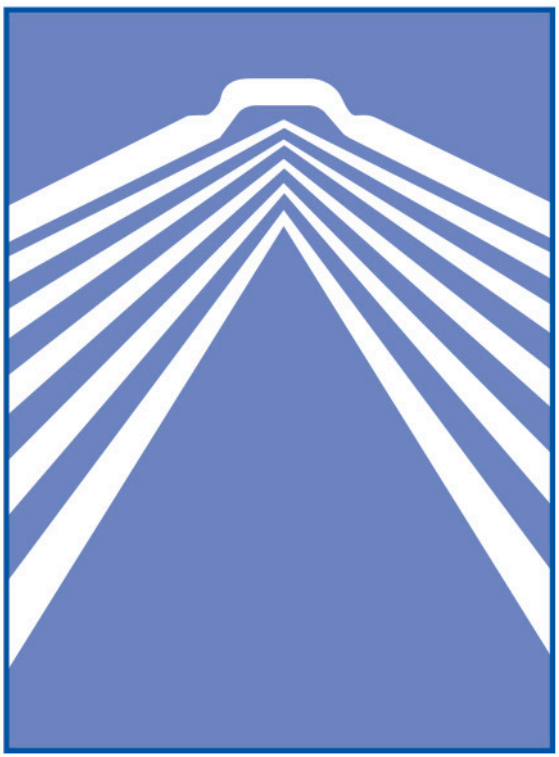
3.ª edición

MATEMÁTICAS BÁSICAS
PARA EL ACCESO A LA UNIVERSIDAD



Ángel Manuel Ramos del Olmo
José María Rey Cabezas

PIRÁMIDE

3.ª edición

MATEMÁTICAS BÁSICAS
PARA EL ACCESO
A LA UNIVERSIDAD

ÁNGEL MANUEL RAMOS DEL OLMO
JOSÉ MARÍA REY CABEZAS
PROFESORES TITULARES DE UNIVERSIDAD EN EL INSTITUTO DE MATEMÁTICA INTERDISCIPLINAR
Y EN EL DEPARTAMENTO DE ANÁLISIS MATEMÁTICO Y MATEMÁTICA APLICADA
DE LA UNIVERSIDAD COMPLUTENSE DE MADRID

3.ª edición

MATEMÁTICAS BÁSICAS
PARA EL ACCESO A LA UNIVERSIDAD

EDICIONES PIRÁMIDE

COLECCIÓN «CIENCIA Y TÉCNICA»

Edición en versión digital

Está prohibida la reproducción total o parcial de este libro electrónico, su transmisión, su descarga, su descompilación, su tratamiento informático, su almacenamiento o introducción en cualquier sistema de repositorio y recuperación, en cualquier forma o por cualquier medio, ya sea electrónico, mecánico, conocido o por inventar, sin el permiso expreso escrito de los titulares del copyright.

© Ángel Manuel Ramos del Olmo y José María Rey Cabezas, 2018
© Tercera edición electrónica publicada por Ediciones Pirámide (Grupo Anaya, S. A.), 2018
Para cualquier información pueden dirigirse a piramide_legal@anaya.es
Juan Ignacio Luca de Tena, 15. 28027 Madrid
Teléfono: 91 393 89 89
www.edicionespiramide.es
ISBN digital: 978-84-368-3954-8

A mis padres,
Alejandra del Olmo y Claudio Ramos.
In memoriam.

A mi hermana,
Mari Gracia.

Índice

Prefacio a la tercera edición 15

Notación general 17

I ÁLGEBRA Y GEOMETRÍA 19

1. Introducción al número real 21
- 1.1. Introducción 21
- 1.2. Números naturales, enteros, racionales y primos 21
- 1.3. Números irracionales. Números reales 40
- 1.4. Radicales y potencias. Operaciones 46
- 1.5. Problemas 53
- 1.6. Soluciones 55

2. Ecuaciones algebraicas 57
- 2.1. Introducción 57
- 2.2. Polinomios de una variable real. Álgebra de polinomios. Binomio de Newton 57
- 2.3. Ecuaciones algebraicas de primer y segundo orden 69
- 2.4. Problemas 76
- 2.5. Soluciones 78

3. Matrices y determinantes 79
- 3.1. Introducción 79
- 3.2. Matrices. Álgebra de matrices 79
- 3.3. Determinantes. Propiedades 86
- 3.4. Cálculo de la inversa de una matriz 91
- 3.5. Problemas 94
- 3.6. Soluciones 96

4. Sistemas de ecuaciones lineales 99
- 4.1. Introducción 99
- 4.2. Motivación 100
- 4.3. Expresión matricial de los sistemas de ecuaciones lineales 101

© Ediciones Pirámide

4.4. Método de Gauss . . . 114
4.5. Problemas . . . 116
4.6. Soluciones . . . 120

5. El espacio vectorial . . . 123
5.1. Introducción . . . 123
5.2. El espacio vectorial. Subespacios vectoriales . . . 123
5.3. Dependencia e independencia lineal. Bases . . . 126
5.4. Problemas . . . 135
5.5. Soluciones . . . 136

6. Espacios afines en el plano ($\mathbb{R}^2$) y en el espacio ($\mathbb{R}^3$) . . . 139
6.1. Introducción . . . 139
6.2. Vectores. Espacio afín. Sistemas de referencia . . . 139
6.3. Ecuaciones de las rectas en el plano y de las rectas y los planos en el espacio . . . 146
6.3.1. Rectas en el plano . . . 146
6.3.2. Rectas en el espacio . . . 148
6.3.3. Planos en el espacio . . . 151
6.4. Problemas de incidencia y paralelismo . . . 154
6.4.1. Posiciones relativas de dos rectas en el plano . . . 154
6.4.2. Condición para que tres puntos de $\mathbb{R}^2$ estén alineados . . . 155
6.4.3. Condición para que tres puntos de $\mathbb{R}^3$ estén alineados . . . 156
6.4.4. Posiciones relativas de dos rectas en el espacio . . . 157
6.4.5. Condición para que cuatro puntos espaciales sean coplanarios . . . 161
6.4.6. Posiciones relativas de dos planos en el espacio . . . 162
6.4.7. Posiciones relativas de recta y plano en el espacio . . . 165
6.4.8. Posiciones relativas de tres planos en el espacio . . . 167
6.5. Problemas . . . 174
6.6. Soluciones . . . 176

7. Trigonometría . . . 177
7.1. Introducción . . . 177
7.2. Resultados básicos de Geometría . . . 177
7.3. Razones elementales . . . 192
7.4. Razones del ángulo suma, del ángulo doble y del ángulo mitad . . . 201
7.5. Resolución de triángulos . . . 210
7.6. Problemas . . . 212
7.7. Soluciones . . . 214

8. El espacio euclídeo . . . 217
8.1. Introducción . . . 217
8.2. Producto escalar. Módulo de un vector. Ángulo de dos vectores . . . 217
8.3. Aplicaciones del producto escalar . . . 227
8.3.1. Distancia entre dos puntos . . . 227
8.3.2. Vector perpendicular a una recta en $\mathbb{R}^2$ . . . 227
8.3.3. Distancia de un punto a una recta en $\mathbb{R}^2$ . . . 228

© Ediciones Pirámide

8.3.4. Distancia entre dos rectas en $\mathbb{R}^2$ 230
8.3.5. Vector perpendicular a un plano en $\mathbb{R}^3$ 230
8.3.6. Distancia de un punto a un plano en $\mathbb{R}^3$ 231
8.3.7. Ángulo que forman dos rectas 233
8.3.8. Ángulo que forman dos planos 234
8.3.9. Ángulo que forman una recta y un plano 235
8.4. Producto vectorial 236
8.5. Aplicaciones del producto vectorial 240
8.5.1. Vector perpendicular a dos rectas 240
8.5.2. Vector director de una recta dada por la intersección de dos planos 240
8.5.3. Área de un paralelogramo y de un triángulo 241
8.5.4. Distancia de un punto a una recta 242
8.6. Producto mixto 243
8.7. Aplicaciones del producto mixto 244
8.7.1. Volumen de un paralelepípedo y de un tetraedro 244
8.7.2. Distancia entre dos rectas paralelas y distintas 245
8.7.3. Distancia entre dos rectas que se cruzan 245
8.8. Doble producto vectorial 247
8.9. Aplicaciones del doble producto vectorial 250
8.9.1. Proyección de un vector sobre un plano 250
8.10. Problemas 252
8.11. Soluciones 255

9. Cónicas 257
9.1. Introducción 257
9.2. Descripción geométrica de las cónicas 257
9.3. Ecuaciones de la circunferencia 259
9.4. Ecuaciones de la elipse 270
9.5. Ecuaciones de la hipérbola 287
9.6. Ecuaciones de la parábola 305
9.7. Notas finales sobre cónicas 322
9.8. Problemas 327
9.9. Soluciones 330

II ANÁLISIS **333**

10. Sucesiones. Convergencia 335
10.1. Introducción 335
10.2. Progresiones. Sucesiones de números reales 335
10.2.1. Progresiones aritméticas 335
10.2.2. Progresiones geométricas 337
10.2.3. Sucesiones de números reales 341
10.3. Límites de sucesiones 341
10.4. El número e 353

© Ediciones Pirámide

10.5. Problemas . . . 357
10.6. Soluciones . . . 359

11. Funciones reales . . . 361
11.1. Introducción . . . 361
11.2. Algunos conceptos básicos sobre funciones . . . 362
11.3. Funciones exponenciales y logarítmicas . . . 371
11.4. Funciones hiperbólicas . . . 380
11.5. Funciones elementales . . . 383
11.6. Límites de funciones . . . 384
11.7. Continuidad . . . 398
11.8. Problemas . . . 406
11.9. Soluciones . . . 410

12. Números complejos . . . 413
12.1. Introducción . . . 413
12.2. Definición, conceptos básicos y representación gráfica . . . 413
12.3. Operaciones con números complejos en forma binómica . . . 417
12.3.1. Suma y resta de números complejos . . . 417
12.3.2. Producto y cociente de números complejos . . . 419
12.3.3. Potencias de números complejos . . . 421
12.4. Forma polar de un número complejo . . . 423
12.4.1. Módulo y argumento de un número complejo . . . 423
12.4.2. Paso de la forma polar a la forma binómica . . . 427
12.5. Operaciones con números complejos en forma polar . . . 428
12.5.1. Producto de números complejos . . . 428
12.5.2. Cociente de números complejos . . . 429
12.5.3. Potencias de números complejos . . . 429
12.5.4. Raíces de números complejos . . . 430
12.6. Forma exponencial de un número complejo . . . 434
12.7. Problemas . . . 436
12.8. Soluciones . . . 438

13. Derivadas . . . 439
13.1. Introducción . . . 439
13.2. Derivada de una función en un punto . . . 440
13.3. Cálculo de derivadas. Regla de la cadena . . . 447
13.4. Teoremas de Rolle y del Valor Medio . . . 462
13.5. Fórmula de Taylor . . . 468
13.6. Problemas . . . 479
13.7. Soluciones . . . 483

© Ediciones Pirámide

14. Aplicaciones de las derivadas 485
14.1. Introducción 485
14.2. Cálculo de límites. Regla de L'Hôpital 485
14.3. Crecimiento y decrecimiento de una función. Máximos y mínimos relativos 488
14.4. Concavidad y convexidad de una función. Puntos de inflexión 491
14.5. Representación gráfica de funciones 498
14.6. Problemas de máximos y mínimos 506
14.7. Problemas 509
14.8. Soluciones 511

15. Cálculo integral. Integrales indefinidas 517
15.1. Introducción 517
15.2. Primitivas e integrales indefinidas. Métodos elementales de integración 517
15.2.1. Primitivas e integrales indefinidas 517
15.2.2. Métodos elementales de integración 521
15.3. Integración de funciones racionales 529
15.4. Otros métodos de integración 536
15.5. Problemas 538
15.6. Soluciones 540

16. Cálculo integral. Integrales definidas 543
16.1. Introducción 543
16.2. Integral definida. Propiedades elementales. Regla de Barrow 543
16.3. Aplicaciones de la integral definida 553
16.3.1. Cálculo de áreas de figuras planas 553
16.3.2. Longitud de arco de una curva 556
16.3.3. Volumen de un cuerpo de revolución (eje paralelo al eje de abscisas) 557
16.3.4. Volumen de un cuerpo de revolución (eje paralelo al eje de ordenadas) 559
16.3.5. Área de una superficie de revolución (eje paralelo al eje de abscisas) 562
16.4. Problemas 565
16.5. Soluciones 567

III ESTADÍSTICA Y PROBABILIDAD **569**

17. Análisis combinatorio 571
17.1. Introducción 571
17.2. Permutaciones. Variaciones 571
17.3. Combinaciones 574
17.4. Problemas 578
17.5. Soluciones 580

© Ediciones Pirámide

18. Estadística descriptiva unidimensional 581
18.1. Introducción 581
18.2. Medidas numéricas descriptivas 582
18.2.1. Generalidades 582
18.2.2. Medidas de tendencia central 584
18.2.3. Medidas de dispersión 586
18.2.4. Medidas de posición 592
18.3. Introducción a la Estadística Inferencial 593
18.4. Representaciones gráficas de datos 595
18.5. Problemas 603
18.6. Soluciones 607

19. Probabilidad 609
19.1. Introducción 609
19.2. Álgebra de sucesos 610
19.3. Nociones y propiedades elementales de Probabilidad 614
19.4. Probabilidad condicionada 620
19.5. Teorema de la Probabilidad Total. Teorema de Bayes 626
19.6. Problemas 629
19.7. Soluciones 631

Bibliografía **633**

Índice alfabético **637**

© Ediciones Pirámide

Prefacio a la tercera edición

Al entrar a la universidad los alumnos a menudo se encuentran con material que los profesores suponen que ya han estudiado y con la típica frase "esto ya lo habéis dado, ¿verdad?", con el correspondiente estrés que esto puede generar. Visto desde el otro lado, el profesor suele oír quejas de algunos estudiantes que afirman que no han recibido clases sobre este material en la enseñanza secundaria y/o en Bachillerato. Además, si se le ocurre formular la pregunta antes citada, en muchas ocasiones verá a los estudiantes removiéndose en sus asientos, miradas perdidas, un murmullo general ... y algunas tímidas respuestas.

