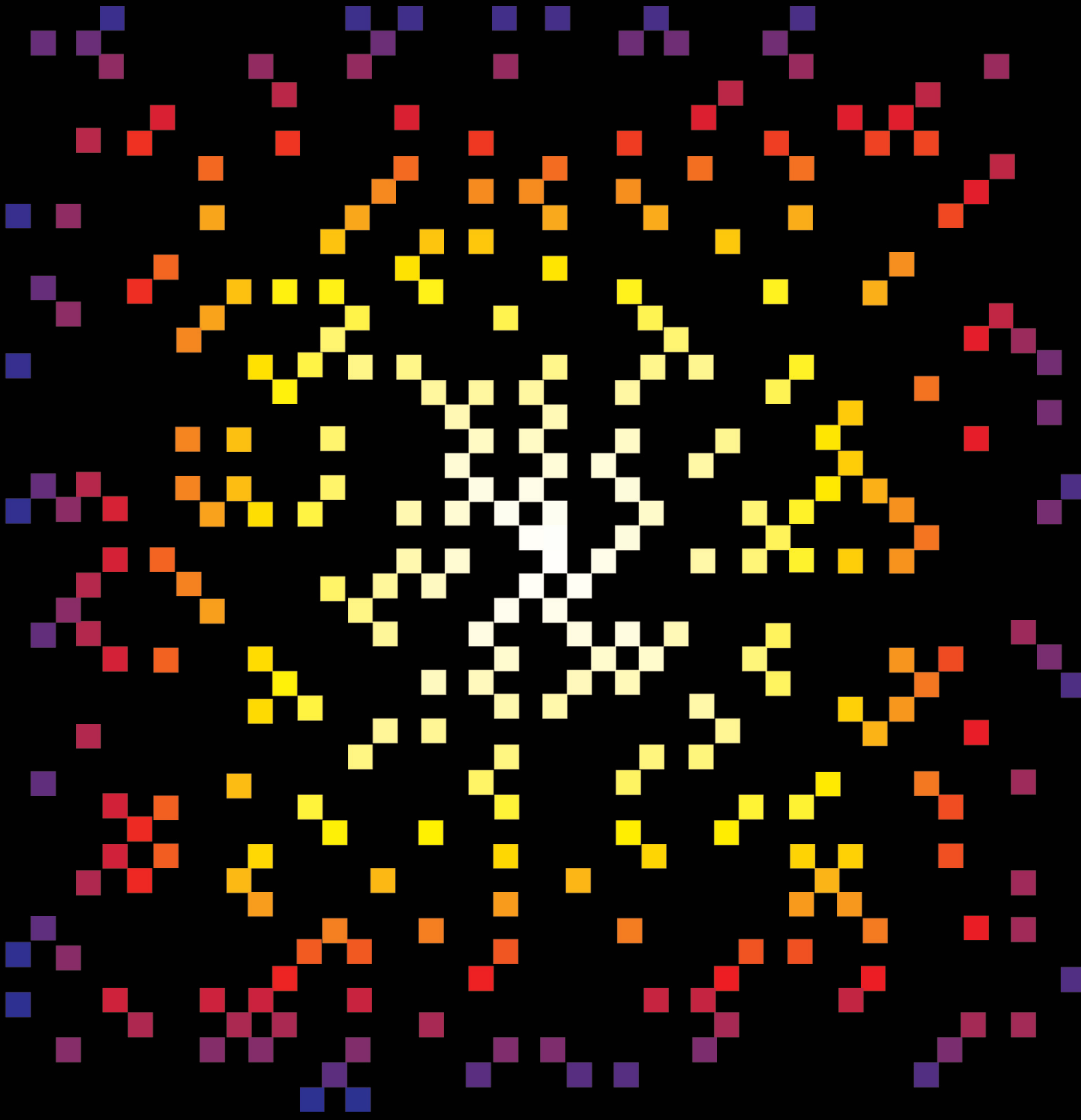
Introducción a la teoría de números

FELIPE ZALDÍVAR



FELIPE ZALDÍVAR

obtuvo su licenciatura y maestría en matemáticas en la UNAM y su doctorado en la University of Western Ontario, en Canadá. Actualmente es profesor de matemáticas en la Universidad Autónoma Metropolitana. Sus áreas de interés en matemáticas son la teoría de números y la geometría algebraica.

