica que un curso no puede hacer justicia a todas sus partes. Problemas que han fascinado a generaciones de matemáticos aficionados y profesionales se discuten junto con algunas de las técnicas para resolverlos.

Una de las metas de este curso consiste en nutrir el interés intrínseco que todos los estudiantes jóvenes de matemáticas parecen tener por la Teoría de números y abrirles algunas puertas a la literatura periódica corriente. Ha resultado grato comprobar que muchos de los estudiantes que han seguido este curso durante los 25 años pasados son matemáticos profesionales, y alguno ha aportado contribuciones notables por sí mismo a la Teoría de números. Este libro va dedicado a todos ellos.

[1] El segundo volumen está a punto de aparecer en la Springer-Verlag Series Graduate Texts in Mathematics bajo el título de **Modular Functions and Dirichlet Series in Number Teory** (En el momento de efectuar la traducción ya ha hecho su aparición. N. d. t.)

Índice analítico

Capítulo 5
Congruencias

Capítulo 6
Grupos abelianos finitos y sus caracteres

Capítulo 7
Teorema de Dirichlet relativa a los primos que se encuentran en progresiones aritméticas

Introducción histórica

La teoría de números es la rama de la Matemática que trata de las propiedades de la totalidad de los números,

$$1, 2, 3, 4, 5, \ldots$$

llamados *números naturales*, o *enteros positivos*.

Los enteros positivos constituyen, sin duda alguna, la primera creación matemática del hombre. Es realmente difícil imaginar los seres humanos sin la habilidad de contar, aunque ésta se hallase reducida a estrechos límites. La Historia nos dice que ya en los años 5700 A.C. los antiguos sumerios disponían de un calendario, luego debían haber desarrollado ya alguna forma de Aritmética.

En los años 2500 A.C. los sumerios desarrollaron un sistema de numeración utilizando 60 como base. Éste pasó a los babilonios que desarrollaron una gran habilidad calculadora. Se han encontrado tablillas de arcilla babilónicas que contienen tablas matemáticas elaboradas, y que se datan en 2000 A.C.

Cuando las antiguas civilizaciones alcanzaron un nivel que les dejaba tiempo libre para pensar sobre las cosas, 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 y celebrarlos y para las transacciones comeciales unos 5000 años antes de que se pensase en estudiarlos en sí mismos de forma sistemática. La primera orientación científica al estudio de los enteros, es decir, el origen de la Teoría de los números, se atribuye generalmente a los griegos. Allá por los años 600 A.C., Pitágoras y sus discípulos efectuaron

un estudio bastante completo de los enteros. Fueron los primeros en clasificar los enteros de diversas formas:

Números pares: 2, 4, 6, 8, 10, 12, 14, 16, ...
Números impares: 1, 3, 5, 7, 9, 11, 13, 15, ...
Números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 73 79, 83, 89, 97, ...
Números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, ...

Un *número primo* es un número mayor que 1 cuyos únicos divisores son 1 y él mismo. Los números que no son primos se llaman *compuestos*, excepto el número 1 que no se considera ni primo ni compuesto.

Los pitagóricos relacionaron además los números con la Geometría. Introdujeron la idea de *números poligonales:* números triangulares, números cuadráticos, números pentagonales, etc. La razón de esta nomenclatura geométrica aparece clara cuando los números se representan por medio de puntos colocados en forma de triángulos, cuadrados, pentágonos, etc., tal como se indica en la figura 1.1.