En este volumen estudiantes y profesores encontrarán una recopilación exhaustiva y autocontenida de material matemático de un nivel previo a la universidad que les puede servir para preparar pruebas de acceso a la universidad, como texto de base para (al menos) el primer año de carrera y como texto al que recurrir, a modo enciclopédico, cuando lo precisen, sin necesidad de buscar en una colección de libros y apuntes de cursos anteriores.

El origen de esta obra es un curso de preparación para pruebas de acceso a la universidad que los autores estuvieron impartiendo durante varios años en la Universidad Complutense de Madrid. Es en ese curso y en la interacción con sus estudiantes, cuando surge la idea inicial de su redacción. Además, la experiencia de los autores como profesores en clases de Matemáticas en los primeros años de universidad y como correctores en las actuales pruebas de acceso les ha permitido observar las carencias y necesidades a nivel matemático de muchos estudiantes, lo cual ha terminado de perfilar y completar la mencionada idea inicial. En este sentido este libro puede ser de especial ayuda como texto básico de referencia en los cursos introductorios de Matemáticas Básicas que, cada vez más, se imparten en los grados de Ciencias, Tecnología e Ingeniería.

Comparada con la segunda, esta tercera edición tiene una cantidad apreciable de cambios, en términos de presentación de ideas y nuevo material, incluyendo nuevas secciones, demostraciones, gráficas, problemas, soluciones y entradas del índice alfabético situado al final del texto, así como la corrección de pequeñas erratas.

© Ediciones Pirámide

El texto está dividido en tres partes en las que se clasifican los contenidos que se abordan: I) Álgebra y Geometría, II) Análisis, III) Estadística y Probabilidad. Cada parte está dividida en varios capítulos en los que se desgranan los principales resultados y la mayoría de sus demostraciones, junto con numerosas gráficas y ejemplos ilustrativos. Se ha considerado conveniente incluir, para los lectores interesados, demostraciones de la mayoría de los resultados presentados, a pesar de que muchas de ellas no suelen aparecer en los libros de enseñanza secundaria y de Bachillerato. Cada capítulo termina con una sección de problemas y otra sección con las correspondientes soluciones, lo que permitirá al lector comprobar el grado de conocimiento que ha adquirido sobre los contenidos de cada capítulo.

La parte de Álgebra y Geometría se inicia con la introducción a los números reales y se termina con el estudio del espacio euclídeo y de las cónicas, pasando previamente por capítulos sobre sistemas de ecuaciones lineales, trigonometría ...

La parte de Análisis se inicia con el estudio de las sucesiones y su convergencia y de las funciones reales de variable real. Se continúa con un capítulo sobre números complejos (que muchos estudiantes de universidad afirman desconocer, a pesar de su enorme utilidad e importancia ... y de ser, supuestamente, parte de los contenido de Bachillerato). Se termina con la parte dedicada al Cálculo (derivadas e integrales) y sus aplicaciones.

Por último, la parte de Estadística y Probabilidad está dividida en tres capítulos. En el primero se estudia el Análisis Combinatorio, y muestra técnicas para facilitar el recuento de casos o cosas, necesario en muchas situaciones científicas y cotidianas. El segundo capítulo está dedicado a la Estadística Descriptiva (sólo en el caso unidimensional) y presenta herramientas que permitan asimilar de una forma razonable grandes cantidades de información. En el tercer y último capítulo se presentan las nociones básicas de la teoría de la Probabilidad, con el objetivo de disponer de herramientas básicas que sirvan a la hora de intentar sacar conclusiones sobre lo que puede ocurrir en fenómenos o experimentos aleatorios.

Agradecemos a nuestros lectores de la primera edición los comentarios y sugerencias que nos han hecho llegar, la mayoría de los cuales han sido tenidos en cuenta al realizar esta tercera edición. Nuevos comentarios y sugerencias (que se pueden enviar por correo electrónico a las direcciones angel@mat.ucm.es y jrey@mat.ucm.es) para mejorar el libro serán bienvenidos.

Á. M. Ramos y J. M. Rey
Abril de 2018

© Ediciones Pirámide

Notación general

Recopilamos, a continuación, una serie de notaciones matemáticas que se emplean a lo largo de todo el texto:

- La expresión "$a \in X$" denota que *a es un elemento del conjunto X* o, dicho de otra forma, que *a pertenece al conjunto X*. La expresión "$a \notin X$" denota que *a no es un elemento del conjunto X* o, dicho de otro modo, que *a no pertenece al conjunto X*.

- El símbolo "$\Rightarrow$" es una forma abreviada de escribir *implica* (o *es una condición suficiente para*). Es decir, si se verifica la afirmación (proposición) que se escribe a su izquierda, entonces se verifica la afirmación (proposición) que se escribe a su derecha. El símbolo "$\not\Rightarrow$" es una forma abreviada de escribir *no implica*.

- El símbolo "$\Leftarrow$" es una forma abreviada de escribir *es implicado por* (o *es una condición necesaria para*). Es decir, si se verifica la afirmación (proposición) que se escribe a su derecha, entonces se verifica la afirmación (proposición) que se escribe a su izquierda. El símbolo "$\not\Leftarrow$" es una forma abreviada de escribir *no es implicado por*.

- El símbolo "$\Leftrightarrow$" es una forma abreviada de escribir *si, y sólo si*. Es decir, la afirmación (proposición) que se escribe a su izquierda es cierta si, y sólo si, es cierta la afirmación (proposición) que se escribe a su derecha. En otras palabras, ambas proposiciones son equivalentes.

- El símbolo "$\cup$" denota *unión de conjuntos*, de forma que la expresión "$a \in A \cup B$" significa que "$a \in A$ o $a \in B$". La expresión $\bigcup_{i=1}^{n} A_i$ es una forma abreviada de expresar la unión $A_1 \cup A_2 \cup \cdots \cup A_n$.

- El símbolo "$\cap$" denota *intersección de conjuntos*, de modo que "$a \in A \cap B$" es una expresión que significa que "$a \in A$ y $a \in B$". La expresión $\bigcap_{i=1}^{n} A_i$ es una forma abreviada de expresar la intersección $A_1 \cap A_2 \cap \cdots \cap A_n$.

© Ediciones Pirámide

- El símbolo "$\emptyset$" denota el *conjunto vacío*, es decir, el conjunto que no contiene elementos.
- El símbolo (cuantificador) "$\forall$" es una forma abreviada de escribir *para todo* o *para cualesquiera* de los elementos que vienen a continuación.
- El símbolo (cuantificador) "$\exists$" es una forma abreviada de escribir *existe*.
- La expresión "$A \subset B$" denota que el conjunto A *está contenido* en el conjunto B. La expresión "$A \not\subset B$" denota que el conjunto A *no está contenido* en el conjunto B.
- La expresión "$A \supset B$" denota que el conjunto A *contiene* al conjunto B. La expresión "$A \not\supset B$" denota que el conjunto A *no contiene* al conjunto B.
- El símbolo "$\sum$" denota *sumatorio* y se utiliza para expresar, de forma abreviada, sumas. Así, por ejemplo, la expresión $\displaystyle\sum_{i=1}^{4} a_i$ es una manera abreviada de expresar $a_1 + a_2 + a_3 + a_4$ y, en general, $\displaystyle\sum_{i=1}^{n} a_i$ es una forma abreviada de expresar la suma $a_1 + a_2 + \cdots + a_n$ para cualquier $n \in \mathbb{N}$ y $a_i \in \mathbb{R}$.
- Los símbolos $<$, $>$, $=$, $\leq$ y $\geq$ denotan, respectivamente, *menor que, mayor que, igual a, menor o igual que* y *mayor o igual que* cuando se comparan números reales. Por ejemplo, $x \leq 7$ denota que el número real x es *menor o igual que* 7.
- Los símbolos "$\simeq$" o "$\approx$" denotan *aproximadamente igual*.
- La expresión $0 < a \ll 1$ significa que a es un número positivo que es "muy pequeño" frente a 1.
- La expresión "∂P" denota el *grado* del polinomio $P(x)$.
- La expresión "$\dot{n}$" denota el conjunto formado por los múltiplos del número natural n.
- El símbolo $\square$ indica el final de una demostración o el final del enunciado de una definición, teorema, observación, ejemplo ...

© Ediciones Pirámide

Parte I

ÁLGEBRA Y GEOMETRÍA

1 Introducción al número real

1.1. Introducción

En este capítulo se presentan los *números reales* como una generalización, sin entrar en detalles rigurosos, de los *números naturales*, *enteros*, *racionales* e *irracionales*. Se introducirá el concepto de *divisibilidad* de números naturales, su *factorización en números primos* y las nociones de *máximo común divisor* y *mínimo común múltiplo*. Esto servirá para calcular la *forma irreducible* de un número racional.

Se mostrarán también algunas de las propiedades de los tipos de números estudiados y las operaciones que se pueden hacer entre ellos. En particular, las *raíces* y las *potencias*. Además se introducirán los conjuntos de números que definen los *intervalos abiertos* y *cerrados*.

Éste es, sin duda, un capítulo que proporciona herramientas matemáticas básicas, como son los números y las operaciones que se pueden hacer con ellos, y es fundamental para el desarrollo de los siguientes capítulos.

1.2. Números naturales, enteros, racionales y primos

Definición 1.1 El conjunto de los *números naturales* es el formado por los "números de contar" y se representa

$$\mathbb{N} = \{1, 2, 3 \ldots\}. \quad \square$$

Observación 1.1 Al sumar o multiplicar dos números naturales siempre se obtiene otro número natural. Esto no siempre ocurre al restarlos o dividirlos. Ejemplo:

$$5 + 7 = 12 \in \mathbb{N},\ 5 \times 7 = 35 \in \mathbb{N},\ 5 - 7 = -2 \notin \mathbb{N},\ \frac{5}{7} \notin \mathbb{N}. \quad \square$$

© Ediciones Pirámide

Ejemplo 1.1 Los números naturales sirven para "contar". Por ejemplo uno puede contar cuántas manzanas tiene (por ejemplo, 6) y restar las que se haya comido pasados unos días (por ejemplo, 4). Como siempre se va a comer menos manzanas de las que tenía, la resta efectuada $(6-4)$ siempre volverá a dar un número natural (2), que es el número de manzanas que nos quedan. □

Definición 1.2 Un número a elevado a la potencia $n \in \mathbb{N}$ es

$$a^n = a\times \overset{n)}{\cdots} \times a.$$

En esta definición a puede ser un número natural (es decir $a \in \mathbb{N}$) o de cualquier otro tipo de números de los que vamos a definir más adelante. □

Ejemplo 1.2 $5^2 = 5 \times 5 = 25$, $2^4 = 2 \times 2 \times 2 \times 2 = 16$. □

La división entre números naturales no siempre da como resultado un número natural, por lo que se define de una forma especial los casos en los que sí ocurre:

Definición 1.3 Un número natural $n \in \mathbb{N}$ es *divisible* por otro número natural $m \in \mathbb{N}$, y se denota $m|n$, cuando el cociente entre n y m (que expresamos como $\frac{n}{m}$) es un número natural. Es decir, cuando $\frac{n}{m} \in \mathbb{N}$. En esta situación también se dice que m *divide a* n, m *es un divisor de* n o n *es un múltiplo de* m. □

Ejemplo 1.3 6 es divisible por 3, por lo que $3|6$. □

Ahora bien, ¿qué obtenemos cuando restamos dos números naturales?

Definición 1.4 El conjunto de los *números enteros* es el formado por los números naturales, sus opuestos (con el signo menos "$-$") y el cero, y se representa

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

A la vista del Ejemplo 1.1, parece que los números enteros son sólo un invento de los matemáticos que no tiene aplicación en la vida real. El siguiente ejemplo pone de manifiesto que esto no es cierto en absoluto.