Sección de Obras de Ciencia y Tecnología

INTRODUCCIÓN A LA TEORÍA DE NÚMEROS

Comité de selección de obras

Dr. Antonio Alonso
Dr. Francisco Bolívar Zapata
Dr. Javier Bracho
Dr. Juan Luis Cifuentes
Dra. Rosalinda Contreras
Dra. Julieta Fierro
Dr. Jorge Flores Valdés
Dr. Juan Ramón de la Fuente
Dr. Leopoldo García-Colín Scherer
Dr. Adolfo Guzmán Arenas
Dr. Gonzalo Halffter
Dr. Jaime Martuscelli
Dra. Isaura Meza
Dr. José Luis Morán-López
Dr. Héctor Nava Jaimes
Dr. Manuel Peimbert
Dr. José Antonio de la Peña
Dr. Ruy Pérez Tamayo
Dr. Julio Rubio Oca
Dr. José Sarukhán
Dr. Guillermo Soberón
Dr. Elías Trabulse

FELIPE ZALDÍVAR

Introducción a la teoría de números

FONDO DE CULTURA ECONÓMICA

Primera edición, 2012
Primera edición electrónica, 2014

Diseño de portada: Laura Esponda Aguilar

Carretera Picacho-Ajusco, 227; 14738 México, D. F.
www.fondodeculturaeconomica.com
Empresa certificada ISO 9001:2008

Comentarios:
editorial@fondodeculturaeconomica.com
Tel. (55) 5227-4672

ISBN 978-607-16-1881-8 (PDF)

Hecho en México • *Made in Mexico*

ÍNDICE GENERAL

Prólogo 11
Matemáticos cuyos trabajos se han citado en el libro 12
Lista de símbolos más usados 14

I. El teorema fundamental de la aritmética 15
I.1 Divisibilidad 16
I.1.1 El algoritmo de la división 17
I.1.2 Máximo común divisor 18
Ejercicios 21
I.2 Primos y factorización única 23
I.2.1 Factorización única 24
I.2.2 La criba de Eratóstenes 25
I.2.3 Infinitud del conjunto de primos 26
Ejercicios 27
I.3 El algoritmo de Euclides 28
I.3.1 El mínimo común múltiplo 30
Ejercicios 32
I.4 Ecuaciones diofantinas lineales 32
Ejercicios 35

II. Congruencias y criptografía 37
II.1 Congruencias y aritmética modular 38
II.1.1 Congruencias lineales 42
Ejercicios 47
II.2 Los teoremas de Fermat y Euler 50
Ejercicios 54
II.3 Criptografía 55
II.3.1 Cifradores de substitución 56
II.3.2 Criptoanálisis 57
Ejercicios 59
II.4 El criptosistema RSA 60
II.4.1 Un algoritmo para calcular potencias y raíces . 65
II.4.2 Un algoritmo para escribir un decimal en binario 67

II.4.3 Eficiencia de algunos algoritmos 67
II.4.4 Eficiencia del algoritmo de Euclides 67
II.4.5 Eficiencia del cálculo de potencias y raíces módulo n 69
II.4.6 Firmas digitales 71
Ejercicios 72

III. Números perfectos y funciones multiplicativas 73
III.1 Primos de Mersenne y números perfectos 73
Ejercicios 76
III.2 Funciones multiplicativas 77
III.2.1 Divisores y la función φ de Euler 77
III.2.2 El número de divisores de un entero 79
III.2.3 La función μ de Möbius 79
Ejercicios 82