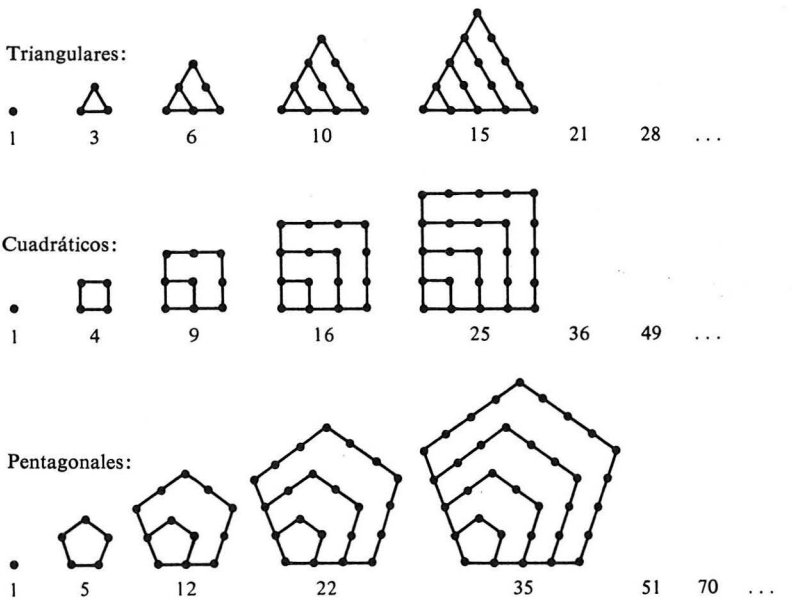

Figura I.1

Otra conexión con la Geometría procede del famoso teorema de Pitágoras que establece 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 (ver figu-

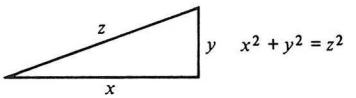

Figura I.2

ra 1.2). Los pitagóricos se interesaron por los triángulos rectángulos cuyos lados eran enteros, como los de la figura 1.3. Tales triángulos se conocen como *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, datada alrededor de 1700 A.C., que contiene una lista extensa de ternas pitagóricas, algunos de cuyos números son bastante grandes. Los pitagóricos fueron los primeros en proporcionar un método para determinar infinidades de ternas. En notación moderna podemos describirlo como sigue: Sea n un número impar mayor que 1, y sea

$$x = n, \qquad y = \tfrac{1}{2}(n^2 - 1), \qquad z = \tfrac{1}{2}(n^2 + 1).$$

La terna que resulta (x, y, z) constituye siempre una terna pitagórica con $z = y + 1$. 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

Además de éstas existen otras ternas pitagóricas; por ejemplo:

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

En estos ejemplos tenemos $z = y + 2$. Platón (430-349 A.C.) justificó un método para determinar todas estas ternas; en notación moderna viene dado por las fórmulas

$$x = 4n, \qquad y = 4n^2 - 1, \qquad z = 4n^2 + 1.$$

Alrededor de 300 A.C. ocurrió, en la historia de la Matemática, un suceso realmente importante. La aparición de los *Elementos* de Euclides, una colección de 13 libros, transformó las matemáticas de la Numerología en una ciencia deductiva. Euclides fue el primero en presentar hechos matemáticos junto con demostraciones rigurosas de tales hechos.

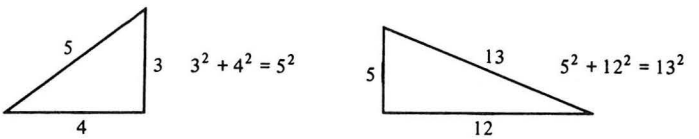

Figura I.3

Tres de tales libros se hallan dedicados a la Teoría de números (Libros VII, IX y X). En el libro IX Euclides demostró que existe una infinidad de números primos. Esta demostración todavía se enseña hoy en nuestras aulas. En el libro X dio un método para obtener todas las ternas pitagóricas si bien no demuestra que este método, realmente, las da todas. El método se puede establecer sumariamente por las fórmulas

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

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

Además Euclides aportó una importante contribución a otro problema planteado por los pitagóricos —el de buscar todos los números perfectos. El número 6 fue llamado número perfecto puesto que $6 = 1 + 2 + 3$, que es la suma de sus divisores propios (esto es, la suma de todos los divisores menores que 6). Otro ejemplo de número perfecto es 28 puesto que $28 = 1 + 2 + 4 + 7 + 14$, y 1, 2, 4, 7, y 14 son los divisores de 28 menores que 28. Los griegos se referían a los divisores propios de un número llamándolos sus «partes». Los números 6 y 28 se llamaron perfectos porque eran iguales a la suma de todas sus partes.

En el libro IX Euclides da todos los números perfectos *pares*. Demuestra que un número par es perfecto si tiene la forma

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

en donde p y $2^p - 1$ son primos.

