LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña
Dra. Gabriela Jeronimo
Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa
Dr. Alejandro Petrovich

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña, Dra. Gabriela Jeronimo y Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa y Dr. Alejandro Petrovich

autoridades

Presidente de la Nación
Dra. Cristina Fernández de Kirchner

Ministro de Educación
Dr. Alberto E. Sileoni

Secretaria de Educación
Prof. María Inés Abrile de Vollmer

Directora Ejecutiva del Instituto Nacional de Educación Tecnológica
Lic. María Rosa Almandoz

Director Nacional del Centro Nacional de Educación Tecnológica
Lic. Juan Manuel Kirschenbaum

Director Nacional de Educación Técnico Profesional y Ocupacional
Ing. Roberto Díaz

Ministerio de Educación.
Instituto Nacional de Educación Tecnológica.
Saavedra 789. C1229ACE.
Ciudad Autónoma de Buenos Aires.
República Argentina.
2010

LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña
Dra. Gabriela Jeronimo
Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa
Dr. Alejandro Petrovich

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección “Las Ciencias Naturales y la Matemática”.
Director de la Colección: Juan Manuel Kirschenbaum
Coordinadora general de la Colección: Haydeé Noceti.

Industria Argentina

ISBN 978-950-00-0748-1

Director de la Colección:
Lic. Juan Manuel Kirschenbaum
Coordinadora general y académica de la Colección:
Prof. Ing. Haydeé Noceti
Diseño didáctico y corrección de estilo:
Lic. María Inés Narvaja
Ing. Alejandra Santos
Coordinación y producción gráfica:
Tomás Ahumada
Diseño gráfico:
Martin Alejandro Gonzalez
Ilustraciones:
Diego Gonzalo Ferreyro
Federico Timerman
Retoques fotográficos:
Roberto Sobrado
Diseño de tapa:
Tomás Ahumada
Administración:
Cristina Caratozzolo
Néstor Hergenrether
Colaboración:
Téc. Op. en Psic. Soc. Cecilia L. Vazquez
Dra. Stella Maris Quiroga

Nuestro agradecimiento al personal del Centro Nacional de Educación Tecnológica por su colaboración.

Graña, Matías
Los números: de los naturales a los complejos / Matías Graña; Gabriela Jerónimo; Ariel Pacetti; dirigido por Juan Manuel Kirschenbaum.
- 1a ed. - Buenos Aires: Ministerio de Educación de la Nación. Instituto Nacional de Educación Tecnológica, 2009.
200 p.: il.; 24x19 cm. (Las ciencias naturales y la matemática / Juan Manuel Kirschenbaum.)

ISBN 978-950-00-0748-1

1. Enseñanza Secundaria.
I. Jerónimo, Gabriela
II. Pacetti, Ariel
III. Kirschenbaum, Juan Manuel, dir.
IV. Título

CDD 510.712

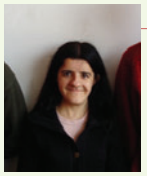
Fecha de catalogación: 16/12/2009

Impreso en Anselmo L. Morvillo S. A., Av. Francisco Pienovi 317 (B1868DRG), Avellaneda, Pcia. de Buenos Aires, Argentina.

Tirada de esta edición: 100.000 ejemplares

Los Autores

Matías Graña
Doctor en Matemática de la Universidad de Buenos Aires; es profesor del Departamento de Matemática de esa universidad e investigador del CONICET. Trabaja en Álgebra no conmutativa.



Gabriela Jeronimo
Doctora en Matemática de la Universidad de Buenos Aires; es profesora del Departamento de Matemática de esa universidad e investigadora del CONICET. Trabaja en Geometría Algebraica.

Ariel Pacetti
Doctor en Matemática de la Universidad de Texas en Austin; es profesor del Departamento de Matemática de la Universidad de Buenos Aires e investigador del CONICET. Trabaja en Teoría de Números.

Con la colaboración de:

Alejandra Patricia Jancsa
Doctora en Matemática de la Universidad Nacional de Córdoba; es investigadora y docente en la Facultad de Ciencias Exactas y Naturales de la UBA. Participa de proyectos de intercambio académico con Francia y España. Ha dictado numerosas conferencias sobre su área de investigación en reuniones científicas nacionales e internacionales. Paralelamente a la matemática, desarrolla actividades musicales como pianista y clavecinista.

Alejandro Petrovich
Doctor en Ciencias Matemáticas. Profesor adjunto del Departamento de Matemática de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. El área principal de investigación es la Lógica Algebraica.