IV. Raíces primitivas y logaritmos discretos 84
Ejercicios 85
IV.1 Raíces primitivas 86
Ejercicios 87
IV.1.1 Raíces primitivas para primos 88
El exponente de $U(\mathbb{Z}/n)$ 89
Ejercicios 90
IV.1.2 Raíces primitivas para potencias de primos . . . 90
Raíces primitivas para potencias de 2 92
Ejercicios 93
IV.1.3 Raíces primitivas en el caso general 93
Resumen 94
Ejercicios 95
IV.2 Logaritmos discretos 95
Ejercicios 96
IV.3 El intercambio de claves de Diffie-Hellman 96
IV.4 El criptosistema de ElGamal 97
IV.4.1 Firmas digitales usando ElGamal 100
Ejercicios 101

V. Residuos cuadráticos 102
V.1 Residuos cuadráticos y raíces primitivas módulo p 104
V.1.1 ¿Cuándo es -1 un RC módulo p? 106
V.1.2 ¿Cuándo es 2 un RC módulo p? 109

Ejercicios 112
V.2 La ley de reciprocidad cuadrática 113
V.2.1 Congruencias cuadráticas en general 119
V.2.2 Primos de la forma $ak + b$ 122
Ejercicios 123
V.3 El símbolo de Jacobi 124
Ejercicios 129
V.4 El criptosistema de Rabin 130
Ejercicios 132

VI. Sumas de potencias 134
VI.1 Ternas Pitagóricas 136
VI.1.1 Una excursión por la geometría 138
Ejercicios 141
VI.2 La conjetura de Fermat 142
Ejercicios 144
VI.3 Sumas de dos cuadrados 145
Ejercicios 148
VI.4 Sumas de cuatro cuadrados 148
VI.4.1 Sumas de tres cuadrados 150
Ejercicios 151
VI.4.2 Un poco de historia 151

VII. La ecuación de Pell y aproximaciones diofantinas 154
VII.1 La ecuación de Pell: un caso particular 155
VII.1.1 El problema del ganado de Arquímedes 156
VII.1.2 El caso particular de la ecuación de Pell 160
Ejercicios 163
VII.2 La ecuación de Pell: el caso general 164
Ejercicios 166
VII.3 Aproximación diofantina y la ecuación de Pell 167
VII.3.1 La existencia de soluciones de la ecuación de Pell 170
Ejercicios 175

VIII. Números congruentes y curvas elípticas 177
VIII.1 Números congruentes 178
VIII.1.1 Puntos racionales en ciertas cúbicas 181
Ejercicios 181
VIII.2 Curvas elípticas 181

VIII.2.1 La operación de grupo 182
VIII.2.2 El teorema de Mordell 186
VIII.2.3 Reducción módulo p 187
Ejercicios 190
VIII.3 La función L de Hasse-Weil de una curva elíptica 190

Bibliografía 195
Índice analítico y onomástico 197

PRÓLOGO

> Dicho esto, rogó al bachiller que, si era poeta, le hiciese merced de componerle unos versos que tratasen de la despedida que pensaba hacer de su señora Dulcinea del Toboso, y que advirtiese que en el principio de cada verso había de poner una letra de su nombre, de manera que al fin de los versos, juntando las primeras letras, se leyese: *Dulcinea del Toboso*.
>
> El bachiller respondió que puesto que él no era de los famosos poetas que había en España, que decían que no eran sino tres y medio, que no dejaría de componer los tales metros, aunque hallaba una dificultad grande en su composición, a causa que las letras que contenían el nombre eran diez y siete; y que si hacía cuatro castellanas de a cuatro versos, sobraría una letra; y si de a cinco, a quien llaman décimas o redondillas, faltaban tres letras; pero con todo eso, procuraría [...] lo mejor que pudiese [...]
>
> *Don Quijote,* Segunda Parte, capítulo IV.