Ejemplo 1.4 Los llamados "números rojos" de una cuenta bancaria indican que no sólo no tenemos dinero en esa cuenta, sino que debemos dinero al banco. Dicho de otra forma: tenemos un saldo negativo en nuestra cuenta. □

Observación 1.2 Al sumar, restar o multiplicar dos números enteros, siempre se obtiene otro número entero. Esto no siempre ocurre al dividirlos. Ejemplo:

$$3+4=7 \in \mathbb{Z},\ 3-4=-1 \in \mathbb{Z},\ \frac{6}{-3}=-2 \in \mathbb{Z},\ \frac{3}{4} \notin \mathbb{Z}.$$ □

© Ediciones Pirámide

La pregunta que nos formulamos a continuación es: ¿qué obtenemos cuando dividimos dos números enteros?

Definición 1.5 El conjunto de los *números racionales* es el formado por los cocientes entre dos enteros que se denominan *numerador* (el de arriba) y *denominador* (el de abajo), siempre que el denominador sea no nulo. Se representa

$$\mathbb{Q} = \left\{ \frac{m}{n} : \ m \in \mathbb{Z} \ \text{y} \ n \in \mathbb{N} \right\}.$$

También suele emplearse la notación m/n para denotar al número racional $\frac{m}{n}$. □

Claramente, los números racionales contienen a los enteros (pues todo número entero $m \in \mathbb{Z}$ puede escribirse como $m = \frac{m}{1} \in \mathbb{Q}$), pero ¿qué representan estos números racionales cuando el resultado no es un número entero?

Si dividimos una tarta en 3 partes iguales, cada parte es un tercio de la tarta. Utilizando los números racionales se dice: $\frac{1}{3}$ de tarta. Dos trozos de la tarta equivalen a dos tercios de tarta. Utilizando los números racionales se dice: $\frac{2}{3}$ de tarta. La tarta completa son tres tercios de tarta (o $\frac{3}{3}$ de tarta). Cuatro tercios de tarta ($\frac{4}{3}$) equivalen a una tarta entera más un tercio de otra, y así sucesivamente. Esto se puede generalizar a cualquier otro número racional. Por ejemplo, el número $\frac{m}{n}$ equivale, en este contexto de tartas, a dividir una tarta en n trozos iguales y coger m trozos de ellos (nótese que si $m > n$, se necesita más de una tarta).

El razonamiento que hemos hecho en términos de una tarta se puede hacer de la misma forma con cualquier otro objeto que sea susceptible de división, por ejemplo una regla de medir. Si un metro lo dividimos en 5 partes iguales, tenemos un quinto de un metro, o $\frac{1}{5}$ de metro. Puesto que 1 metro son 10 dm (decímetros) o 100 cm (centímetros), es fácil observar que $\frac{1}{5}$ de un metro es lo mismo que un $\frac{1}{5}$ de 10 dm o $\frac{1}{5}$ de 100 cm, que es también igual a $\frac{10}{5} = 2$ dm o $\frac{100}{5} = 20$ cm.

Observación 1.3 Es fácil observar que $\frac{1}{3}$ de tarta equivale a $\frac{2}{6}$ de tarta. Basta pensar en una tarta dividida en 6 partes y que al juntar los 6 trozos obtenidos de dos en dos se obtiene una división de la tarta en 3 trozos iguales. Lo que ocurre es que

$$\frac{2}{6} = \frac{2 \times 1}{2 \times 3} = \frac{\cancel{2} \times 1}{\cancel{2} \times 3} = \frac{1}{3}. \quad \square$$

Hemos obtenido, por tanto, una forma sencilla de "simplificar" un número racional: si el numerador y denominador del número racional son divisibles por un número común, se pueden dividir ambos por ese número y se obtiene un número racional equivalente.

Ejemplo 1.5 $\frac{8}{4} = \frac{4}{2}, \frac{63}{36} = \frac{21}{12}.$ □

© Ediciones Pirámide

Con objeto de obtener el número racional equivalente con numerador y denominador más pequeños (*fracción irreducible*), se tienen que dividir el numerador y el denominador por el mayor de los números por el que ambos se puedan dividir (es decir, el mayor de sus divisores comunes, que se conoce como *máximo común divisor* de ambos números).

Ejemplo 1.6 La forma irreducible de los números racionales del Ejemplo 1.5 es

$$\frac{8}{4} = \frac{4 \times 2}{4 \times 1} = \frac{2}{1} = 2, \ \frac{63}{36} = \frac{9 \times 7}{9 \times 4} = \frac{7}{4}. \quad \square$$

Llegados a este punto, cabe preguntarse cómo se calcula el máximo común divisor de dos números enteros a y b cualesquiera ($\mathrm{mcd}(a, b)$).

Proposición 1.1 *Sean $a, b \in \mathbb{N}\backslash\{0\}$ con $a > b$. Si hacemos la división entera de a entre b y escribimos*

$$\begin{array}{r|l} a & b \\ \hline r & c \end{array}$$

o, de forma equivalente,

$$a = cb + r,$$

donde $c \in \mathbb{N}$ es el cociente y $r \in \mathbb{N} \cup \{0\}$, con $r < b$, es el resto de la división, entonces se verifica que, si $r \neq 0$, el conjunto de divisores de a y b coincide con el conjunto de divisores de b y r y, por tanto,

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r).$$

Además, si $r = 0$ entonces $\mathrm{mcd}(a, b) = b$.

DEMOSTRACIÓN. Si A es el conjunto de divisores de a y b y B es el conjunto de divisores de b y r veamos que $A = B$ demostrando, en primer lugar, que $A \subset B$ y, en segundo lugar, que $B \subset A$:

1) Si $m \in A$ y, por tanto, m es un divisor de a y de b, existen $p \in \mathbb{N}$ y $q \in \mathbb{N}$ tales que

$$\left\{ \begin{array}{l} a = mp \\ b = mq \end{array} \right. \Rightarrow \ r = a - cb = m(p - cq) \ \Rightarrow \ m|r \ \Rightarrow \ m \in B.$$

2) Si $n \in B$ y, por tanto, n es un divisor de b y de r, existen $p \in \mathbb{N}$ y $q \in \mathbb{N}$ tales que

$$\left\{ \begin{array}{l} b = np \\ r = nq \end{array} \right. \Rightarrow \ a = cb + r = n(cp + q) \ \Rightarrow \ n|a \ \Rightarrow \ n \in A.$$

© Ediciones Pirámide

Consecuentemente, el máximo de los números del conjunto A, que es el $\mathrm{mcd}(a,b)$, coincide (por tratarse del mismo conjunto) con el máximo de los números del conjunto B, que es el $\mathrm{mcd}(b,r)$.

Por último, como cualquier divisor de a y b es menor o igual que b, se tiene que el $\mathrm{mcd}(a,b) \leq b$. Además, en el caso de que $r = 0$ se verifica que b es un divisor de a (y, obviamente, también de b) por lo que $b \leq \mathrm{mcd}(a,b)$; ambas desigualdades concluyen que, en este caso, $b = \mathrm{mcd}(a,b)$. □

Ejemplo 1.7

a) Puesto que

$$\begin{array}{r|l} 8 & 4 \\ \cline{2-2} 0 & 2 \end{array}$$

se verifica que $\mathrm{mcd}(8,4) = 4$.

b) Teniendo en cuenta que

$$\begin{array}{r|l} 3468 & 468 \\ \cline{2-2} 192 & 7 \end{array}$$

se tiene que

$$\mathrm{mcd}(3468,468) = \mathrm{mcd}(468,192)$$

(véanse los Ejemplos 1.9 y 1.13). □

Algoritmo de Euclides: Sean $a, b \in \mathbb{N}\backslash\{0\}$ con $a > b$. Para calcular el $\mathrm{mcd}(a,b)$ en primer lugar, siguiendo el proceso visto en la Proposición 1.1, hacemos la división entera de a entre b y escribimos

$$a = c_0 b + r_1,$$

donde $c_0 \in \mathbb{N}$ y $r_1 \in \mathbb{N} \cup \{0\}$ con $r_1 < b$. En este punto, como se ha visto en la Proposición 1.1, hay dos posibilidades:

1) Si $r_1 = 0$, entonces $\mathrm{mcd}(a,b) = b$ y se ha terminado el cálculo.

2) En caso contrario, se verifica que $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r_1)$ y repetimos el proceso anterior: hacemos la división entera de b entre r_1 y escribimos

$$b = c_1 r_1 + r_2,$$

donde $c_1 \in \mathbb{N}$ y $r_2 \in \mathbb{N} \cup \{0\}$ con $r_2 < r_1$. De nuevo, pueden presentarse dos casos:

   a) Si $r_2 = 0$, entonces $\mathrm{mcd}(a,b) = r_1$, con lo que se termina el proceso.

   b) En caso contrario, se tiene que $\mathrm{mcd}(a,b) = \mathrm{mcd}(r_1,r_2)$ y volvemos a repetir el proceso anterior, y así sucesivamente.

© Ediciones Pirámide

Nótese que el proceso anterior acaba en un número finito de iteraciones, pues los restos que se van obteniendo están ordenados de forma que

$$r_1 > r_2 > \cdots \geq 0,$$

con lo que en alguna iteración $k \in \mathbb{N}$, con $k \leq b$, el resto será $r_k = 0$ y, por tanto, el máximo común divisor buscado será el último resto no nulo, es decir,

$$\mathrm{mcd}(a, b) = r_{k-1}.$$

Ejemplo 1.8 En el Ejemplo 1.7 se había mostrado que

$$\mathrm{mcd}(3468, 468) = \mathrm{mcd}(468, 192). \tag{1.1}$$

Continuando con el algoritmo de Euclides, como

$$\begin{array}{r|l} 468 & 192 \\ \hline 84 & 2 \end{array} \Rightarrow \mathrm{mcd}(468, 192) = \mathrm{mcd}(192, 84). \tag{1.2}$$

Como

$$\begin{array}{r|l} 192 & 84 \\ \hline 24 & 2 \end{array} \Rightarrow \mathrm{mcd}(192, 84) = \mathrm{mcd}(84, 24). \tag{1.3}$$

Puesto que

$$\begin{array}{r|l} 84 & 24 \\ \hline 12 & 3 \end{array} \Rightarrow \mathrm{mcd}(84, 24) = \mathrm{mcd}(24, 12). \tag{1.4}$$

Finalmente, teniendo en cuenta que

$$\begin{array}{r|l} 24 & 12 \\ \hline 0 & 2 \end{array} \Rightarrow \mathrm{mcd}(84, 24) = \mathrm{mcd}(24, 12) = 12. \tag{1.5}$$

Consecuentemente, las relaciones (1.1), (1.2), (1.3), (1.4) y (1.5) determinan que

$$\mathrm{mcd}(3468, 468) = 12.$$

Una vez visto en detalle el proceso, una forma más rápida de presentarlo y visualizarlo es la siguiente:

$$\begin{aligned} 3468 &= 7 \times 468 + 192 \\ 468 &= 2 \times 192 + 84 \\ 192 &= 2 \times 84 + 24 \\ 84 &= 3 \times 24 + \boxed{12} \\ 24 &= 2 \times 12 + 0. \end{aligned}$$

El máximo común divisor buscado es el último resto no nulo de la tabla anterior, es decir,

$$\mathrm{mcd}(3468, 468) = 12. \quad \square$$

© Ediciones Pirámide

Ejemplo 1.9 Veamos cómo calcular la forma irreducible de $\frac{3468}{468}$. Como se ha visto en el Ejemplo 1.8, se verifica que

$$\mathrm{mcd}(3468, 468) = 12,$$

de donde se obtiene que

$$\frac{3468}{468} = \frac{\frac{3468}{12}}{\frac{468}{12}} = \frac{289}{39}. \quad \square$$

Definición 1.6 Un número natural $n > 1$ es *primo* cuando sólo es divisible por n y por la unidad. Los números naturales mayores que 1 que no son primos se denominan *compuestos*. $\square$

Observación 1.4 Como, por convenio, el número 1 no se considera primo, los primeros números primos son $2, 3, 5, 7, 11, 13 \ldots$ Nótese que el número 1 no es primo ni compuesto. $\square$

Una forma alternativa de obtener el máximo común divisor de dos números naturales (que, en ciertas ocasiones, puede ser más rápida) es utilizar la descomposición de los números como producto de factores primos basada en el *teorema Fundamental de la Aritmética* (véase el Teorema 1.2). Para poder demostrar dicho teorema necesitamos unos resultados previos que vemos a continuación.

