



Introducción a la teoría de números

FELIPE ZALDÍVAR

Nueva edición

SECCIÓN DE OBRAS DE CIENCIA Y TECNOLOGÍA

INTRODUCCIÓN A LA TEORÍA DE NÚMEROS

FELIPE ZALDÍVAR

Introducción a la teoría de números



FONDO DE CULTURA ECONÓMICA

Primera edición, 2012

Segunda edición, 2024

[Segunda edición en libro electrónico, 2024]

Zaldívar, Felipe

Introducción a la teoría de números / Felipe Zaldívar. — 2ª ed. — México : FCE, 2024

198 p. ; ilus. ; 23 × 17 cm — (Colec. Ciencia y Tecnología)

ISBN 978-607-16-8281-9

1. Números, Teoría de 2. Matemáticas I. Ser. II. t.

LC QA241

Dewey 512.7 Z324i

Distribución mundial

D. R. © 2012, Fondo de Cultura Económica

Carretera Picacho-Ajusco, 227; 14110 Ciudad de México

www.fondodeculturaeconomica.com

Comentarios: editorial@fondodeculturaeconomica.com

Tel.: 55-5227-4672

Diseño de portada: Laura Esponda Aguilar

Se prohíbe la reproducción total o parcial de esta obra, sea cual fuere el medio, sin la anuencia por escrito del titular de los derechos.

ISBN 978-607-16-8281-9 (rústico)

ISBN 978-607-16-8411-0 (electrónico-pdf)

Impreso en México • *Printed in Mexico*

ÍNDICE GENERAL

PRÓLOGO	9
Matemáticos cuyos trabajos se han citado en el libro	10
Lista de símbolos más usados	12
I. EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA	13
I.1 Divisibilidad	14
I.1.1 El algoritmo de la división	15
I.1.2 Máximo común divisor	16
<i>Ejercicios</i>	19
I.2 Primos y factorización única	21
I.2.1 Factorización única	22
I.2.2 La criba de Eratóstenes	23
I.2.3 Infinitud del conjunto de primos	24
<i>Ejercicios</i>	25
I.3 El algoritmo de Euclides	26
I.3.1 El mínimo común múltiplo	28
<i>Ejercicios</i>	30
I.4 Ecuaciones diofantinas lineales	30
<i>Ejercicios</i>	33
II. CONGRUENCIAS Y CRIPTOGRAFÍA	35
II.1 Congruencias y aritmética modular	36
II.1.1 Congruencias lineales	40
<i>Ejercicios</i>	45
II.2 Los teoremas de Fermat y Euler	48
<i>Ejercicios</i>	52
II.3 Criptografía	53
II.3.1 Cifradores de substitución	54
II.3.2 Criptoanálisis	55
<i>Ejercicios</i>	57
II.4 El criptosistema RSA	58
II.4.1 Un algoritmo para calcular potencias y raíces	63
II.4.2 Un algoritmo para escribir un decimal en bi- nario	65

II.4.3	Eficiencia de algunos algoritmos	65
II.4.4	Eficiencia del algoritmo de Euclides	65
II.4.5	Eficiencia del cálculo de potencias y raíces módulo n	67
II.4.6	Firmas digitales	69
	<i>Ejercicios</i>	70
III.	NÚMEROS PERFECTOS Y FUNCIONES MULTIPLICATIVAS	71
III.1	Primos de Mersenne y números perfectos	71
	<i>Ejercicios</i>	74
III.2	Funciones multiplicativas	75
III.2.1	Divisores y la función φ de Euler	75
III.2.2	El número de divisores de un entero	77
III.2.3	La función μ de Möbius	77
	<i>Ejercicios</i>	80
IV.	RAÍCES PRIMITIVAS Y LOGARITMOS DISCRETOS	82
	<i>Ejercicios</i>	83
IV.1	Raíces primitivas	84
	<i>Ejercicios</i>	85
IV.1.1	Raíces primitivas para primos	86
	El exponente de $U(\mathbb{Z}/n)$	87
	<i>Ejercicios</i>	88
IV.1.2	Raíces primitivas para potencias de primos	88
	Raíces primitivas para potencias de 2	90
	<i>Ejercicios</i>	91
IV.1.3	Raíces primitivas en el caso general	91
	Resumen	92
	<i>Ejercicios</i>	93
IV.2	Logaritmos discretos	93
	<i>Ejercicios</i>	94
IV.3	El intercambio de claves de Diffie-Hellman	94
IV.4	El criptosistema de ElGamal	95
	IV.4.1 Firmas digitales usando ElGamal	98
	<i>Ejercicios</i>	99
V.	RESIDUOS CUADRÁTICOS	100
V.1	Residuos cuadráticos y raíces primitivas módulo p	102
V.1.1	¿Cuándo es -1 un RC módulo p ?	104
V.1.2	¿Cuándo es 2 un RC módulo p ?	107