Los números primos —como el 17, el cual Cervantes finge que el bachiller debe factorizar— han fascinado a los matemáticos desde tiempos remotos: por el teorema fundamental de la aritmética, son los átomos a partir de los cuales se construyen todos los otros enteros mayores que 1 y exhiben propiedades que atraen y maravillan al mismo tiempo, y su aparente sencillez esconde riquezas que se asoman apenas uno se detiene a reflexionar un poco; por ejemplo, aun cuando existe un número infinito de ellos, en ocasiones suelen estar tan dispersos que hay lagunas arbitrariamente grandes de enteros que carecen de primos, y es muy fácil visualizar algunas propiedades acerca de los primos y sin embargo puede ser muy difícil dar una demostración de estas propiedades; por ejemplo, una vista rápida a una tabla de los primeros números primos, digamos menores que 1000, puede mostrar que en ocasiones los primos aparecen separados por la distancia mínima de 2, por ejemplo 11 y 13, 17 y 19, 29 y 31 (a estos pares de números primos se los llama *primos gemelos*), y uno puede conjeturar que hay un número infinito de éstos; no obstante, a pesar de progresos recientes, todavía no se tiene una demostración de esta conjetura. La historia

de la teoría de números, o aritmética superior, está llena de conjeturas como la anterior, muy fáciles de hacer, aparentemente naturales, elementales en su formulación y cuya demostración está en muchas ocasiones todavía muy lejana.

La atracción que ejerce la teoría de números sólo es comparable a la de la geometría, ambas con raíces profundas en la historia (y prehistoria) de la humanidad. En todas las culturas del norte y sur, este y oeste, impulsados por simple curiosidad, aparentemente sin conexión con la "realidad" o "aplicaciones", en tablillas con textos cuneiformes de los babilonios o en palimpsestos de origen griego, en estelas mayas o en manuscritos árabes, matemáticos cuyo nombre recuerda la historia o cuyas aportaciones sobreviven al olvido de sus nombres adornan la historia de nuestra ciencia.

Este libro es una introducción elemental a la aritmética superior. Comenzando con una discusión sencilla de la noción de divisibilidad, siguiendo la tradición clásica introduce las propiedades elementales de las congruencias, de las cuales deduce inmediatamente una aplicación a la criptografía de clave pública; después estudia en forma económica, y con un lenguaje cercano al de la teoría de grupos, la existencia de raíces primitivas, para dar luego una aplicación al intercambio de claves y al criptosistema de ElGamal, ambos basados en la noción de logaritmo discreto. Después, se estudian congruencias cuadráticas, entre ellas, la ley de reciprocidad cuadrática de Gauss, Legendre y Euler, y se aplica lo anterior al criptosistema de Rabin. El libro incluye un estudio de algunas ecuaciones diofantinas de grado 2 y 3, desde la existencia y caracterización de ternas pitagóricas hasta la formulación de la conjetura de Fermat, para finalizar con un estudio de la llamada ecuación de Pell. El último capítulo es una introducción elemental a la aritmética de las curvas elípticas.

Una novedad del libro es que, en muchos casos y cuando es necesario para algún tipo de aplicaciones, las demostraciones se dan en tal forma que permitan su algoritmización casi inmediata, lo cual se refuerza en ocasiones dando el pseudocódigo correspondiente, de tal manera que el estudiante con interés en aspectos computacionales pueda escribir un programa para la implementación de estos algoritmos. Sin llegar a la exageración, se han incluido algunas aplicaciones de interés relativamente reciente, tales como los criptosistemas de RSA, ElGamal y Rabin que sólo requieren los conocimientos incluidos en el texto.

Matemáticos cuyos trabajos se han citado en el libro

1) Pitágoras, *circa* 572–500 a.C.

2) Euclides, 323-285 a.C.

3) Arquímedes, 287-212 a.C.
4) Eratóstenes, *circa* 230 a.C.
5) Diofanto, *circa* 250 d.C.
6) Sun-Tzu, *circa* siglo v d.C.
7) Al-Khwarizmi, *circa* 780-850
8) Bhaskara (1114–*circa* 1185)
9) Leonardo de Pisa, Fibonacci, *circa* 1175–1250
10) Claude Bachet, 1587–1638
11) Marin Mersenne, 1588–1648
12) Pierre de Fermat, 1601–1655
13) Bernard Frenicle de Bessy, *circa* 1602–1675
14) John Pell, 1611–1683
15) Leonhard Euler, 1707–1783
16) Joseph-Louis Lagrange, 1736–1813
17) Adrien-Marie Legendre, 1752–1833
18) Sophie Germain, 1776–1831
19) Carl Friedrich Gauss, 1777–1855
20) August Ferdinand Möbius, 1790–1868
21) Gabriel Lamé, 1795–1870
22) Carl Gustav Jacobi, 1804–1851
23) Peter Lejeune Dirichlet, 1805–1859
24) Joseph Liouville, 1809–1882
25) Ernst Eduard Kummer, 1810–1893
26) Edouard Lucas, 1842–1891
27) Axel Thue, 1863–1922
28) Emil Artin, 1898–1962
29) Jean-Pierre Serre, 1926–
30) Barry Mazur, 1937–
31) Gerhard Frey, 1944–
32) Kenneth Ribet, 1948–
33) Andrew Wiles, 1953–