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, para 6 y 28 tenemos

$$6 = 2^{2-1}(2^2 - 1) = 2 \cdot 3 \qquad \text{y} \qquad 28 = 2^{3-1}(2^3 - 1) = 4 \cdot 7.$$

Los cinco primeros números pares perfectos son

$$6, 28, 496, 8128 \qquad \text{y} \qquad 33\,550\,336.$$

Los números perfectos son, realmente, muy raros. En el momento actual (1980) sólo se conocen 24 números perfectos. Corresponden a los siguientes valores de p en la fórmula de Euclides:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937.

Los números de la forma $2^p - 1$, en donde p es primo, se conocen con el nombre de *números de Mersenne* y se designan por M_p en honor de Mersenne, que los estudió en 1644. Se sabe que M_p es primo para los 24 primos dados en la lista anterior y compuesto para todos los demás valores de $p \leq 257$, excepto quizás para

$$p = 157, 167, 193, 199, 227, 229;$$

para éstos no se sabe si M_p es primo o compuesto.

No se conoce ningún número perfecto *impar;* tampoco se sabe si existen. Pero si existen deben ser muy grandes; de hecho, mayores que 10^{50} (ver Hagis [29]).

Ahora volvemos a una breve descripción histórica de la Teoría de números desde el tiempo de Euclides.

Después de Euclides, 300 A.C., no se efectuaron avances significativos en Teoría de números hasta aproximadamente 250 D.C. en que otro matemático griego, Diofanto de Alejandría, publicó 13 libros, de los que se han conservado seis. Esta es la primera obra griega en la que se realiza un uso sistemático de los símbolos algebraicos. Si bien dicha notación algebraica parece torpe frente a la usual de hoy día, Diofanto fue hábil para resolver ecuaciones algebraicas con dos o tres incógnitas. Muchos de estos problemas se originaron en la Teoría de números y a él le pareció natural buscar soluciones *enteras* para las ecuaciones. Las ecuaciones que deben ser resueltas por medio de valores enteros de las incógnitas se llaman hoy *ecuaciones diofánticas*, y el estudio de tales ecuaciones recibe el nombre de *Análisis diofántico*. La ecuación $x^2 + y^2 = z^2$ relativas a las ternas pitagóricas constituye un ejemplo de ecuación diofántica.

Tras Diofanto no se realizaron muchos progresos en Teoría de números hasta el siglo diecisiete, si bien existe evidencia de que el tema empezaba a florecer en el Lejano Oriente —especialmente en la India— en el período entre 500 D.C. y 1200 D.C.

En el siglo diecisiete el tema renació en la Europa Oeste, en gran manera gracias a los esfuerzos de un matemático francés, Pierre de Fermat (1601-1665), que se conoce 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. Fermat demostró los siguientes teoremas sorprendentes:

Todo entero o es un número triangular o una suma de 2 o 3 números triangulares; todo entero o es cuadrático o es una suma de 2, 3 *o* 4 *cuadráticos; todo entero es pentagonal o es una suma de* 2, 3, 4 *ó* 5 *números pentagonales*, y así sucesivamente.

Fermat descubrió también que todo número primo de la forma $4n + 1$ tal como 5, 13, 17, 29, 37, 41, etc., es una suma de dos cuadrados. Por ejemplo,

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2,$$
$$37 = 1^2 + 6^2, \quad 41 = 4^2 + 5^2.$$

Poco tiempo después de Fermat, los nombres de Euler (1707-1783), Lagrange (1763-1813), Legendre (1752-1833), Gauss (1777-1855), y Dirichlet (1805-1859) resultaron prominentes en el posterior desarrollo de la teoría. El primer libro de Teoría de números fue publicado por Legendre en 1798. Tres años más tarde Gauss publicó *Disquisitiones Arithmeticae*, un libro que transformaba la materia en una ciencia sistemática y bella. Sin embargo utilizaba gran cantidad de contribuciones de otras ramas de la Matemática, así como de otras ciencias. El mismo Gauss consideraba este libro sobre Teoría de números su mejor obra.

En los últimos doscientos años, o sea desde los tiempos de Gauss, ha existido un desarrollo intenso de la materia en muchas direcciones. Es imposible dar en pocas páginas una clara exposición de los tipos de problemas que se estudian en la Teoría de números. El campo es muy vasto y algunas de sus partes requieren un profundo conocimiento de matemáticas superiores. A pesar de todo, existen muchos problemas de Teoría de números que resulta muy fácil enunciarlos. Algunos de ellos se refieren a números primos, y dedicamos el resto de esta introducción a tales problemas.