Proposición 1.2 (Identidad de Bézout) *Para todo $a \in \mathbb{N}$ y $b \in \mathbb{N}$ se verifica que existen $p \in \mathbb{Z}$ y $q \in \mathbb{Z}$ tales que*

$$\mathrm{mcd}(a, b) = pa + qb.$$

DEMOSTRACIÓN. Con la notación utilizada en el *algoritmo de Euclides* visto anteriormente, se tiene que

$$\begin{cases} a = bc_0 + r_1 & \Rightarrow \quad r_1 = a - bc_0 = \alpha_1 a + \beta_1 b \ \text{ con } \ \alpha_1, \beta_1 \in \mathbb{Z} \\ b = r_1 c_1 + r_2 & \Rightarrow \quad \begin{aligned} r_2 &= b - r_1 c_1 = b - (\alpha_1 a + \beta_1 b) c_1 \\ &= \alpha_2 a + \beta_2 b \ \text{ con } \ \alpha_2, \beta_2 \in \mathbb{Z} \end{aligned} \\ r_1 = r_2 c_2 + r_3 & \Rightarrow \quad \begin{aligned} r_3 &= r_1 - r_2 c_2 = (\alpha_1 a + \beta_1 b) - \big(\alpha_2 a + \beta_2 b\big) c_2 \\ &= \alpha_3 a + \beta_3 b \ \text{ con } \ \alpha_3, \beta_3 \in \mathbb{Z} \end{aligned} \\ \ldots & \\ r_{k-3} = r_{k-2} c_{k-2} + r_{k-1} & \Rightarrow \quad \begin{aligned} r_{k-1} &= r_{k-3} - r_{k-2} c_{k-2} \\ &= \alpha_{k-1} a + \beta_{k-1} b \ \text{ con } \ \alpha_{k-1}, \beta_{k-1} \in \mathbb{Z} \end{aligned} \\ r_{k-2} = r_{k-1} c_{k-1} & \end{cases}$$

y, por tanto,

$$\mathrm{mcd}(a, b) = r_{k-1} = pa + qb \ \text{ con } \ p = \alpha_{k-1} \ \text{ y } \ q = \beta_{k-1} \in \mathbb{Z}. \quad \square$$

© Ediciones Pirámide

Observación 1.5 Dados $a, b \in \mathbb{N}$ hemos probado la existencia de dos números $p, q \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,b) = pa + qb$, pero estos números no son únicos. Por ejemplo,

$$1 = \mathrm{mcd}(2,3) = -2 + 3 = 2 \times 2 - 3.$$

En particular, todas las parejas de la forma $(r,s) = (p + \alpha b, q - \alpha a)$ con $\alpha \in \mathbb{Z}$ verifican

$$\mathrm{mcd}(a,b) = ra + sb. \tag{1.6}$$

En la Proposición 1.3 se demuestra (tomando $c = \mathrm{mcd}(a,b)$) que el conjunto de todas las parejas $(r,s) \in \mathbb{Z}^2$ que cumplen la propiedad (1.6) es

$$\left\{ \left(p + k\,\frac{b}{d}, q - k\,\frac{a}{d} \right) : \; k \in \mathbb{Z} \right\}, \tag{1.7}$$

siendo $d = \mathrm{mcd}(a,b)$. □

Definición 1.7 Se denomina *ecuación diofántica lineal* con dos incógnitas a cualquier ecuación algebraica de la forma $ax + by = c$, con $a, b, c \in \mathbb{Z}$, de la que se buscan soluciones enteras $x, y \in \mathbb{Z}$. □

Proposición 1.3 Sean $a, b, c \in \mathbb{Z}$ y $d = \mathrm{mcd}(a,b)$.

a) La solución general de la ecuación diofántica lineal homogénea $ax + by = 0$ es

$$\left\{ \left(k\frac{b}{d}, -k\frac{a}{d} \right) : \; k \in \mathbb{Z} \right\}$$

(es decir, cualquier solución (X,Y) de la ecuación diofántica $ax + by = 0$ es de la forma $(X,Y) = \left(k\frac{b}{d}, -k\frac{a}{d}\right)$ para algún $k \in \mathbb{Z}$).

b) Una condición necesaria y suficiente para que la ecuación diofántica lineal

$$ax + by = c \tag{1.8}$$

tenga solución es que $d|c$. En caso afirmativo, la solución general de la ecuación diofántica lineal $ax + by = c$ es (1.7), siendo $(p,q) \in \mathbb{Z}^2$ una solución particular de la ecuación diofántica (1.8) (es decir, cualquier solución (X,Y) de la ecuación diofántica (1.8) es de la forma $(X,Y) = \left(p + k\frac{b}{d}, q - k\frac{a}{d}\right)$ para algún $k \in \mathbb{Z}$).

DEMOSTRACIÓN.

a) Si $(X,Y) \in \mathbb{Z}^2$ es una solución arbitraria de $ax + by = 0$ se verifica que $aX + bY = 0$ y, por tanto, $bY = -aX$. Dividiendo por d (para eliminar los divisores comunes) se tiene que

$$b'Y = -a'X \;\text{ siendo }\; a' = \frac{a}{d} \in \mathbb{Z} \;\text{ y }\; b' = \frac{b}{d} \in \mathbb{Z}. \tag{1.9}$$

© Ediciones Pirámide

De la igualdad (1.9) se deduce (aplicando el apartado a) del Lema 1.1 que veremos más adelante) que

$$\begin{cases} b'|(a'X); & \mcd(b',a')=1 \;\Rightarrow\; b'|X \;\Rightarrow\; X=kb' \text{ para algún } k\in\mathbb{Z} \\ a'|(b'Y); & \mcd(a',b')=1 \;\Rightarrow\; a'|Y \;\Rightarrow\; Y=k'a' \text{ para algún } k'\in\mathbb{Z}. \end{cases}$$

Para ver que $k'=-k$ basta sustituir en la igualdad (1.9), ya que

$$b'Y=-a'X \;\Leftrightarrow\; k'a'b'=-ka'b' \;\Leftrightarrow\; k'=-k.$$

De esta forma, se tiene que $(X,Y)=(kb',-ka')=\left(k\frac{b}{d},-k\frac{a}{d}\right)$ con $k\in\mathbb{Z}$.

b) $\boxed{\Rightarrow}$ Si $(x,y)\in\mathbb{Z}^2$ es tal que $ax+by=c$, entonces para cualquier divisor D de a y b (por ejemplo, $D=d$) se verifica que $D|(ax)$ y $D|(by)$ (es decir, D es un divisor de ax y también de by), por lo que $D|(ax+by)$ y, por tanto, $D|c$.

$\boxed{\Leftarrow}$ Si $d|c$ entonces $c'=\frac{c}{d}\in\mathbb{Z}$. Por otra parte, por la identidad de Bézout (véase la Proposición 1.2), existen $p,q\in\mathbb{Z}$ tales que $d=\mcd(a,b)=pa+qb$. De esta forma, tomando $X=pc'$ e $Y=qc'$, se verifica que

$$aX+bY=apc'+bqc'=(ap+bq)c'=d\,\frac{c}{d}=c.$$

Por último, en el caso de que $d|c$, si $(X,Y)\in\mathbb{Z}^2$ es una solución arbitraria de la ecuación diofántica $ax+by=c$, se verifica que

$$aX+bY=c. \tag{1.10}$$

Por otra parte, por ser $(p,q)\in\mathbb{Z}^2$ una solución particular de $ax+by=c$, se tiene que

$$ap+bq=c. \tag{1.11}$$

De esta forma, haciendo la diferencia entre las ecuaciones (1.10) y (1.11), se tiene que

$$a(X-p)+b(Y-q)=0$$

y, por tanto, $(X-p,Y-q)$ es solución de la ecuación homogénea $ax+by=0$. Consecuentemente, por el apartado a), se tiene que existe $k\in\mathbb{Z}$ tal que

$$(X-p,Y-q)=\left(k\frac{b}{d},-k\frac{a}{d}\right),$$

de donde se deduce que

$$(X,Y)=\left(p+k\frac{b}{d},q-k\frac{a}{d}\right). \quad \square$$

© Ediciones Pirámide

Ejemplo 1.10

a) La ecuación diofántica lineal $2x+4y=7$ no tiene solución, ya que $\mathrm{mcd}(2,4)=2$ no divide a 7.

b) La ecuación diofántica lineal $4x+7y=8$ tiene infinitas soluciones enteras, ya que $\mathrm{mcd}(4,7)=1$ divide a 8. Para obtenerlas tenemos que hallar primeramente una solución particular (p,q) que, en la práctica, suele obtenerse a partir de la *identidad de Bézout*. En efecto, a partir de la igualdad

$$1=4\times 2+7\times(-1)$$

y multiplicando la igualdad anterior por 8, se verifica que

$$8=4\times 16+7\times(-8),$$

por lo que una solución particular de esta ecuación diofántica es $(p,q)=(16,-8)$. Por tanto, de acuerdo con la Proposición 1.3, las infinitas soluciones enteras de la ecuación diofántica lineal $4x+7y=8$ son

$$(x,y)=(16+7k,-8-4k)\ \text{ con }\ k\in\mathbb{Z}.\quad \square$$

Observación 1.6 Tanto en la Observación 1.5 como en el Ejemplo 1.10 se ha utilizado la identidad de Bézout sin hacer una deducción de los correspondientes valores de p y q (simplemente se han dado dos parejas que cumplían los requisitos). No obstante, esto se puede hacer de forma sencilla (aunque a veces puede ser tediosa), siguiendo el esquema de la demostración de la Proposición 1.2. Así, en el Ejemplo 1.10, para obtener una identidad de Bézout para los números $a=4$ y $b=7$, se pueden realizar los siguientes cálculos:

$$\begin{cases} 4=7\times 0+4 & \Rightarrow \quad 4=1\times 4+0\times 7\\ 7=4\times 1+3 & \Rightarrow \quad 3=(-1)\times 4+1\times 7\\ 4=3\times 1+1 & \Rightarrow \quad 1=4-((-1)\times 4+1\times 7)=2\times 4+(-1)\times 7\\ 3=1\times 3, & \end{cases}$$

de donde se obtiene que $\mathrm{mcd}(4,7)=1=2\times 4+(-1)\times 7$. $\square$

Definición 1.8 Dos números $p,q\in\mathbb{Z}$ son *primos entre sí* (también se les llama *coprimos* o *relativamente primos*) si $\mathrm{mcd}(p,q)=1$. $\square$

Teorema 1.1 (Bézout) *Para todo $a,b\in\mathbb{N}$ se verifica que*

$$a \text{ y } b \text{ son primos entre sí } \Leftrightarrow \exists\, p,q\in\mathbb{Z} \text{ tales que } 1=pa+qb.$$

© Ediciones Pirámide

DEMOSTRACIÓN.

$\boxed{\Rightarrow}$ Es consecuencia inmediata de la Proposición 1.2.

$\boxed{\Leftarrow}$ Supongamos que $\exists\, p, q \in \mathbb{Z}$ tales que $1 = pa + qb$ y que a y b no son primos entre sí. Veamos que se llega a una contradicción. En efecto, como $\mathrm{mcd}(p, q) \neq 1$, se verifica que existe $n \in \mathbb{N}\backslash\{1\}$ tal que

$$n|a \ \text{ y } \ n|b.$$

Esta propiedad, junto con la hipótesis de que $1 = pa + qb$, determinan que

$$\frac{1}{n} = p\,\frac{a}{n} + q\,\frac{b}{n} \in \mathbb{Z},$$

lo cual no es posible, pues $\frac{1}{n} \notin \mathbb{Z}$. □

Observación 1.7 Si a y b son primos entre sí, por la Proposición 1.3 se verifica que la ecuación diofántica lineal $ax + by = c$ siempre tiene infinitas soluciones enteras (dado que $\mathrm{mcd}(a, b) = 1$ siempre divide a c). □

Lema 1.1 (Lema de Euclides) *Sean* $a, b, p, q \in \mathbb{N}$.

a) Si $\mathrm{mcd}(p, q) = 1$ *y* $q|pa \ \Rightarrow \ q|a$.

b) Si p *es un número primo y* $p|ab \ \Rightarrow \ p|a$ *o* $p|b$.

DEMOSTRACIÓN.

a) Por la *identidad de Bézout* se verifica que existen $n, m \in \mathbb{Z}$ tales que

$$1 = np + mq \ \Rightarrow \ a = npa + mqa.$$

Consecuentemente, como $q|pa$, se verifica que

$$\frac{a}{q} = n\,\frac{pa}{q} + ma \in \mathbb{Z} \ \Rightarrow \ q|a.$$

b) Como p es primo se tiene que el $\mathrm{mcd}(p, a)$ sólo puede ser 1 o p:

i) Si $\mathrm{mcd}(p, a) = p \ \Rightarrow \ p|a$.

ii) Si $\mathrm{mcd}(p, a) = 1$ entonces, como $p|ab$, por el apartado a) se verifica que $p|b$. □

Basándose en el *lema de Euclides* puede demostrarse (no lo hacemos aquí por simplicidad de la exposición, pero se puede probar de forma sencilla por inducción) la siguiente versión generalizada del lema anterior:

© Ediciones Pirámide

Lema 1.2 (Lema de Euclides generalizado) *Sean* $a_1, a_2, \ldots, a_n \in \mathbb{N}$ *y* p *un número primo. Si* p *es divisor del producto* $a_1 a_2 \cdots a_n$ *se verifica que existe* $j \in \{1, 2, \ldots, n\}$ *tal que* $p | a_j$. □

Corolario 1.1 *Si* $p_1, p_2, \ldots, p_n$ *y* $q_1, q_2, \ldots, q_m$ *son números primos tales que*

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

para todo $i \in \{1, 2, \ldots, n\}$ *se verifica que existe* $j \in \{1, 2, \ldots, m\}$ *tal que* $p_i = q_j$ *y, por tanto,* $m = n$.