Lista de símbolos más usados

Símbolo	*Significado*	*Página(s) en que se introduce*
$a \mid b$	a divide a b	16
$a \nmid b$	a no divide a b	16
$\mathrm{mcd}(a, b)$	máximo común divisor de a y b	20
$\mathrm{mcm}[a, b]$	mínimo común múltiplo de a y b	30
$a \equiv b \pmod{m}$	a es congruente con b módulo m	37
$\varphi(m)$	función de Euler	52
$\sigma(n)$	suma de los divisores de n	74
$\tau(n)$	número de divisores de n	79
$\mu(n)$	función de Möbius	79
$\mathrm{ord}_n(a)$	orden de a módulo n	84
$\log_g(a)$	logaritmo discreto de a	95
$\left(\frac{a}{p}\right)$	símbolo de Legendre	105
$\lceil x \rceil$	menor entero mayor o igual que x	114
$\lfloor x \rfloor$	mayor entero menor o igual a x	67 y 114
$\left(\frac{a}{m}\right)$	símbolo de Jacobi	124
$\mathbb{Z}$	el anillo de enteros	15
$\mathbb{Z}/m$	el anillo de enteros módulo m	38
$(\mathbb{Z}/n)^* = U(\mathbb{Z}/n)$	grupo de unidades módulo n	41 y 84

I. EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

El conjunto $\mathbb{Z}$ de los números enteros positivos y negativos

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

es un *anillo conmutativo con uno*, es decir, se tienen dos operaciones, llamadas *suma* y *producto*, que satisfacen:

i) *Propiedades de la suma*

1) La suma es *asociativa*, esto es, $a+(b+c) = (a+b)+c$, para cualesquiera $a, b, c \in \mathbb{Z}$.

2) Existe un *neutro aditivo*, a saber el $0 \in \mathbb{Z}$, que satisface

$$a + 0 = a = 0 + a$$

para todo $a \in \mathbb{Z}$.

3) Cada entero $a \in \mathbb{Z}$ tiene un *inverso aditivo*, $-a \in \mathbb{Z}$, que satisface

$$a + (-a) = 0 = -a + a$$

para todo $a \in \mathbb{Z}$.

4) La suma es *conmutativa*, es decir, para cualesquiera $a, b \in \mathbb{Z}$, se tiene que

$$a + b = b + a.$$

ii) *Propiedades del producto*

1) El producto es *asociativo*, esto es, $a(bc) = (ab)c$, para cualesquiera $a, b, c \in \mathbb{Z}$.

2) Existe un *neutro multiplicativo*, a saber el $1 \in \mathbb{Z}$, que satisface

$$a \cdot 1 = a = 1 \cdot a$$

para todo $a \in \mathbb{Z}$.

3) El producto es *conmutativo*, es decir, para cualesquiera $a, b \in \mathbb{Z}$, se tiene que

$$ab = ba.$$

III) *Distributividad.* La suma y el producto de $\mathbb{Z}$ se relacionan mediante la igualdad

$$a(b+c) = ab + ac,$$

para todos los $a, b, c \in \mathbb{Z}$.

Como en todo anillo conmutativo con uno, se satisfacen las propiedades siguientes —las propiedades *3)* y *4)* se conocen como las reglas de los signos—:

1) $a \cdot 0 = 0$, para todo $a \in \mathbb{Z}$.

2) $(-1) \cdot a = -a$, para todo $a \in \mathbb{Z}$.