En las páginas anteriores hemos dado la lista de los primos menores que 100. Una tabla que daba la lista de todos los números primos menores que 10 millones fue publicada en 1914 por un matemático americano, D. N. Lehmer [43]. Existen exactamente 664 579 primos menores que 10 millones, o aproximadamente $6\frac{1}{2}\%$. Más recientemente D. H. Lehmer (el hijo de D. N. Lehmer) calculó el total de primos menores que 10 mil millones; hay exactamente 455 052 512 de tales primos, o sea aproximadamente $4\frac{1}{2}\%$ si bien no se conocen todos estos primos individualmente (ver Lehmer [41]).

Un examen detallado de una tabla de primos pone de manifiesto que se hallan distribuidos de forma muy irregular. Las tablas muestran grandes espacios entre

primos. Por ejemplo, el primo 370 261 va seguido de 111 compuestos. No existe primo alguno entre 20 831 323 y 20 831 533. Es facil demostrar que entre números primos se pueden presentar eventualmente espacios arbitrariamente grandes.

Por otro lado, las tablas muestran que se presentan reiteradamente primos consecutivos tales como 3 y 5, o 101 y 103. Los primos que, como éstos, difieren sólo en dos unidades se conocen como *primos gemelos*. Hay unos 1000 pares gemelos por debajo de 100 000 y unos 8000 por debajo de 1 000 000. El par más grande conocido hoy por hoy (ver Williams y Zarnke [76]) es $76 \cdot 3^{139} - 1$ y $76 \cdot 3^{139} + 1$. Muchos matemáticos creen que existe una infinidad de estos pares, pero ninguno ha sido capaz de demostrarlo.

Una de las razones de la irregularidad en la distribución de primos es que no existe ninguna fórmula simple que produzca todos los números primos. Algunas fórmulas proporcionan muchos primos. Por ejemplo, la expresión

$$x^2 - x + 41$$

da un primo para $x = 0, 1, 2, \ldots, 40$, mientras que

$$x^2 - 79x + 1601$$

da un primo para $x = 0, 1, 2, \ldots, 79$. Sin embargo, ninguna de tales fórmulas simples puede dar un primo para todo x, aunque se utilicen cubos y potencias superiores. De hecho, en 1752 Goldbach probó que ningún polinomio en x con coeficientes enteros puede ser primo para todo x, e incluso para x suficientemente grande.

Algunos polinomios representan infinidad de primos. Por ejemplo, cuando x, recorre los enteros $0, 1, 2, 3, \ldots$, el polinomio lineal

$$2x + 1$$

da todos los números impares por lo tanto una infinidad de primos. También, cada uno de los polinomios

$$4x + 1 \qquad \text{y} \qquad 4x + 3$$

representa una infinidad de primos. En un trabajo famoso [15] publicado en 1837, Dirichlet demostró que, si a y b son enteros positivos carentes de factores comunes, el polinomio

$$ax + b$$

da una infinidad de primos cuando x recorre todos los enteros positivos. Este resultado se conoce como teorema de Dirichlet sobre la existencia de primos en una progresión aritmética dada.

Para demostrar el teorema, Dirichet salió fuera del reino de los enteros e introdujo instrumentos de Análisis tales como los límites y la continuidad. Por este motivo puso los fundamentos de una nueva rama de la Matemática llamada *Teoría analítica de números*, en la cual se utilizan ideas y métodos del Análisis real y complejo para resolver problemas sobre enteros.

No se sabe si existe un polinomio cuadrático $ax^2 + bx + c$ con $a \neq 0$ que representa una infinidad de primos. Sin embargo, Dirichley [16] utilizó sus poderosos métodos analíticos para demostrar que, si a, $2b$, y c carecían de factores primos comunes, el polinomio cuadrático en dos variables

$$ax^2 + 2bxy + cy^2$$

representa una infinidad de primos cuando x e y recorren los enteros positivos.

Fermat creía que la fórmula $2^{2^n} + 1$ daría siempre un primo para $n = 0, 1, 2, \ldots$ Estos números se llaman *números de Fermat* y se designan por F_n. Los cinco primeros son:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \quad \text{y} \quad F_4 = 65\,537,$$

y todos ellos son primos. Sin embargo, en 1732 Euler halló que F_5 es compuesto; de hecho

$$F_5 = 2^{32} + 1 = (641)(6\,700\,417).$$

Estos números son de interés también en Geometría plana. Gauss demostró que, si F_n es un primo, por ejemplo $F_n = p$, entonces se puede construir un polígono regular de p lados con regla y compás.