DEMOSTRACIÓN. Sea $i \in \{1, 2, \ldots, n\}$. Por el *lema de Euclides generalizado*, como $p_i | q_1 q_2 \cdots q_m$, se verifica que existe $j \in \{1, 2, \ldots, m\}$ tal que $p_i | q_j$. Ahora bien, como q_j es primo, sólo es divisible por 1 y por él mismo, por lo que, al ser $p_i \neq 1$, se concluye que $p_i = q_j$. A partir de este hecho se deduce, de forma evidente, que m y n son iguales. □

Definición 1.9 La *factorización en números primos* de un número natural consiste en expresar éste como producto de potencias de números primos. □

Ejemplo 1.11 $75 = 3 \times 25 = 3 \times 5^2$, $300 = 3 \times 100 = 3 \times 4 \times 25 = 3 \times 2^2 \times 5^2$, $5544 = 2^3 \times 3^2 \times 7 \times 11$, $2057 = 11^2 \times 17$. □

Observación 1.8 Una manera sencilla de hallar la factorización en números primos de un numero natural consiste en ir dividiendo por el número primo más pequeño que se pueda, de forma sucesiva, hasta que se obtenga el número 1. Por ejemplo, para el número 924, mostramos a continuación, de manera esquemática, cómo se llevaría a cabo este proceso:

924	2
462	2
231	3
77	7
11	11
1	

lo que nos permite escribir que $924 = 2^2 \times 3 \times 7 \times 11$. □

Teorema 1.2 (Teorema Fundamental de la Aritmética) *Cualquier número natural mayor que* 1 *puede descomponerse como producto de factores primos de forma única, salvo el orden de dichos factores.*

DEMOSTRACIÓN.

1) Cualquier número natural puede descomponerse como producto de factores primos. En efecto, si esto no fuera cierto, existiría un mínimo número natural $m > 1$ que no

© Ediciones Pirámide

puede descomponerse como producto de números primos; este número m no puede ser un primo, porque todo primo se puede descomponer de forma obvia como el producto de un único número primo: él mismo. Así pues, $m = ab$, donde a y b son números naturales mayores que 1 y menores que m. Como m es el mínimo número natural para el que falla el teorema, tanto a como b pueden escribirse como producto de primos. Pero entonces el número $m = ab$ también puede escribirse como producto de primos, lo que es una contradicción.

2) La descomposición como producto de factores primos es única, salvo el orden de dichos factores. En efecto, supongamos que tenemos dos factorizaciones de un número natural $a > 1$

$$p_1 p_2 \cdots p_n = a = q_1 q_2 \cdots q_m,$$

donde $p_1, p_2, \ldots, p_n$ y $q_1, q_2, \ldots, q_m$ son números primos. Entonces, por el Corolario 1.1, se tiene que $m = n$ y que para todo $i \in \{1, 2, \ldots, n\}$ existe $j \in \{1, 2, \ldots, n\}$ tal que $p_i = q_j$, lo que concluye la demostración. □

Observación 1.9 El *teorema Fundamental de la Aritmética* pone de manifiesto la importancia que tienen los números primos, en el sentido de que los demás números naturales se pueden escribir como producto de números primos de forma única, salvo el orden de éstos. Resulta, así, de gran ayuda a la hora de calcular los divisores de un número natural (véase el Problema 1.6). □

Teorema 1.3 (Euclides) *Hay infinitos números primos.*

DEMOSTRACIÓN. Basta probar que si $\{p_1, p_2, \ldots, p_n\}$ es un conjunto finito de números primos entonces existe otro número primo que no está en dicho conjunto. Sea P el producto de todos los números primos del conjunto anterior, es decir, $P = p_1 p_2 \cdots p_n$, y sea $q = P + 1$. Pueden presentarse dos casos:

1) Si q es primo, entonces q es un primo tal que $q \notin \{p_1, p_2, \ldots, p_n\}$.

2) Si q no es primo, entonces, por el *teorema Fundamental de la Aritmética*, existe algún primo p que divide a q. En el caso de que p fuera uno de los primos del conjunto $\{p_1, p_2, \ldots, p_n\}$, se tendría que p dividiría (obviamente) a P a $q = P + 1$ y, por tanto, también a su diferencia $(P + 1) - P = 1$; puesto que ningún primo divide a 1, se concluye que p es un primo tal que $p \notin \{p_1, p_2, \ldots, p_n\}$. □

Proposición 1.4 *Dados $a, b, d \in \mathbb{N}$ se verifica que $d = \mathrm{mcd}(a, b)$ si y sólo si se cumplen las dos condiciones siguientes:*

1) d es divisor de a y de b.

2) Si $n \in \mathbb{N}$ es divisor de a y de b entonces n es divisor de d.

© Ediciones Pirámide

DEMOSTRACIÓN.

$\boxed{\Leftarrow}$ Las dos condiciones anteriores implican que d es el mayor de todos los divisores de a y b y, por tanto, $d = \mathrm{mcd}(a, b)$.

$\boxed{\Rightarrow}$ Si $d = \mathrm{mcd}(a, b)$ entonces d es, obviamente, un divisor de a y de b. Por tanto, por la Proposición 1.2, se verifica que existen $p \in \mathbb{Z}$ y $q \in \mathbb{Z}$ tales que $d = pa + qb$. De esta forma, si $n \in \mathbb{N}$ es divisor de a y de b, se verifica que

$$\frac{d}{n} = p\,\frac{a}{n} + q\,\frac{b}{n} \in \mathbb{Z},$$

de donde se concluye que n es divisor de d. □

Observación 1.10 El concepto de máximo común divisor de dos números naturales estudiado aquí puede extenderse a números enteros y a otras estructuras más complejas (como los anillos conmutativos). Para ello se utiliza como definición de máximo común divisor las dos propiedades de la Proposición 1.4. No entraremos en más detalles sobre este asunto, por ser de un nivel más avanzado a la temática de este libro. □

Observación 1.11 De acuerdo con la Proposición 1.4, una forma alternativa al algoritmo de Euclides para calcular el $\mathrm{mcd}(a, b)$ es la siguiente: en primer lugar se hace la factorización de a y b en números primos:

$$a = 2^{i_2} \times 3^{i_3} \times 5^{i_5} \times 7^{i_7} \times \cdots \text{ y } b = 2^{j_2} \times 3^{j_3} \times 5^{j_5} \times 7^{j_7} \times \cdots$$

El $\mathrm{mcd}(a, b)$ se obtiene como el producto de los factores comunes elevados al menor exponente. Es decir,

$$\mathrm{mcd}(a, b) = 2^{\mathrm{mín}\{i_2, j_2\}} \times 3^{\mathrm{mín}\{i_3, j_3\}} \times 5^{\mathrm{mín}\{i_5, j_5\}} \times 7^{\mathrm{mín}\{i_7, j_7\}} \times \cdots$$

De manera análoga se puede calcular el máximo común divisor de varios números (simplemente habrá que hacer el mínimo de tantos exponentes como números tengamos). □

Ejemplo 1.12 Para hallar el $\mathrm{mcd}(56, 196, 70)$ hacemos la factorización de 56, 196 y 70 en números primos:

$$56 = 2^3 \times 7,\ 196 = 2^2 \times 7^2 \text{ y } 70 = 2 \times 5 \times 7.$$

Entonces (nótese que $n = n^1$ y que, tal y como veremos en la Definición 1.20 y en la Observación 1.37, $n^0 = 1$, para todo $n \in \mathbb{N}$):

$$\mathrm{mcd}(56, 196, 70) = 2^{\mathrm{mín}\{3,2,1\}} \times 5^{\mathrm{mín}\{0,0,1\}} \times 7^{\mathrm{mín}\{1,2,1\}} = 2^1 \times 5^0 \times 7^1 = 14.$$

Por tanto, 14 es el mayor entero por el que se puede dividir 56, 196 y 70. □

© Ediciones Pirámide

Ejemplo 1.13 Una forma de calcular el $\mathrm{mcd}(3468, 468)$, alterrnativa a la utilizada en el Ejemplo 1.8, es la siguiente: a partir de las tablas

$$\begin{array}{r|l} 3468 & 2 \\ 1734 & 2 \\ 867 & 3 \\ 289 & 17 \\ 17 & 17 \\ 1 & \end{array} \quad \text{y} \quad \begin{array}{r|l} 468 & 2 \\ 234 & 2 \\ 117 & 3 \\ 39 & 3 \\ 13 & 13 \\ 1 & \end{array}$$

se obtiene que

$$3468 = 2^2 \times 3 \times 17^2 \ \text{ y } \ 468 = 2^2 \times 3^2 \times 13,$$

de donde se deduce que

$$\begin{aligned} \mathrm{mcd}(3468, 468) &= 2^{\text{mín}\{2,2\}} \times 3^{\text{mín}\{1,2\}} \times 13^{\text{mín}\{0,1\}} \times 17^{\text{mín}\{2,0\}} \\ &= 2^2 \times 3^1 \times 13^0 \times 17^0 = 12. \quad \square \end{aligned}$$

La descomposición en factores primos de un número con un factor primo muy grande puede ser muy engorrosa y lenta (se puede intentar, a modo de ejemplo, calcular la factorización en números primos del número 54991, que utilizaremos en el Problema 1.3). Esta dificultad es utilizada en la actualidad en métodos de encriptación, en particular para los pagos electrónicos seguros.

Es por eso por lo que, cuando uno de los números $m, n \in \mathbb{Z}$ tiene como factor un número primo grande, el método mostrado anteriormente para calcular el $\mathrm{mcd}(m, n)$ mediante la factorización en números primos no es viable, por lo que se suele recurrir a alternativas mucho más rápidas y de fácil implementación, como el *algoritmo de Euclides*.

Observación 1.12 Dos *números racionales* son *iguales* si su forma irreducible coincide. $\square$

Ejemplo 1.14 Los números racionales $\frac{765}{228}$ y $\frac{1275}{380}$ son iguales, pues tienen la misma forma irreducible $\frac{255}{76}$. En efecto, basta observar que

$$\frac{765}{228} = \frac{3^2 \times 5 \times 17}{2^2 \times 3 \times 19} = \frac{3 \times 5 \times 17}{2^2 \times 3 \times 19} = \frac{255}{76}$$

y

$$\frac{1275}{380} = \frac{3 \times 5^2 \times 17}{2^2 \times 19} = \frac{3 \times 5 \times 17}{2^2 \times 3 \times 19} = \frac{255}{76}. \quad \square$$

Ahora bien, ¿cómo se suman o restan los números racionales? Pensemos de nuevo en la tarta. Supongamos que tenemos que sumar $\frac{1}{3}$ de la tarta con $\frac{2}{5}$ de la tarta. Lo más sencillo

© Ediciones Pirámide

es dividir la tarta en un número de porciones que sea múltiplo de ambos denominadores. Por ejemplo dividir la tarta en $3 \times 5 = 15$ porciones. De esta forma,

$$\frac{1}{3} + \frac{2}{5} = \frac{5 \times 1}{5 \times 3} + \frac{3 \times 2}{3 \times 5} = \frac{5}{15} + \frac{6}{15} = \frac{11}{15}.$$

Observación 1.13 Según lo anterior, una manera simple de sumar o restar números racionales es la siguiente:

$$\frac{m}{n} + \frac{p}{q} = \frac{q \times m}{q \times n} + \frac{n \times p}{n \times q} = \frac{q \times m + n \times p}{n \times q}$$

y

$$\frac{m}{n} - \frac{p}{q} = \frac{q \times m}{q \times n} - \frac{n \times p}{n \times q} = \frac{q \times m - n \times p}{n \times q}.$$

Esto último nos indica que dos *números racionales* $\frac{m}{n} \in \mathbb{Q}$ y $\frac{p}{q} \in \mathbb{Q}$ son *iguales* si

$$m \times q = n \times p$$

(compárese esto con lo dicho en la Observación 1.12). □

Ejemplo 1.15 Los números racionales $\frac{765}{228}$ y $\frac{1275}{380}$ considerados en el Ejemplo 1.14 son iguales, dado que se verifica que

$$765 \times 380 = 290700 = 228 \times 1275. \quad \square$$

Una forma alternativa de sumar y restar números racionales $\frac{m}{n}$ y $\frac{p}{q}$ a la contemplada en la Observación 1.13 consiste en utilizar en el denominador el múltiplo común a los denominadores n y q que sea más pequeño, también conocido como *mínimo común múltiplo* de n y q, que se suele denotar como $\mathrm{mcm}(n, q)$.

Ejemplo 1.16 Para calcular la diferencia

$$\frac{5}{4} - \frac{3}{2},$$

dado que es evidente que $\mathrm{mcm}(4, 2) = 4$, se escribe cada número de la resta como un número con denominador igual a 4, de la siguiente forma:

$$\frac{5}{4} - \frac{3}{2} = \frac{5}{4} - \frac{2 \times 3}{2 \times 2} = -\frac{1}{4}$$

(nótese la diferencia de este método con el de la Observación 1.13). □

¿Cómo se calcula, en general, el mínimo común múltiplo de dos números enteros a y b cualesquiera ($\mathrm{mcm}(a, b)$)?