3) $a(-b) = -(ab) = (-a)b$.

4) $(-a)(-b) = ab$.

Más aún, el anillo $\mathbb{Z}$ es un *dominio entero*, es decir, si $ab = 0$ en $\mathbb{Z}$, entonces $a = 0$ o $b = 0$. Esta propiedad es equivalente a la *ley de cancelación para el producto* en $\mathbb{Z}$: si $ab = ac$ en $\mathbb{Z}$ y $a \neq 0$, entonces $b = c$. Observe que en $\mathbb{Z}$ los únicos enteros que tienen *inverso multiplicativo* son los enteros ± 1 (vea el ejercicio 5).

I.1 Divisibilidad

Si a, b son dos enteros, con $b \neq 0$, diremos que *a divide* a b, o que b es *múltiplo* de a, si existe otro entero q tal que $b = aq$. Usaremos la notación $a \mid b$ para decir que a divide a b y también diremos que a es un *divisor* de b. Si a no divide a b lo denotaremos mediante $a \nmid b$. La relación de divisibilidad satisface las propiedades siguientes:

Proposición I.1.

1) $a \mid a$, *para todo* $a \neq 0$.

2) Si $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$.

3) $1 \mid a$, *para todo* $a \in \mathbb{Z}$.

4) $a \mid 0$, *para todo* $a \neq 0$.

5) Si $a \mid b$, *entonces* $a \mid br$, *para cualquier* $r \in \mathbb{Z}$.

6) Si $a \mid b$ *y* $a \mid c$, *entonces* $a \mid b + c$.

7) Si $a \mid b$ y $a \mid c$, entonces a divide a cualquier combinación lineal de b y c, esto es, $a \mid br + cs$, para cualesquiera $r, s \in \mathbb{Z}$.

8) Si $a \mid b$, entonces $a \mid -b$, $-a \mid b$, $-a \mid -b$, $|a| \mid |b|$.

9) Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.

10) Si $a \mid 1$, entonces $a = \pm 1$.

11) Si $a \mid b$, entonces $|a| \leq |b|$.

Demostración. Sólo probaremos algunas de estas propiedades, dejando las demás como un ejercicio. Para *1),* se tiene que $a = a \cdot 1$. Para *2),* $b = aq$ y $c = bq'$ implican que $c = bq' = aqq'$ y así $a \mid c$. □

I.1.1 El algoritmo de la división

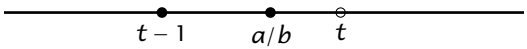
Un *algoritmo* es una lista de instrucciones[1] para hacer algo; por ejemplo, una serie de instrucciones para calcular un número.

Teorema I.2 (Algoritmo de la división). *Si $a, b \in \mathbb{Z}$, con $b \neq 0$, entonces existen $q, r \in \mathbb{Z}$ tales que*

$$a = bq + r \quad \text{con } 0 \leq r < |b|.$$

El entero q se llama el *cociente* y el entero r es el *residuo* de dividir a entre b.

Demostración. Podemos suponer que a y b no son negativos. Considere el cociente a/b y localícelo en la recta real:



y sea M el conjunto de números enteros mayores que a/b. Por el principio del buen orden, M tiene un elemento menor, digamos t (en la gráfica anterior, t es el número que está a la derecha de a/b). Entonces, $t - 1 \leq a/b < t$. Pongamos $q = t - 1$ de tal forma que $q \leq a/b < q + 1$ y así $bq \leq a < (q+1)b$. Sea $r := a - bq$. Entonces, las desigualdades anteriores dicen que $0 \leq r < b$ y así $a = bq + r$ con $0 \leq r < b$, como se quería. □

[1]La palabra *algoritmo*, tiene una etimología híbrida: originalmente es de origen árabe, relacionada con el matemático Al-Juarismi, quien introdujo la numeración decimal de los indios en la cultura árabe del siglo ix. Al llegar estos conocimientos a la Europa de la Edad Media, se llamó *algoristas* a quienes calculaban usando los *números arábigos* en notación decimal. Por esas cosas extrañas que suelen suceder, la palabra algoritmo *aparenta llevar* la raíz griega *arithmos*, que significa *número*.