Más allá de F_5 *no se han hallado otros primos de Fermat.* En efecto, para $5 \leq n \leq 16$, cada número de Fermat F_n es compuesto. Además, se sabe que F_n es compuesto para los siguientes valores aislados de n:

$n =$ 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, y 1945.

El mayor número de Fermat compuesto, F_{1945}, tiene más de 10^{582} dígitos, un número mayor que el número de letras de los listines telefónicos de Los Angeles y New York juntos (ver Robinson [59] y Wrathall [77]).

Ya hemos mencionado anteriormente que no existe ninguna fórmula simple que dé todos los primos. En conexión con este hecho, mencionemos un resultado descubierto en 1947 por un matemático americano, W. H. Mills [50]. Demostro que existe algún número A, mayor que 1 pero no entero tal que

$$[A^{3^x}] \text{ es primo para todo } x = 1\ 2, 3, \ldots$$

Aquí $[A^{3^x}]$ significa el mayor entero $\leq A^{3^x}$. Por desgracia se desconoce a qué es igual A.

Los resultados anteriores ilustran la irregularidad de la distribución de los números primos. Sin embargo, si se examinan grandes bloques de primos se encuentra que su distribución media parece bastante regular. Si bien no se terminan los números primos, se presentan cada vez más espaciados, en media, a medida que se avanza en la tabla. La cuestión del enrarecimiento en la distribución fue motivo de muchas especulaciones en el siglo diecinueve. Para estudiar esta distribución, consideramos una función, designada por $\pi(x)$, que cuenta el número de primos $\leq x$. Luego

$$\pi(x) = \text{al número de primos } p \text{ que verifican } 2 \leq p \leq x.$$

A continuación se da una breve tabla de esta función y su comparación con $x/\log x$, en donde $\log x$ es el logaritmo neperiano de x.

x	$\pi(x)$	$x/\log x$	$\pi(x) \Big/ \dfrac{x}{\log x}$
10	4	4,3	0,93
10^2	25	21,7	1,15
10^3	168	144,9	1,16
10^4	1 229	1 086	1,11
10^5	9 592	8 686	1,10
10^6	78 498	72 464	1,08
10^7	664 579	621 118	1,07
10^8	5 761 455	5 434 780	1,06
10^9	50 847 534	48 309 180	1,05
10^{10}	455 052 512	434 294 482	1,048

Examinando una tabla como ésta para $x \leq 10^6$, Gauss [24] y Legendre [40] propusieron independientemente que, para x grande, el cociente

$$\pi(x) \Big/ \frac{x}{\log x}$$

era próximo a 1 y conjeturaron que este cociente tendía a 1 cuando x tendía a ∞. Tanto Gauss como Legendre intentaron demostrar esta afirmación pero no tuvieron éxito. El problema de determinar la veracidad o falsedad de esta conjetura atrajo la atención de matemáticos eminentes durante cerca de 100 años.

En 1851 el matemático ruso Chebyshev [9] dio un paso importante al demostrar que *si* dicho cociente tenía límite, este límite debía ser 1. Sin embargo no fue capaz de demostrar que el cociente *tenía* límite.

En 1859 Riemann [58] atacó el problema con métodos analíticos, utilizando una fórmula descubierta por Euler en 1737 que relaciona los números primos con la función

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

para s real > 1. Riemann consideró valores complejos de s y dio un método ingenioso para conectar la distribución de los primos con las propiedades de la función $\zeta(s)$. Las matemáticas necesarias para justificar todos los detalles de este método no habían sido desarrolladas completamente y Riemann no fue capaz de resolver completamente el problema anterior antes de su muerte en 1866.

Treinta años más tarde se establecieron las herramientas analíticas necesarias y en 1896 J. Hadamard [28] y C. J. de la Vallée Poussin [71] demostraron, independientemente y casi simutáneamente, que

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

Este resultado notable se llama el *teorema del número primo*, y su demostración constituyó uno de los éxitos más completos de la Teoría analítica de números.