© Ediciones Pirámide

Proposición 1.5 *Dados $a, b, m \in \mathbb{N}$ se verifica que $m = \text{mcm}(a, b)$ si y sólo si se cumplen las dos condiciones siguientes:*

1) m es múltiplo de a y de b.

2) Si $n \in \mathbb{N}$ es múltiplo de a y de b entonces n es múltiplo de m.

DEMOSTRACIÓN.

$\boxed{\Leftarrow}$ Las dos condiciones anteriores implican que m es el más pequeño de todos los múltiplos de a y b y, por tanto, $m = \text{mcm}(a, b)$.

$\boxed{\Rightarrow}$ Si $m = \text{mcm}(a, b)$ entonces m es, obviamente, un múltiplo de a y de b. Por otra parte, si $n \in \mathbb{N}$ es múltiplo de a y de b veamos que $m|n$. En efecto, por hipótesis, existen $\alpha, \beta, \alpha', \beta' \in \mathbb{N}$ tales que

$$\begin{cases} m = a\alpha,\ m = b\beta \text{ y } \text{mcd}(\alpha, \beta) = 1 \\ n = a\alpha',\ n = b\beta', \end{cases}$$

por lo que

$$\begin{cases} 1 = \dfrac{a\alpha}{b\beta} = \dfrac{a\alpha'}{b\beta'} \\ \text{mcd}(\alpha, \beta) = 1 \end{cases} \Rightarrow \begin{cases} \alpha\beta' = \alpha'\beta \\ \text{mcd}(\alpha, \beta) = 1 \end{cases} \Rightarrow \begin{cases} \dfrac{\alpha\beta'}{\beta} = \alpha' \in \mathbb{N} \\ \text{mcd}(\alpha, \beta) = 1. \end{cases}$$

De esta forma, por el *lema de Euclides*, se tiene que $\beta|\beta'$ y, por tanto, existe $k \in \mathbb{N}$ tal que $\beta' = k\beta$. Consecuentemente

$$n = \beta' b = k\beta b = km,$$

de donde se concluye que $m|n$. □

Observación 1.14 De acuerdo con la Proposición 1.5, una forma de calcular el $\text{mcm}(a, b)$ es la siguiente: en primer lugar se hace la descomposición de a y b en producto de potencias de números primos

$$a = 2^{i_2} \times 3^{i_3} \times 5^{i_5} \times 7^{i_7} \times \cdots \text{ y } b = 2^{j_2} \times 3^{j_3} \times 5^{j_5} \times 7^{j_7} \times \cdots$$

El $\text{mcm}(a, b)$ se obtiene como el producto de todos los factores (comunes y no comunes) elevados a su mayor exponente. Es decir,

$$\text{mcm}(a, b) = 2^{\text{máx}\{i_2, j_2\}} \times 3^{\text{máx}\{i_3, j_3\}} \times 5^{\text{máx}\{i_5, j_5\}} \times 7^{\text{máx}\{i_7, j_7\}} \times \cdots$$

De manera análoga se puede calcular el mínimo común múltiplo de varios números (simplemente habrá que hacer el máximo de tantos exponentes como números tengamos). □

© Ediciones Pirámide

Ejemplo 1.17 Para hallar el $\mathrm{mcm}(56, 196, 70)$ hacemos la factorización de 56, 196 y 70 en números primos:

$$56 = 2^3 \times 7,\ 196 = 2^2 \times 7^2 \ \text{ y } \ 70 = 2 \times 5 \times 7.$$

Entonces (nótese que $n = n^1$ y que, tal y como veremos en la Definición 1.20 y en la Observación 1.37, $n^0 = 1$, para todo $n \in \mathbb{N}$):

$$\mathrm{mcm}(56, 196, 70) = 2^{\text{máx}\{3,2,1\}} \times 5^{\text{máx}\{0,0,1\}} \times 7^{\text{máx}\{1,2,1\}} = 2^3 \times 5^1 \times 7^2 = 1960.$$

Por tanto, 1960 es el menor número natural que es múltiplo de 56, 196 y 70. □

Al igual que sucedía con el máximo común divisor, la aplicación de este método de cálculo no siempre es conveniente, pues necesita realizar la descomposición en números primos, que, a veces, puede ser lenta y engorrosa. Para obtener un método de cálculo alternativo usaremos el siguiente resultado:

Proposición 1.6 *Dados dos números naturales a y b, se verifica que*

$$ab = \mathrm{mcd}(a, b)\,\mathrm{mcm}(a, b). \tag{1.12}$$

DEMOSTRACIÓN. De acuerdo con lo visto en las Observaciones 1.11 y 1.14, si

$$a = 2^{i_2} \times 3^{i_3} \times 5^{i_5} \times 7^{i_7} \times \cdots \ \text{ y } \ b = 2^{j_2} \times 3^{j_3} \times 5^{j_5} \times 7^{j_7} \times \cdots$$

son, respectivamente, las factorizaciones de a y b en números primos, se verifica que

$$\begin{aligned} ab &= 2^{\text{mín}\{i_2,j_2\}+\text{máx}\{i_2,j_2\}} \times 3^{\text{mín}\{i_3,j_3\}+\text{máx}\{i_3,j_3\}} \times 5^{\text{mín}\{i_5,j_5\}+\text{máx}\{i_5,j_5\}} \times \cdots \\ &= 2^{\text{mín}\{i_2,j_2\}} 2^{\text{máx}\{i_2,j_2\}} \times 3^{\text{mín}\{i_3,j_3\}} 3^{\text{máx}\{i_3,j_3\}} \times 5^{\text{mín}\{i_5,j_5\}} 5^{\text{máx}\{i_5,j_5\}} \times \cdots \\ &= \left(2^{\text{mín}\{i_2,j_2\}} \times 3^{\text{mín}\{i_3,j_3\}} \times 5^{\text{mín}\{i_5,j_5\}} \times 7^{\text{mín}\{i_7,j_7\}} \times \cdots\right) \\ &\quad \times \left(2^{\text{máx}\{i_2,j_2\}} \times 3^{\text{máx}\{i_3,j_3\}} \times 5^{\text{máx}\{i_5,j_5\}} \times 7^{\text{máx}\{i_7,j_7\}} \times \cdots\right) \\ &= \mathrm{mcd}(a, b)\,\mathrm{mcm}(a, b). \quad \square \end{aligned}$$

Teniendo en cuenta la Proposición 1.6, una forma alternativa de calcular el mínimo común múltiplo de dos números consiste en hallar su máximo común divisor usando el *algoritmo de Euclides* y en utilizar la fórmula (1.12).

Ejemplo 1.18 A partir del Ejemplo 1.8 se deduce que

$$\mathrm{mcm}(3468, 468) = \frac{3468 \times 468}{\mathrm{mcd}(3468, 468)} = \frac{3468 \times 468}{12} = 289 \times 468 = 135252.$$

© Ediciones Pirámide

De esta forma, podemos sumar fracciones con estos denominadores. Así, por ejemplo, teniendo en cuenta que

$$135252 = 3468 \times 39 \text{ y } 135252 = 468 \times 289,$$

se verifica que

$$\frac{34}{3468} + \frac{21}{468} = \frac{34 \times 39}{3468 \times 39} + \frac{21 \times 289}{468 \times 289} = \frac{1326}{135252} + \frac{6069}{135252} = \frac{7395}{135252} = \frac{145}{2652}. \quad \square$$

La multiplicación y división de números racionales siguen reglas de muy sencilla aplicación:

$$\frac{m}{n} \times \frac{p}{q} = \frac{m \times p}{n \times q}$$

y

$$\frac{m}{n} \div \frac{p}{q} = \frac{\frac{m}{n}}{\frac{p}{q}} = \frac{m}{n} \times \frac{q}{p} = \frac{m \times q}{n \times p}.$$

Observación 1.15 La suma, resta, multiplicación y división de números racionales (excepto la división por cero) son un número racional. Ejemplo:

$$\frac{3}{4} + \frac{7}{5} = \frac{3 \times 5 + 4 \times 7}{4 \times 5} = \frac{43}{20}, \ \frac{3}{4} - \frac{7}{5} = \frac{3 \times 5 - 4 \times 7}{4 \times 5} = -\frac{13}{20},$$

$$\frac{3}{4} \times \frac{7}{5} = \frac{3 \times 7}{4 \times 5} = \frac{21}{20}, \ \frac{3}{4} \div \frac{7}{5} = \frac{\frac{3}{4}}{\frac{7}{5}} = \frac{3}{4} \times \frac{5}{7} = \frac{3 \times 5}{4 \times 7} = \frac{15}{28}. \quad \square$$

Observación 1.16 Un número racional siempre puede expresarse, al hacer la división, mediante un número decimal con un número finito o infinito de cifras. En el último caso, las cifras decimales son periódicas. Así, por ejemplo

$$\frac{1}{8} = 0'125, \ \frac{1}{3} = 0'333333\ldots = 0'\widehat{3}.$$

Recíprocamente, todo número decimal con una cantidad finita o infinita periódica de cifras decimales puede expresarse como un número racional. Así, por ejemplo:

a) $x = 15'75$ (número *decimal no periódico*). Claramente,

$$x = \frac{1575}{100} = \frac{63}{4}.$$

b) $x = 3'\widehat{48}$ (número *decimal periódico puro*). Si multiplicamos x por 100 y restamos x, obtenemos

$$99x = 100x - x = 348'\widehat{48} - 3'\widehat{48} = 345 \Rightarrow x = \frac{345}{99} = \frac{115}{33}.$$

© Ediciones Pirámide

c) $x = 2'7\widehat{82}$ (número *decimal periódico mixto*). Argumentando como en b), se tiene

$$2'7\widehat{82} = \frac{27'\widehat{82}}{10} = \frac{\frac{2755}{99}}{10} = \frac{2755}{990} = \frac{551}{198}. \quad \square$$

Observación 1.17 En general debe prescindirse de los números racionales que tienen a 9 como periodo, puesto que éstos admiten otra representación decimal equivalente. Así, por ejemplo, $0'\widehat{9} = 1$. $\square$

Observación 1.18 El conjunto $\mathbb{Q}$ de los números racionales:

a) Está *totalmente ordenado* respecto de la operación $\leq$, es decir, dados dos números racionales arbitrarios $a, b \in \mathbb{Q}$, se verifica que

$$a \leq b \text{ o } b \leq a.$$

Si hacemos una representación gráfica, $a \leq b$ significa que a es más pequeño que b (y se representa a a la izquierda de b) o coincide con b (en cuyo caso a y b se representan en la misma posición). Además, la relación de orden $\leq$ es compatible con las operaciones de suma y producto de números racionales, es decir, para cada terna de números racionales $a, b, c \in \mathbb{Q}$ se verifica:

i) $a \leq b \Leftrightarrow a + c \leq b + c$.

ii) $a \leq b \Leftrightarrow ac \leq bc$, supuesto $c > 0$.

b) Verifica la *propiedad arquimediana*: si $a, b \in \mathbb{Q}$ con $0 < a < b$ se verifica que existe $n \in \mathbb{N}$ tal que $na > b$. Ejemplo: si $a = \frac{1}{10}$ y $b = 1000000$, basta tomar $n > 10000000$.

c) Es un conjunto *denso*, es decir, entre dos números racionales existe siempre un número racional. En efecto, si $a, b \in \mathbb{Q}$ y $a < b$, siempre se verifica que

$$a < \frac{a+b}{2} < b$$

donde la *media aritmética* de los números racionales a y b verifica que $\frac{a+b}{2} \in \mathbb{Q}$. $\square$

1.3. Números irracionales. Números reales

Con el conjunto $\mathbb{Q}$ de números racionales aparentemente nos podríamos dar ya por satisfechos. No obstante, si imaginamos todos los números racionales representados sobre la recta numérica, encontramos "huecos", es decir, existen números (como $\sqrt{2}$) que no corresponden con ningún número racional.

© Ediciones Pirámide

Proposición 1.7 $\sqrt{2}$ *no es un número racional.*

La afirmación que aparece en la Proposición 1.7 podría ser falsa. Es necesario, por tanto, demostrar su veracidad. Hay muchas técnicas para probar distintas afirmaciones o resultados matemáticos. Nosotros utilizaremos, en este caso, la técnica que se conoce como *reducción al absurdo*, que consiste en probar que si no se cumple el resultado que se quiere probar, entonces se llega a un resultado falso (o absurdo), por lo que se concluye que la afirmación o resultado que se quería demostrar es cierto.