Advierta que si al dividir a entre b, en $a = bq + r$ el residuo $r = 0$, entonces $b|a$.

Observación. Así como está formulado y demostrado, el teorema anterior no parece un algoritmo. Sin embargo, podríamos pensar en cómo hacerlo con un conjunto de instrucciones de la manera siguiente:

1. Divida a entre b para obtener el racional a/b.
2. Escoja el entero q que esté a la izquierda o sea igual a a/b.
3. Ponga $r := a - bq$.

Note que si se tiene una calculadora y los números con que trabajamos no son muy grandes, lo anterior es bastante rápido. Sin embargo, estas "instrucciones" no son de mucha ayuda si queremos programarlas en una computadora. En el libro VII de los *Elementos* de Euclides, la proposición VII.2 describe un algoritmo para dividir a entre b, cada uno de cuyos pasos es una resta:

1. Si $a < b$, ponga $q = 0$ y $r = a$; es decir, $a = b \cdot 0 + a$.
2. Si $a \geq b$, calcule $a - b$. Si $a - b < a$, ponga $q := 1$ y $r := a - b$, por lo que $a = b \cdot 1 + (a - b)$.
3. Si $a - b \geq b$, calcule $(a - b) - b = a - 2b$. Si $a - 2b < a$, ponga $q := 2$ y $r := a - 2b$, y así $a = b \cdot 2 + (a - 2b)$.
4. Si $a - 2b \geq b$, calcule $(a - 2b) - b = a - 3b$, etcétera; esto es, continúe restando b hasta que el resultado sea menor que a, es decir, hasta que $a - qb < a$, y entonces ponga $r := a - qb$.

I.1.2 Máximo común divisor

Sean a, b dos enteros. Note que el 1 siempre es un divisor común de a y de b por I.1.3 (p. 16).[2] Si $a = 0 = b$, entonces por I.1.4 cualquier entero distinto de 0 divide a a y a b y por lo tanto no existe un entero mayor que divida a ambos. Supongamos entonces que alguno de a o b es $\neq 0$. Sin perder generalidad supongamos que $a \neq 0$. Por I.1.11 (p. 17), todos los divisores de a son $\leq |a|$ y así el conjunto de divisores comunes de a y de b tiene un elemento mayor. A este entero se le llama *máximo común divisor* de a y b. Una forma equivalente

[2] Si no se hace referencia explícita a capítulo o sección, estos números (I.1, I.1.4, etc.) remiten a teoremas, proposiciones, etc., los cuales tienen numeración corrida dentro del capítulo; por ejemplo, a la Proposición I.1 ha seguido el Teorema I.2. Por supuesto, I.1.4 remite al inciso 4 de la Proposición I.1.

de definirlo es, a saber, el *máximo común divisor* de a y b es un entero g que satisface:

1) $g \mid a$ y $g \mid b$, es decir, g es *divisor común*.

2) Si d es cualquier entero tal que $d \mid a$ y $d \mid b$, entonces $d \mid g$. Note que I.1.11 (p. 17) implica que en este caso $|d| \leq |g|$, por lo que g es, en efecto, el divisor común máximo.

Teorema I.3. *Sean a, b dos enteros con uno de ellos distinto de cero; entonces:*

1) Existe un máximo común divisor de a y b y es la menor combinación lineal positiva de a y b, es decir, es de la forma $as + bt$, con $s, t \in \mathbb{Z}$.

2) Cualesquiera dos máximos comunes divisores de a y b difieren sólo por el signo.

Demostración.