En 1949, dos matemáticos contemporáneos, Atle Selberg [62] y Paul Erdös [19] causaron sensación en el mundo matemático al descubrir una demostración elemental del teorema del número primo. Su demostración, si bien es muy intrincada no utiliza ni $\zeta(s)$ ni la teoría de las funciones complejas y, en principio, es accesible a todo el que se halle familiarizado con el Cálculo elemental.

Uno de los problemas más famosos relativos a números primos lo constituye la llamada *conjetura de Goldbach*. En 1742, Goldbach [26] escribió a Euler sugiriéndole que cada número par ≥ 4 es una suma de dos primos. Por ejemplo,

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5,$$
$$10 = 3 + 7 = 5 + 5, \quad 12 = 5 + 7.$$

Esta conjetura está sin decidir hasta hoy, si bien en los últimos años se han efectuado ciertos progresos que indican que probablemente es verdadera. ¿Por qué los matemáticos piensan actualmente que *probablemente* es verdadera si no han sido capaces de demostrarla? Ante todo, la conjetura ha sido comprobada por computación efectiva para todo número par menor que 33×10^6. Se ha establecido que cada número par mayor que 6 y menor que 33×10^6 es, en efecto, no sólo la suma de dos primos impares sino la suma de dos primos impares *distintos* (ver Shen [66]). Pero en Teoría de números la comprobación de unos pocos centenares de casos no constituye evidencia suficiente para convencer a los matemáticos de que algo es *probablemente* verdadero. Por ejemplo, todos los primos impares se dividen en dos categorías, los de la forma $4n + 1$ y los de la forma $4n + 3$. Sea $\pi_1(x)$ la notación de todos los primos $\neq x$ que son de la forma $4n + 1$, y sea $\pi_3(x)$ la de los números que son de la forma $4n + 3$. Sabemos que existe una infinidad de primos de ambos tipos. Por computación se estableció que $\pi_1(x) \neq \pi_3(x)$ para todo $x < 26\,861$. Pero en 1957, J. Leech [39] estableció que para $x = 26\,861$ se verificaba $\pi_1(x) = 1473$ y $\pi_3(x) = 1472$, luego la desigualdad se invertía. En 1914, Littlewood [49] demostró que con una frecuencia infinita esta desigualdad se invertía de sentido. Esto es, existe una infinidad de x para los que $\pi_1(x) \leq \pi_3(x)$ y también una infinidad de x para los que $\pi_3(x) \leq \pi_1(x)$. Las conjeturas relativas a los números primos pueden ser erróneas a pesar de haber sido comprobadas por el cálculo de centenares de casos.

Por consiguiente, el hecho de que la conjetura de Goldbach se haya verificado para todos los números pares menores que 33×10^6 constituye únicamente un poco de evidencia a su favor.

Otra forma que tienen los matemáticos para evidenciar la veracidad de una conjetura particular consiste en demostrar otros teoremas que son algo parecidos a la conjetura. Por ejemplo, en 1930 el matemático ruso Schnirelmann [61] demostró que existe un M tal que cada n, a partir de un lugar, es una suma de M o menos primos:

$$n = p_1 + p_2 + \cdots + p_M \qquad \text{(para } n \text{ suficientemente grande)}$$

Si supiésemos que M es igual a 2 para todo n par, habríamas demostrado la conjetura de Goldbach para n suficientemente grande. En 1956 el matemático chino Yin Wen-Lin [78] demostró que $M \leq 18$. Esto es, cada número n, a partir de un lugar, es suma de 18 o menos primos. El resultado de Schnirelmann se considera un paso de gigante con vistas a demostrar la conjetura de Goldbach. Es el primer progreso real efectuado en este problema en casi 200 años.

Un planteamiento más preciso a la solución del problema de Goldbach fue establecido en 1937 por otro matemático ruso, I. M. Vinogradov [73], el cual demostró que, a partir de un lugar, todo número *impar* es la suma de *tres* primos:

$$n = p_1 + p_2 + p_3 \qquad (n \text{ impar}, n \text{ suficientemente grande}).$$

De hecho, este resultado es verdadero para todo n impar mayor que $3^{3^{15}}$ (ver Borodzkin [5]. Hoy constituye la pieza más importante de evidencia en favor de la conjetura de Goldbach. Por un lado, es fácil demostrar que el teorema de Vinogradov es una consecuencia de la afirmación de Goldbach. Es decir, si la conjetura de Goldbach es verdadera, entonces la afirmación de Vinogradov se deduce fácilmente. La conquista más sobresaliente de Vinogradov fue su habilidad para probar su resultado sin utilizar la conjetura de Goldbach. Por desgracia, nadie ha sido capaz de establecerlo en el otro sentido y de demostrar la afirmación de Goldbach a partir de la de Vinogradov.