DEMOSTRACIÓN DE LA PROPOSICIÓN 1.7. Argumentamos por reducción al absurdo. Si $\sqrt{2}$ fuera un número racional, podríamos expresarlo como

$$\sqrt{2} = \frac{m}{n} \text{ (fracción irreducible).} \tag{1.13}$$

Nuestro objetivo es deducir, a partir de la igualdad (1.13), algo que sea falso. Ahora bien, a partir de (1.13), puesto que los números que aparecen en cada lado de la igualdad son iguales, seguirán siendo iguales si los elevamos al cuadrado, de donde se deduce que

$$m^2 = 2n^2. \tag{1.14}$$

Como, por hipótesis, $\frac{m}{n}$ es una fracción irreducible, al menos uno de ellos es impar, pues en otro caso los dos se podrían dividir por 2 y entonces la fracción no sería irreducible. Pueden presentarse, por tanto, dos casos:

a) Si m es impar, entonces m^2 es también impar, lo que contradice (1.14).

b) Si m es par, entonces n es impar. Luego $m = 2k$ con $k \in \mathbb{Z}$ y, por tanto, de la relación (1.14) se deduce que

$$2n^2 = m^2 = 4k^2 \Rightarrow n^2 = 2k^2,$$

lo que implica que n tiene que ser par, obteniéndose así una contradicción. □

Esta nueva clase de números, como $\sqrt{2}$, son los *números irracionales*.

Definición 1.10 El conjunto de los *números irracionales* es el formado por los números con infinitas cifras decimales no periódicas, y se representa por $\mathbb{I}$. □

Ejemplo 1.19 $\sqrt{2} = 1'414213562373095\ldots \in \mathbb{I}$, $\pi = 3'141592653589793\ldots \in \mathbb{I}$, $e = 2'718281828459046\ldots \in \mathbb{I}$. □

Ejemplo 1.20 Como extensión de la Proposición 1.7, en general, para todo número natural $n \in \mathbb{N}$ se verifica que $\sqrt{n}$ es entero o irracional. Así, por ejemplo,

$$\sqrt{16} = 4 \in \mathbb{Z} \text{ pero } \sqrt{7} = 2'645751311064591\ldots \in \mathbb{I}. \quad \square$$

© Ediciones Pirámide

Definición 1.11 El conjunto de los *números reales* es el formado por los números racionales e irracionales y se representa por $\mathbb{R}$, es decir, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. □

Observación 1.19 El conjunto $\mathbb{R}$ de los números reales es, por tanto, el formado por todos los números decimales: los decimales finitos o periódicos se corresponden con los números racionales, y los decimales infinitos no periódicos, con los números irracionales. □

Observación 1.20 El conjunto $\mathbb{R}$ de los números reales cumple las siguientes propiedades: para todo $a, b, c \in \mathbb{R}$ se verifica:

a) Axiomas de la suma:

   1) Propiedad conmutativa: $a + b = b + a$.
   2) Propiedad asociativa: $(a + b) + c = a + (b + c)$.
   3) Existencia de elemento neutro, 0, tal que $a + 0 = 0 + a = a$.
   4) $\forall\, a \in \mathbb{R}$ existe su elemento opuesto, $-a$, tal que $a + (-a) = 0$.

b) Axiomas de la multiplicación:

   1) Propiedad conmutativa: $a \times b = b \times a$.
   2) Propiedad asociativa: $(a \times b) \times c = a \times (b \times c)$.
   3) Existencia de elemento neutro, 1, tal que $a \times 1 = 1 \times a = a$.
   4) $\forall\, a \neq 0$ existe su elemento inverso, $\frac{1}{a}$, tal que $a \times \frac{1}{a} = 1$.
   5) Propiedad distributiva de la multiplicación con respecto a la suma: $(a + b) \times c = a \times c + b \times c$.

c) Axiomas de orden:

   1) Propiedad reflexiva: $a \leq a$.
   2) Propiedad antisimétrica: $a \leq b$ y $b \leq a \;\Rightarrow\; a = b$.
   3) Propiedad transitiva: $a \leq b$ y $b \leq c \;\Rightarrow\; a \leq c$.
   4) Orden total: $a, b \in \mathbb{R} \;\Rightarrow\; a \leq b$ o $b \leq a$.
   5) Compatibilidad del orden con la suma: $a \leq b \;\Leftrightarrow\; a + c \leq b + c$.
   6) Compatibilidad del orden con el producto: $a \leq b \;\Leftrightarrow\; a \times c \leq b \times c$, $\forall\, c > 0$.
   7) Propiedad arquimediana: si $a, b \in \mathbb{R}$ son tales que $0 < a < b \;\Rightarrow\; \exists\, n \in \mathbb{N}$ tal que $na > b$.

d) Axioma de completitud (o axioma del supremo): todo conjunto de números reales no vacío y acotado superiormente tiene *supremo* en $\mathbb{R}$ (es decir, el supremo, que es la mínima cota superior, pertenece a $\mathbb{R}$). □

© Ediciones Pirámide

Observación 1.21 El conjunto $\mathbb{R}$ se diferencia del conjunto $\mathbb{Q}$ por la *completitud*: la recta real es "completa" mientras que la recta racional no lo es (es decir, los números reales "llenan" la recta real o, dicho de otra forma, en la recta real "no hay huecos"). Para ver que el conjunto $\mathbb{Q}$ de números racionales no cumple el axioma de completitud basta considerar el conjunto

$$A = \{x \in \mathbb{Q} : \ x^2 < 2\},$$

que es un subconjunto de $\mathbb{Q}$ no vacío (por ejemplo, $1 \in A$), está acotado superiormente en $\mathbb{Q}$ (por ejemplo, $3 \in \mathbb{Q}$ es una cota superior de A, pues se verifica que $x \leq 3$ para todo $x \in A$) pero no tiene supremo en $\mathbb{Q}$ (pues el supremo de A es $\sqrt{2}$ y, como se ha visto en la Proposición 1.7, se verifica que $\sqrt{2} \notin \mathbb{Q}$). □

Definición 1.12 Sean $a, b \in \mathbb{R}$.

a) *Restar* al número a el número b consiste en sumar a a el opuesto de b, es decir,

$$a - b = a + (-b).$$

b) *Dividir* el número a entre el número $b \neq 0$ consiste en multiplicar a por el inverso de b, es decir,

$$\frac{a}{b} = a \times \frac{1}{b}. \quad \square$$

Observación 1.22 Algunas consecuencias de los axiomas de la Observación 1.20:

a) Los elementos que intervienen en una suma o en un producto pueden agruparse en cualquier orden. Ejemplo: para todo $a, b, c, d \in \mathbb{R}$ se verifica que

$$\begin{aligned}[(a+b)+c]+d &= a+[(b+c)+d] = (a+b)+(c+d)\\ &= a+(b+c)+d = a+b+c+d\end{aligned}$$

y

$$\begin{aligned}[(a \times b) \times c] \times d &= a \times [(b \times c) \times d] = (a \times b) \times (c \times d)\\ &= a \times (b \times c) \times d = a \times b \times c \times d.\end{aligned}$$

b) $a = b \ \Leftrightarrow \ a + c = b + c, \ \forall\, a, b, c \in \mathbb{R}$.

c) $a = b \ \Leftrightarrow \ a \times c = b \times c, \ \forall\, a, b, c \in \mathbb{R}, \ \forall\, c \neq 0$.

d) El elemento neutro de la suma y del producto es único.

e) Los elementos opuesto e inverso son únicos.

f) $a \times 0 = 0, \ \forall\, a \in \mathbb{R}$.

g) $a \times (-b) = -(a \times b), \ \forall\, a, b \in \mathbb{R}$. □

© Ediciones Pirámide

Definición 1.13 Sea $x \in \mathbb{R}$.

a) x es *positivo* si $x > 0$. El conjunto de números reales positivos se representa por

$$\mathbb{R}_+ = \{x \in \mathbb{R} : \ x > 0\}.$$

b) x es *negativo* si $x < 0$. El conjunto de números reales negativos se representa por

$$\mathbb{R}_- = \{x \in \mathbb{R} : \ x < 0\}. \quad \square$$

Observación 1.23

a) El opuesto de un número positivo es negativo y el opuesto de un número negativo es positivo.

b) 0 no es un número positivo ni negativo.

c) $\mathbb{R} = \mathbb{R}_- \cup \{0\} \cup \mathbb{R}_+$.

d) Si $a, b \in \mathbb{R}$ tienen el mismo signo (ya sea positivo o negativo), entonces $a \times b$ es positivo.

e) Si $a, b \in \mathbb{R}$ tienen signos opuestos, entonces $a \times b$ es negativo.

f) Si $a, b \in \mathbb{R}$, se verifica que: $a \times b \neq 0 \ \Leftrightarrow \ a \neq 0 \ \text{ y } \ b \neq 0$.

g) $-(a+b) = -a - b, \ \forall\, a, b \in \mathbb{R}$.

h) $-(a-b) = b - a, \ \forall\, a, b \in \mathbb{R}$. $\quad \square$

Observación 1.24 Cuando aparecen sumas, restas, multiplicaciones, divisiones y potencias, hay que tener en cuenta la siguiente regla de prioridad en el orden de las operaciones:

1) potencias,

2) multiplicaciones/divisiones y

3) sumas/restas. $\quad \square$

Ejemplo 1.21 $\dfrac{1}{2} - \dfrac{3}{4}\left(\dfrac{1}{2}\right)^3 = \dfrac{1}{2} - \dfrac{3}{4}\dfrac{1}{8} = \dfrac{1}{2} - \dfrac{3}{32} = \dfrac{13}{32}$. $\quad \square$

Definición 1.14 Sean $a, b \in \mathbb{R}$ tales que $a \leq b$. Los conjuntos

$$[a,b] = \{x \in \mathbb{R} : \ a \leq x \leq b\}, \quad (a,b) = \{x \in \mathbb{R} : \ a < x < b\}$$
$$[a,b) = \{x \in \mathbb{R} : \ a \leq x < b\}, \quad (a,b] = \{x \in \mathbb{R} : \ a < x \leq b\}$$

se denominan *intervalos* de extremos a y b. Más concretamente, $[a,b]$ es un *intervalo cerrado* (se incluyen los extremos), (a,b) es un *intervalo abierto* (no se incluyen los extremos) y $[a,b)$, $(a,b]$ son *intervalos semiabiertos* (o *semicerrados*) (no se incluye uno de los extremos). $\quad \square$

© Ediciones Pirámide

Observación 1.25 En la ordenación total de los números reales no hay un primer elemento ni un último. Por ello, vamos a completar el conjunto $\mathbb{R}$ de los números reales con dos nuevos símbolos $+\infty$ y $-\infty$ que designaremos, respectivamente, *más infinito* y *menos infinito* y que tienen las siguientes propiedades:

a) $-\infty < x < +\infty$ para todo $x \in \mathbb{R}$. Estas desigualdades introducen un *orden total* en la *recta real ampliada*

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\} \tag{1.15}$$

que completa el de $\mathbb{R}$. De esta forma, $-\infty$ y $+\infty$ son, respectivamente, el *extremo inferior* y el *extremo superior* del conjunto totalmente ordenado de los números reales.

b) $x + (+\infty) = +\infty$ y $x + (-\infty) = -\infty$ para todo $x \in \mathbb{R}$.

c) $\begin{cases} x(+\infty) = +\infty,\ x(-\infty) = -\infty & \text{si} \quad x > 0 \\ x(+\infty) = -\infty,\ x(-\infty) = +\infty & \text{si} \quad x < 0. \end{cases}$

d) $(+\infty) + (+\infty) = +\infty$ y $(-\infty) + (-\infty) = -\infty$.

e) $(+\infty)(+\infty) = +\infty$, $(-\infty)(-\infty) = +\infty$ y $(+\infty)(-\infty) = (-\infty)(+\infty) = -\infty$.

Con estos nuevos símbolos podemos ampliar las definiciones anteriores de intervalo. Así,

$$[a, +\infty) = \{x \in \mathbb{R} :\ x \geq a\}, \quad (-\infty, b] = \{x \in \mathbb{R} :\ x \leq b\}$$
$$(a, +\infty) = \{x \in \mathbb{R} :\ x > a\}, \quad (-\infty, b) = \{x \in \mathbb{R} :\ x < b\}.$$

Nótese que $+\infty$ y $-\infty$ no son números reales, $(-\infty, +\infty) = \mathbb{R}$ y $[-\infty, +\infty] = \overline{\mathbb{R}}$. □

Observación 1.26 Obsérvese que en la *recta real ampliada* $\overline{\mathbb{R}}$ definida en (1.15) ya no son operaciones ni la suma (no está definido $(+\infty) + (-\infty)$) ni la multiplicación (no está definido $0 \cdot \infty$ ni $\frac{\infty}{\infty}$). □

Definición 1.15 El *valor absoluto* de un número real $x \in \mathbb{R}$ es el mayor de los números x y $-x$ y se representa por $|x|$, es decir,

$$|x| = \begin{cases} x, & x > 0 \\ 0, & x = 0 \\ -x, & x < 0. \end{cases}$$ □

Ejemplo 1.22 $|5| = 5$ y $|-3| = -(-3) = 3$. □

Observación 1.27 Nótese que el valor absoluto de un número real es siempre un número mayor o igual que cero. □

© Ediciones Pirámide

Observación 1.28 (Propiedades del valor absoluto) Para todo $a, b \in \mathbb{R}$ y $r \in (0, +\infty)$ se verifican las siguientes propiedades:

a) $|a| = 0 \Leftrightarrow a = 0$.

b) $|a \times b| = |a| \times |b|$.

c) $|a + b| \leq |a| + |b|$ (*Desigualdad triangular*).

d) $-|a| \leq a \leq |a|$.

e) $|a| \leq r \Leftrightarrow -r \leq a \leq r$. □

1.4. Radicales y potencias. Operaciones

Tal y como se ha visto en la Definición 1.2, recordamos que a elevado a la potencia n es

$$a^n = a \times \overset{n)}{\cdots} \times a, \ \forall\, a \in \mathbb{R}, \ \forall\, n \in \mathbb{N}.$$

Esta operación está claro cómo hacerla cuando a es un número racional, pero ¿cómo se hace cuando a es irraccional? Éstos son detalles sutiles que se escapan al carácter básico de este libro pero que conviene tener presentes (véase la Observación 1.41 para saber más sobre este asunto).