<i>Ejercicios</i>	110
V.2 La ley de reciprocidad cuadrática	111
V.2.1 Congruencias cuadráticas en general	117
V.2.2 Primos de la forma $ak + b$	120
<i>Ejercicios</i>	121
V.3 El símbolo de Jacobi	122
<i>Ejercicios</i>	127
V.4 El criptosistema de Rabin	128
<i>Ejercicios</i>	130
VI. SUMAS DE POTENCIAS	132
VI.1 Ternas Pitagóricas	134
VI.1.1 Una excursión por la geometría	136
<i>Ejercicios</i>	139
VI.2 La conjetura de Fermat	140
<i>Ejercicios</i>	142
VI.3 Sumas de dos cuadrados	143
<i>Ejercicios</i>	146
VI.4 Sumas de cuatro cuadrados	146
VI.4.1 Sumas de tres cuadrados	148
<i>Ejercicios</i>	149
VI.4.2 Un poco de historia	149
VII. LA ECUACIÓN DE PELL Y APROXIMACIONES DIOFANTINAS	152
VII.1 La ecuación de Pell: un caso particular	153
VII.1.1 El problema del ganado de Arquímedes	154
VII.1.2 El caso particular de la ecuación de Pell	158
<i>Ejercicios</i>	161
VII.2 La ecuación de Pell: el caso general	162
<i>Ejercicios</i>	164
VII.3 Aproximación diofantina y la ecuación de Pell	165
VII.3.1 La existencia de soluciones de la ecuación de Pell	168
<i>Ejercicios</i>	173
VIII. NÚMEROS CONGRUENTES Y CURVAS ELÍPTICAS	175
VIII.1 Números congruentes	176
VIII.1.1 Puntos racionales en ciertas cúbicas	179
<i>Ejercicios</i>	179
VIII.2 Curvas elípticas	179

VIII.2.1	La operación de grupo	180
VIII.2.2	El teorema de Mordell	184
VIII.2.3	Reducción módulo p	185
	<i>Ejercicios</i>	188
VIII.3	Curvas elípticas y criptografía	188
VIII.3.1	La cota de Hasse	190
VIII.3.2	Criptosistemas de curvas elípticas	192
	Diffie-Hellman para curvas elípticas	192
	ElGamal para curvas elípticas	192
	<i>Ejercicio</i>	194
	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

<i>Símbolo</i>	<i>Significado</i>	<i>Página(s) en que se introduce</i>
$a b$	a divide a b	14
$a \nmid b$	a no divide a b	14
$\text{mcd}(a, b)$	máximo común divisor de a y b	18
$\text{mcm}[a, b]$	mínimo común múltiplo de a y b	28
$a \equiv b \pmod{m}$	a es congruente con b módulo m	35
$\varphi(m)$	función de Euler	50
$\sigma(n)$	suma de los divisores de n	72
$\tau(n)$	número de divisores de n	77
$\mu(n)$	función de Möbius	77
$\text{ord}_n(a)$	orden de a módulo n	82
$\log_g(a)$	logaritmo discreto de a	93
$\left(\frac{a}{p}\right)$	símbolo de Legendre	103
$[x]$	menor entero mayor o igual que x	112
$\lfloor x \rfloor$	mayor entero menor o igual a x	65 y 112
$\left(\frac{a}{m}\right)$	símbolo de Jacobi	122
$\mathbb{Z}$	el anillo de enteros	13
$\mathbb{Z}/m$	el anillo de enteros módulo m	36
$(\mathbb{Z}/n)^* = U(\mathbb{Z}/n)$	grupo de unidades módulo n	39 y 82

I. EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

EL CONJUNTO $\mathbb{Z}$ de los números enteros positivos y negativos

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

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, 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 $a|b$ 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) $a|a$, para todo a .

2) Si $a|b$ y $b|c$, entonces $a|c$.

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

4) $a|0$, para todo a .

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

6) Si $a|b$ y $a|c$, entonces $a|b + c$.