Otra pieza de la evidencia en favor de la conjetura de Goldbach fue establecida en 1948 por el matemático húngaro Rényi [57] que demostró que existe un número M tal que cada número impar n suficientemente grande se puede escribir como suma de un primo con otro número que no posee más de M factores primos:

$$n = p + A,$$

en donde A no posee más de M factores primos (n par, n suficientemente grande). Si supiésemos que $M = 1$ entonces la conjetura de Goldbach sería cierta para todo n suficientemente grande. En 1965 A. A. Buhstab [6] y A. I. Vinogradov [72] demostraron que $M \leq 3$, y en 1966 Chen Jing-run [10] demostró que $M \leq 2$.

Concluimos esta introducción con una breve mención de algunos de los problemas no resueltos concernientes a números primos.

1. (Problema de Goldbach). ¿Existe un número par > 2 que no sea suma de dos primos?
2. ¿Existe un número par > 2 que no sea la diferencia de dos primos?
3. ¿Existe una infinidad de primos gemelos?
4. ¿Existe una infinidad de primos de Mersenne, esto es, primos de la forma $2^p - 1$, p primo?
5. ¿Existe una infinidad de números compuestos de Mersenne?
6. ¿Existe una infinidad de primos de Fermat, esto es, primos de la forma $2^{2^n} + 1$?
7. ¿Existe una infinidad de números de Fermat compuestos?
8. ¿Existe una infinidad de primos de la forma $x^2 + 1$, en donde x es un entero? (Sabemos que existe una infinidad de primos de la forma $x^2 + y^2$, y de la forma $x^2 + y^2 + 1$, y de la forma $x^2 + y^2 + z^2 + 1$).
9. ¿Existe una infinidad de primos de la forma $x^2 + k$ (k dado)?

10. ¿Existe siempre un primo, por lo menos, entre n^2 y $(n+1)^2$ para cada entero $n \geq 1$?
11. ¿Existe siempre un primo, por lo menos, entre n^2 y $n^2 + n$ para cada entero $n > 1$?
12. ¿Existe una infinidad de primos cuyos dígitos (en base 10) son todos unos? (Existen dos ejemplos: 11 y 11 111 111 111 111 111 111 111.)

El matemático profesional se siente atraído por la Teoría de números porque en sus métodos se pueden utilizar todas las armas de la Matemática moderna para esclarecer sus problemas. Es una realidad que ramas muy importantes de la Matemática han tenido su origen en la Teoría de números. Por ejemplo, los primeros intentos para resolver el teorema del número primo estimularon el desarrollo de la teoría de las funciones complejas, especialmente la teoría de las funciones enteras. Los intentos para demostrar que la ecuación diofántica $x^n + y^n + z^n$ no posee soluciones no triviales si $n \geq 3$ (conjetura de Fermat) contribuyeron al desarrollo de la Teoría algebraica de números, una de las áreas más activas de la investigación matemática actual. Si bien la conjetura de Fermat permanece sin decidir, ello parece poco importante frente a la gran cantidad de teorías matemáticas que han sido creadas como resultado de los trabajos acerca de dicha conjetura. Otro ejemplo lo constituye la teoría de las particiones que ha constituido un factor importante en el desarrollo del Análisis combinatorio y en el estudio de las funciones modulares.

Existen centenares de problemas no resueltos en Teoría de números. Aparecen problemas nuevos más rápidamente que se resuelven los antiguos, y muchos de los antiguos llevan siglos sin resolverse. Como dijo una vez el matemático Sierpinski, «...el progreso de nuestro conocimiento de los números avanza no sólo por lo que de ellos ya conocemos, sino también porque nos damos cuenta de lo que todavía de ellos desconocemos».