1) Como $a \neq 0$ o $b \neq 0$, entonces el conjunto de combinaciones lineales distintas de cero de a, b

$$M = \{as + bt \ : \ s, t \in \mathbb{Z}\} - \{0\}$$

es no vacío y, de hecho, eligiendo s, t adecuadamente se tiene que existen combinaciones lineales $as + bt > 0$, por lo que $M \cap \mathbb{N} \neq \varnothing$. Por el principio del buen orden existe un elemento menor g en $M \cap \mathbb{N}$, es decir, g es la menor combinación lineal positiva de a, b, digamos $g = as_0 + bt_0$. Mostraremos ahora que $g \mid a$ y $g \mid b$. Basta mostrar que $g \mid a$, y para esto supongamos que $g \nmid a$. Entonces $g \nmid -a$, y por lo tanto $g \nmid |a|$, por lo que podemos suponer, sin perder generalidad, que $a > 0$, y como $g \nmid a$ entonces $a = gq + r$ con $0 < r < g$. Observamos ahora que $r = a - gq \in M$, ya que

$$r = a - gq = a - (as_0 + bt_0)q = a(1 - s_0q) + b(-t_0q),$$

esto es, r es combinación lineal de a, b, y como $r > 0$ entonces r es una combinación lineal positiva de a, b, lo cual contradice la minimalidad de g, puesto que $r < g$. Se debe entonces tener que $g \mid a$ e igualmente $g \mid b$.

Finalmente, si $d \in \mathbb{Z}$ es tal que $d \mid a$ y $d \mid b$, entonces d divide a cualquier combinación lineal de a y b, en particular $d \mid g$. Hemos así probado que g es un máximo común divisor de a y b.

2) Si g_1 y g_2 son dos máximos comunes divisores de a y b, por la propiedad 2 de la definición, $g_1 \mid g_2$ y $g_2 \mid g_1$. Por I.1.9 (p. 17) se sigue que $g_1 = \pm g_2$. □

La propiedad *2* del teorema anterior nos dice que al elegir el signo positivo se tiene un único máximo común divisor de a y b, al que denotaremos mediante $g = \mcd(a, b)$. La propiedad *1* del teorema anterior nos dice que el mcd de a y b se puede escribir de la forma

$$g = \mcd(a, b) = as + bt,$$

con $s, t \in \mathbb{Z}$ y, de hecho, g es el menor entero positivo que es combinación lineal de a y b. En la sección I.3 (p. 28) daremos un algoritmo, bastante eficiente, para calcular el mcd de dos enteros.

Dados dos enteros a, b, se dice que son *coprimos* si $\mcd(a, b) = 1$. El resultado siguiente[3] es de fundamental importancia para la aritmética.

Teorema I.4 (Euclides). *Si $a \mid bc$ y $\mcd(a, b) = 1$, entonces $a \mid c$.*

Demostración. Como $1 = \mcd(a, b)$, entonces 1 es combinación lineal de a y b, digamos $1 = as + bt$. Multiplicando esta igualdad por c queda

$$c = c \cdot 1 = acs + bct,$$

donde $a \mid acs$ y $a \mid bct$, ya que $a \mid bc$. Se sigue que $a \mid acs + bct = c$, esto es, $a \mid c$ como se quería. □

En este teorema es importante observar que la condición $\mcd(a, b) = 1$ es necesaria, pues sin esta condición puede suceder que $a \mid bc$ y sin embargo $a \nmid b$ y $a \nmid c$. Por ejemplo, $6 \mid (2)(3)$ pero $6 \nmid 2$ y $6 \nmid 3$.

Un entero p se dice que es *primo* si $p \neq 0, \pm 1$ y si sus únicos divisores son ± 1 y $\pm p$. Se acostumbra considerar sólo los primos positivos, ya que si p es primo entonces $-p$ también es primo. Cuando dos primos difieren a lo más por un signo, decimos que son *asociados*. Así, todo primo es asociado de un primo positivo. Un entero a que no sea 0 o ± 1 y que no sea primo se llama *compuesto*.

Ejemplo 1. Los enteros siguientes son primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

Nuestro objetivo ahora es probar que todo entero $a > 1$ se puede factorizar, en forma esencialmente única, como producto de primos, de tal forma que los enteros primos son como los ladrillos a partir de los cuales se construyen todos los otros enteros. La parte importante de este resultado es la unicidad de la factorización, y para probar esto necesitaremos una consecuencia del teorema I.4 de Euclides, para lo cual precisamos también el cálculo siguiente:

[3] Véase la proposición 30 del libro VII de los *Elementos* de Euclides.