Proposición 1.8 $a^n \times a^m = a^{n+m}$, $\forall\, a \in \mathbb{R}$, $\forall\, n, m \in \mathbb{N}$.

DEMOSTRACIÓN. Basta observar que

$$a^n \times a^m = \left(a \times \overset{n)}{\cdots} \times a\right)\left(a \times \overset{m)}{\cdots} \times a\right) = a \times \overset{n+m)}{\cdots} \times a = a^{n+m}. \quad \square$$

Ejemplo 1.23 $2^3 \times 2^2 = 2^5 = 32$, $(-3)^4 \times (-3)^5 = (-3)^9 = -19683$. □

Observación 1.29 Argumentando como en la demostración de la Proposición 1.8, fácilmente se comprueba que para todo $a, b \in \mathbb{R}$ y $n, m \in \mathbb{N}$ se verifica que:

a) $\dfrac{a^n}{a^m} = a^{n-m}$.

b) $(a^n)^m = a^{nm}$.

c) $\left(\dfrac{a}{b}\right)^n = \dfrac{a^n}{b^n}$. □

Ejemplo 1.24 $\dfrac{3^4}{3^3} = 3$, $(4^2)^5 = 4^{10} = 1048576$, $\left(\dfrac{5}{2}\right)^2 = \dfrac{5^2}{2^2} = \dfrac{25}{4}$. □

© Ediciones Pirámide

Dado $a > 0$, pensemos en el siguiente problema: encontrar $x \in \mathbb{R}$ tal que

$$x^2 = a. \tag{1.16}$$

Nótese que si $\alpha^2 = a$, entonces también se cumple que $(-\alpha)^2 = a$. Por tanto, dado $a > 0$, existen dos números reales x solución de la ecuación (1.16). Estos números son, por tanto, $x = \pm\alpha$.

Definición 1.16 La *raíz cuadrada* de un número real no negativo $a \geq 0$ es un número real $\alpha > 0$ que verifica

$$\alpha^2 = a.$$

Se denota $\alpha = \sqrt{a}$. □

Por tanto, las dos soluciones de (1.16) vienen dadas por $x = \pm\sqrt{a}$. Ejemplo:

$$x^2 = 49 \Leftrightarrow x = \pm\sqrt{49} = \pm 7. \quad \square$$

Observación 1.30 Otra forma de denotar la raíz cuadrada de un número a es como su potencia $\frac{1}{2}$. Es decir,

$$a^{\frac{1}{2}} = \sqrt{a}. \quad \square$$

Observación 1.31 (Propiedades de la raíz cuadrada)

a) No están definidas (como números reales) las raíces cuadradas de números negativos.

b) $(\sqrt{a})^2 = a, \ \forall\, a \geq 0.$

c) $\sqrt{0} = 0.$

d) Para todo $a, b \in \mathbb{R}:\ a^2 = b^2 \Leftrightarrow |a| = |b|.$

e) Si $0 < a < b \Rightarrow \sqrt{a} < \sqrt{b}$. □

Proposición 1.9 *La raíz cuadrada de un producto es igual al producto de las raíces cuadradas de los factores, es decir, si $a, b \geq 0$, se tiene que*

$$\sqrt{a \times b} = \sqrt{a} \times \sqrt{b}.$$

Cuando $a, b \in \mathbb{R}_-$, se verifica que

$$\sqrt{a \times b} = \sqrt{|a|} \times \sqrt{|b|}.$$

DEMOSTRACIÓN. Basta observar que para $a, b \geq 0$ se cumple

$$(\sqrt{a} \times \sqrt{b})^2 = (\sqrt{a} \times \sqrt{b}) \times (\sqrt{a} \times \sqrt{b}) = (\sqrt{a} \times \sqrt{a}) \times (\sqrt{b} \times \sqrt{b}) = a \times b.$$

Para el caso en que $a < 0$ y $b < 0$, basta aplicar el caso anterior, pues

$$\sqrt{a \times b} = \sqrt{|a \times b|} = \sqrt{|a| \times |b|} = \sqrt{|a|} \times \sqrt{|b|}. \quad \square$$

© Ediciones Pirámide

Ejemplo 1.25 $\sqrt{4\times 25} = \sqrt{4}\times\sqrt{25} = 2\times 5 = 10$, $\sqrt{(-9)\times(-4)} = \sqrt{9}\times\sqrt{4} = 3\times 2 = 6$. □

Proposición 1.10 *La raíz cuadrada de un cociente es igual al cociente de las raíces cuadradas del numerador y del denominador, es decir, si $a \geq 0$ y $b > 0$, se tiene que*

$$\sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}}.$$

DEMOSTRACIÓN. Basta tener en cuenta que

$$\left(\frac{\sqrt{a}}{\sqrt{b}}\right)^2 = \frac{\sqrt{a}}{\sqrt{b}}\times\frac{\sqrt{a}}{\sqrt{b}} = \frac{\sqrt{a\times a}}{\sqrt{b\times b}} = \frac{a}{b}. \quad \square$$

Ejemplo 1.26 $\sqrt{\dfrac{9}{4}} = \dfrac{\sqrt{9}}{\sqrt{4}} = \dfrac{3}{2}$. □

Proposición 1.11 *La raíz cuadrada de una potencia de exponente par es igual a otra potencia de la misma base y de exponente la mitad del exponente original, es decir, si $a \geq 0$ y $n \in \mathbb{N}$, se tiene que*

$$\sqrt{a^{2n}} = a^n.$$

DEMOSTRACIÓN. Basta observar que

$$(a^n)^2 = a^n \times a^n = a^{n+n} = a^{2n}. \quad \square$$

Ejemplo 1.27

$$\begin{cases} \sqrt{2^4\times 3^8\times 4^2} \overset{(1)}{=} \sqrt{2^4}\times\sqrt{3^8}\times\sqrt{4^2} \overset{(2)}{=} 2^2\times 3^4\times 4 = 1296 \\ (\sqrt{7})^4 = \sqrt{7}\times\sqrt{7}\times\sqrt{7}\times\sqrt{7} \overset{(1)}{=} \sqrt{7^4} \overset{(2)}{=} 7^2 = 49, \end{cases}$$

donde en (1) se ha aplicado la Proposición 1.9 y en (2) la Proposición 1.11. □

Hasta ahora nos hemos limitado al caso de raíces cuadradas. Hagamos una extensión a raíces generales. Pensemos para ello en el siguiente problema: encontrar $x \in \mathbb{R}$ tal que

$$x^n = a. \tag{1.17}$$

Nótese que si n es par y $\alpha^n = a$ con $a > 0$, entonces también se cumple que $(-\alpha)^n = a$. Por tanto, dado $a > 0$, existen dos números reales x solución de la ecuación (1.17). Estos números vienen dados por $x = \pm\alpha$.

© Ediciones Pirámide

Definición 1.17 Si $n \in \mathbb{N}$ es un número par, la *raíz n–ésima* de un número real no negativo a es otro número real $\alpha > 0$ que verifica

$$\alpha^n = a.$$

Se denota $\alpha = \sqrt[n]{a}$ (> 0) y se dice que n es el *índice* o *grado* de la raíz. Cuando $n = 2$, se puede omitir el índice. □

Por tanto, las dos soluciones de (1.17) con $a > 0$ vienen dadas por $x = \pm\sqrt[n]{a}$.

Observación 1.32 Otra forma de denotar la raíz n–ésima de un número a es como su potencia $\frac{1}{n}$. Es decir,

$$a^{\frac{1}{n}} = \sqrt[n]{a}. \quad \square$$

Ejemplo 1.28 $\sqrt[4]{54} = 3$ y las soluciones de $x^4 = 54$ son $x = \pm\sqrt[4]{54} = \pm 3$. □

Por otro lado, si n es impar y $a \in \mathbb{R}$ arbitrario (no se necesita ningún signo predeterminado), entonces existe un único $x \in \mathbb{R}$ solución de la ecuación (1.17).

Definición 1.18 Si $n \in \mathbb{N}$ es un número impar, la *raíz n–ésima* de un número real a es el único número real α que verifica

$$\alpha^n = a.$$

Se denota $\alpha = \sqrt[n]{a}$ (> 0 si $a > 0$ y < 0 si $a < 0$) y se dice que n es el *índice* o *grado* de la raíz. □

Ejemplo 1.29

a) $\sqrt[3]{27} = 3$ y la solución de $x^3 = 27$ es $x = \sqrt[3]{27} = 3$.

b) $\sqrt[3]{-27} = -3$ y la solución de $x^3 = -27$ es $x = \sqrt[3]{-27} = -3$. □

Observación 1.33 Cuando $n = 2$, la raíz se denomina *cuadrada*, para $n = 3$ se denomina *cúbica* ... □

Observación 1.34 (Propiedades de la raíz n–ésima) (Compárense con las propiedades de la raíz cuadrada de la Observación 1.31):

a) Si n es par, no están definidas (como números reales) las raíces n–ésimas de números reales negativos.

b) Si n es impar, están definidas (como números reales) las raíces n–ésimas de todos los números reales.

c) Si n es par, $(\pm\sqrt[n]{a})^n = a$, $\forall\, a \geq 0$.

© Ediciones Pirámide

d) Si n es impar, $(\sqrt[n]{a})^n = a,\ \forall\, a \in \mathbb{R}$.

e) $\sqrt[n]{0} = 0,\ \forall\, n \in \mathbb{N}$.

f) Si n es par: $a^n = b^n \ \Leftrightarrow\ |a| = |b|,\ \forall\, a, b \in \mathbb{R}$.

g) Si n es impar: $a^n = b^n \ \Leftrightarrow\ a = b,\ \forall\, a, b \in \mathbb{R}$.

h) Si n es par y $0 < a < b \ \Rightarrow\ \sqrt[n]{a} < \sqrt[n]{b}$.

i) Si n es impar y $a < b \ \Rightarrow\ \sqrt[n]{a} < \sqrt[n]{b}$. □

Observación 1.35 Todas las propiedades estudiadas anteriormente para raíces cuadradas son extensibles, con las convenientes modificaciones, a raíces n–ésimas generales. Así, por ejemplo, si $a, b, c > 0$ y $n \in \mathbb{N}$, entonces

$$\sqrt[n]{a \times b \times c} = \sqrt[n]{a} \times \sqrt[n]{b} \times \sqrt[n]{c}. \quad \square$$

Definición 1.19 Una *potencia de exponente negativo* es igual a una fracción que tiene por numerador la unidad y por denominador la base de la potencia elevada a exponente positivo. Es decir, si $a \neq 0$ y $n \in \mathbb{N}$, entonces

$$a^{-n} = \frac{1}{a^n}. \quad \square$$

Ejemplo 1.30 $10^{-2} = \dfrac{1}{10^2} = \dfrac{1}{100} = 0'01,\ (-5)^{-2} = \dfrac{1}{(-5)^2} = \dfrac{1}{25} = 0'04.$ □

Observación 1.36 Las reglas de cálculo para potencias de exponente positivo son válidas para potencias de exponente entero negativo. En efecto, si $a, b \in \mathbb{R}\backslash\{0\}$ y $n, m \in \mathbb{N}$, se verifica que:

a) $a^n \times a^{-m} = a^n \times \dfrac{1}{a^m} = \dfrac{a^n}{a^m} = a^{n-m} = a^{n+(-m)}$.

b) $\dfrac{a^{-n}}{a^{-m}} = \dfrac{\frac{1}{a^n}}{\frac{1}{a^m}} = \dfrac{a^m}{a^n} = a^{m-n} = a^{(-n)-(-m)}$.

c) $(a^n)^{-m} = \dfrac{1}{(a^n)^m} = \dfrac{1}{a^{nm}} = a^{-nm} = a^{n(-m)}$.

d) $\left(\dfrac{a}{b}\right)^{-n} = \dfrac{1}{\left(\frac{a}{b}\right)^n} = \dfrac{1}{\frac{a^n}{b^n}} = \dfrac{\frac{1}{a^n}}{\frac{1}{b^n}} = \dfrac{a^{-n}}{b^{-n}}.$ □

Ejemplo 1.31 Para todo $x \neq 0$ se tiene que:

$$(x^{-1}+1)(x^{-1}-1) = x^{-2}-1 = \frac{1}{x^2}-1 = \frac{1-x^2}{x^2} \text{ y } \frac{x^{2n-1}}{x^{-1}} = x^{2n-1-(-1)} = x^{2n}. \quad \square$$

© Ediciones Pirámide