Nota. Todo estudiante serio de Teoría de números ha de estar familiarizado con los tres volúmenes de la obra de Dickson, *History of the Theory of Numbers* [13], y con los seis volúmenes de la de Le Veque, *Reviews in Number Theory* [45]. La *History* de Dickson proporciona un conocimiento enciclopédico de toda la literatura de la Teoría de números hasta 1918. Los volúmenes de Le Veque reproducen todos los artículos de los volúmenes 1-44 de las *Mathematical Reviews* (1940-(1972) que se refieren directamente a cuestiones consideradas comúnmente como parte de la Teoría de números. Estas dos valiosas colecciones proporcionan prácticamente una historia de todos los descubrimientos importantes en Teoría de números desde la antigüedad hasta 1972.

Capítulo 1

El teorema fundamental de la Aritmética

1.1 INTRODUCCIÓN

En este capítulo se introducen conceptos básicos de la Teoría elemental de números tales como la divisibilidad, el máximo común divisor, y los números primos y compuestos. Los resultados principales son el teorema 1.2, que establece la existencia del máximo común divisor para todo par de enteros, y el teorema 1.10, (el teorema fundamental de la Aritmética), que demuestra que todo entero mayor que 1 se puede representar como producto de factores primos de forma única (salvo el orden de los factores). Muchas de las demostraciones utilizan la siguiente propiedad de los enteros.

El principio de inducción. *Si Q es un conjunto de enteros tales que*

(a) $1 \in Q$,
(b) $n \in Q$ *implica* $n + 1 \in Q$,

entonces

(c) *todo entero* ≥ 1 *pertenece a* Q.

Existen, además, otras formulaciones de este principio. Por ejemplo, en (a) podemos substituir 1 por un entero cualquiera k, siempre que en (c) la desigualdad ≥ 1 se substituya por $\geq k$. Además (b) se puede substituir por 1, 2, 3, ..., $n \in Q$ implica $(n + 1) \in Q$.

Suponemos que el lector se halla familiarizado con este principio así como con su uso en las demostraciones de teoremas por inducción. Le suponemos también familiarizado con el siguiente principio que es lógicamente equivalente al principio de inducción.

El principio de buena ordenación. *Si A es un conjunto no vacío de enteros positivos, entonces A posee un elemento mínimo.*

De nuevo, este principio posee formulaciones equivalentes. Por ejemplo, «enteros positivos» se puede substituir por «enteros $\geq k$ para un cierto k».

1.2 DIVISIBILIDAD

Notación. En este capítulo, las letras latinas minúsculas a, b, c, d, n, etc., denotan enteros; pueden ser positivos, negativos, o cero.

Definición de divisibilidad. Diremos que d divide n y escribiremos $d|n$ si $n = cd$ para un c. Diremos también que n es un múltiplo de d, que d es un divisor de n, o que d es un factor de n. Si d no divide a n escribiremos $d \nmid n$.

La divisibilidad establece una relación binaria entre enteros con las siguientes propiedades elementales cuyas demostraciones se dejan como ejercicio para el lector, (Salvo indicación expresa, las letras a, b, d, m, n del teorema 1,1 representan enteros arbitrarios.)

Teorema 1.1 *La divisibilidad verifica las siguientes propiedades:*

(a) $n\|n$	*(propiedad reflexiva)*
(d) $d\|n$ *y* $n\|m$ *implica* $d\|m$	*(propiedad transitiva)*
(c) $d\|n$ *y* $d\|m$ *implica* $d\|(an + bm)$	*(propiedad lineal)*
(d) $d\|n$ *implica* $ad\|an$	*(propiedad de multiplicación)*
(e) $ad\|an$ *y* $a \neq 0$ *implica* $d\|n$	*(propiedad de simplificación)*
(f) $1\|n$	*(1 divide a todos los enteros)*
(g) $n\|0$	*(cada entero divide a cero)*
(h) $0\|n$ *implica* $n = 0$	*(el cero sólo divide al cero)*
(i) $d\|n$ *y* $n \neq 0$ *implica* $\|d\| \leq \|n\|$	*(propiedad de comparación)*
(j) $d\|n$ *y* $n\|d$ *implica* $\|d\| = \|n\|$	
(k) $d\|n$ *y* $d \neq 0$ *implica* $(n/d)\|n$.	

Nota. Si $d|n$ entonces n/d se llama el divisor conjugado de d.