- 7) Si $a|b$ y $a|c$, entonces a divide a cualquier combinación lineal de b y c , esto es, $a|br + cs$, para cualesquiera $r, s \in \mathbb{Z}$.
- 8) Si $a|b$, entonces $a|-b$, $-a|b$, $-a|-b$, $|a| \mid |b|$.
- 9) Si $a|b$ y $b|a$, entonces $a = \pm b$.
- 10) Si $a|1$, entonces $a = \pm 1$.
- 11) Si $a|b$, 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 $a|c$. $\square$

I.1.1 El algoritmo de la división

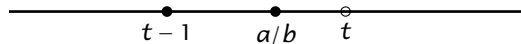
Un *algoritmo* es una lista de instrucciones¹ para hacer algo; por ejemplo, una serie de instrucciones para calcular un número.

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. $\square$

¹La 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 $b \mid a$.

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. 14).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. 15), 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

²Si 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) $g|a$ y $g|b$, es decir, g es *divisor común*.
- 2) Si d es cualquier entero tal que $d|a$ y $d|b$, entonces $d|g$. Note que I.1.11 (p. 15) 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 $M \cap \mathbb{N} \neq \emptyset$. 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 $g|a$ y $g|b$. Basta mostrar que $g|a$, 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 $g|a$ e igualmente $g|b$.

Finalmente, si $d \in \mathbb{Z}$ es tal que $d|a$ y $d|b$, entonces d divide a cualquier combinación lineal de a y b , en particular $d|g$. 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, $g_1|g_2$ y $g_2|g_1$. Por I.1.9 (p. 15) se sigue que $g_1 = \pm g_2$. $\square$

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 $g = \text{mcd}(a, b)$. La propiedad 1 del teorema anterior nos dice que el mcd de a y b se puede escribir de la forma

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

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. 26) daremos un algoritmo, bastante eficiente, para calcular el mcd de dos enteros.

Dados dos enteros a, b , se dice que son *coprimos* si $\text{mcd}(a, b) = 1$. El resultado siguiente³ es de fundamental importancia para la aritmética.

TEOREMA I.4 (Euclides). Si $a \mid bc$ y $\text{mcd}(a, b) = 1$, entonces $a \mid c$.

Demostración. Como $1 = \text{mcd}(a, b)$, 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. $\square$

En este teorema es importante observar que la condición $\text{mcd}(a, b) = 1$ 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:

³El teorema I.4 no se encuentra como tal en los *Elementos* de Euclides, donde la proposición 30 del libro VII sólo considera un caso importante del teorema I.4, a saber, el corolario I.6 siguiente.

LEMA I.5. Si p es primo, entonces $\text{mcd}(p, a) = \begin{cases} 1 & \text{si } p \nmid a \\ p & \text{si } p \mid a \end{cases}$

Demostración. Los únicos divisores positivos de p son 1 y p , así que $\text{mcd}(p, a)$ es 1 o p . Se sigue que $p \nmid a \Leftrightarrow \text{mcd}(p, a) = 1$ y $p \mid a \Leftrightarrow \text{mcd}(p, a) = p$. $\square$

Usando este lema, junto con el teorema de Euclides I.4, se tiene la consecuencia⁴ siguiente:

COROLARIO I.6. Si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

Demostración. Si $p \mid a$ no hay nada que probar. Supongamos entonces que $p \nmid a$; entonces, por el lema anterior $\text{mcd}(p, a) = 1$ y como $p \mid ab$, por el teorema de Euclides se sigue que $p \mid b$. $\square$

El resultado siguiente, nos será útil en varias instancias, en particular para concluir que el algoritmo de descriptamiento de RSA en efecto recupera el mensaje original.

COROLARIO I.7. Si $a \mid c$ y $b \mid c$ y $\text{mcd}(a, b) = 1$, entonces $ab \mid c$.

Demostración. Escribamos $c = aq$ y $c = bq'$. Como $1 = as + bt$, multiplicando por c obtenemos

$$c = acs + bct = abq's + baqt = ab(q's + qt)$$

y así $ab \mid c$. $\square$

Ejercicios

- 1) Demuestre las propiedades listadas en la página 14 antes de sección I.1.
- 2) Demuestre las propiedades faltantes en la proposición I.1 (p. 14).
- 3) Demuestre la unicidad del cociente q y del residuo r en el algoritmo de la división.
- 4) Demuestre que si a divide cualquier combinación lineal $bs + ct$ de b y c , entonces $a \mid b$ y $a \mid c$.
- 5) Demuestre que si $a \mid 1$ entonces $a = \pm 1$.
- 6) Use inducción (sobre n) para probar que si $a \mid b_1, \dots, a \mid b_n$ y $r_1, \dots, r_n \in \mathbb{Z}$ son arbitrarios, entonces $a \mid (r_1b_1 + \dots + r_nb_n)$.

⁴Como se ha dicho en la nota previa, este corolario es, de hecho, la proposición 30 del libro VII de los *Elementos* de Euclides.