ÍNDICE

Prólogo

Este libro está pensado principalmente para estudiantes de la escuela secundaria y docentes. A lo largo del libro se ve el producto de siglos de avances en la matemática. Algunos de estos avances son pequeños, mientras que otros son importantes y revolucionarios. Es imposible entender el contenido del libro sin dedicarle tiempo. La comprensión en matemática es usualmente producto de la ejercitación y del trabajo, trabajo que se hace con la cabeza, con el lápiz y el papel.

Presentamos conjuntos de números, destinándole un capítulo a cada uno de ellos. El libro está organizado de la siguiente manera: primero, un capítulo donde se presentan algunas de las herramientas básicas que se utilizarán a medida que avanza el texto. A continuación, seis capítulos sobre los conjuntos de números naturales, enteros, enteros modulares, racionales, reales y complejos, respectivamente. Las construcciones se hacen formalmente, pero incluimos numerosos ejemplos, aplicaciones y ejercicios para facilitar la comprensión del material (las resoluciones están en el capítulo 7 y recomendamos al lector que no consulte la resolución de un ejercicio sin tratar de resolverlo previamente). El orden seguido no es el histórico, sino el que permite "avanzar sin sobresaltos". Usualmente, hay una concepción errónea sobre la matemática, que dice que los conceptos matemáticos son inmutables e independientes de acontecimientos culturales o históricos. Nada más lejos de la realidad. Los distintos conjuntos de números se fueron introduciendo en la medida en que hicieron falta para avanzar. Y muchas veces estos conceptos, forjados por alguien "adelantado a su época", o incorporados de otras culturas, necesitaron de varias generaciones de matemáticos para ser aceptados.

Por último, incluimos un apéndice con algunos de los algoritmos presentados en el libro, desarrollados en lenguaje Python, para mostrar la interacción de la matemática con la computación.

En cada capítulo, las proposiciones, teoremas, propiedades, corolarios y lemas están numerados de manera correlativa: tienen un primer número que indica el capítulo, y un segundo número correlativo que sirve para todos a la vez. Por ejemplo, en el capítulo 2, presentamos el teorema 2.1, luego el teorema 2.2, y luego la proposición 2.3 y la proposición 2.4. Los ejercicios tienen una numeración similar, también con dos números, donde el primero es el número del capítulo, mientras que el segundo indica el número de ejercicio dentro de ese capítulo.

Introducción

En el transcurso de la historia, los números surgieron naturalmente para contar (números cardinales: uno, dos, tres, etcétera) y, a la vez, para ordenar (números ordinales: primero, segundo, tercero, etcétera). Por este motivo, el primer conjunto de números que aparece es el de los números *naturales*. Es razonable comenzar cualquier estudio de los números con ellos, porque los números naturales están en la base de todos los otros conjuntos. Sin embargo, con el tiempo aparecieron nuevos usos para los números y, con los usos, nuevos números.

Los números naturales se pueden sumar y multiplicar. Y, a veces, se pueden restar. Sin embargo, no se puede restar a un número natural otro mayor, porque el resultado ya no es un número natural. Es así como, para poder restar, se necesitan el cero y los números negativos. A la humanidad le tomó siglos aceptar estos nuevos números, pese a que pasan a tener un sentido muy concreto cuando se los usa, por ejemplo, para expresar deudas. Hoy en día, los números negativos son de uso cotidiano. Los naturales dan lugar así a los *enteros.* Con los enteros se puede multiplicar, sumar y restar.

Con los enteros también se pueden hacer divisiones, siempre que se acepte que las divisiones pueden tener resto. Dado un número natural fijo n, si se divide un entero cualquiera por él, el resto será un número entero entre 0 y n-1. En el conjunto de todos los restos posibles se pueden hacer operaciones, dando lugar a los *enteros modulares.* Hoy en día, muchas de las propiedades de los números enteros se expresan, de manera muy satisfactoria, usando enteros modulares. Si bien estos conjuntos aparecieron definidos de manera clara hace poco tiempo (desde una perspectiva histórica), su uso permite entender más cabalmente a los números enteros, y por ello les dedicamos un capítulo.

Sin embargo, los números enteros no permiten divisiones si no se está dispuesto a tener resto. Si trabajamos en geometría, incluso si se adoptan unidades de medida tales que las cantidades a medir sean enteras, poco se podrá hacer si no se utilizan fracciones, es decir sin introducir los números *racionales.* Por ejemplo, el Teorema de Tales habla de longitudes proporcionales, que inmediatamente dan lugar a las fracciones.

Pero pronto se ve que si se quiere medir distancias, tampoco alcanza con números racionales. Por el Teorema de Pitágoras, la diagonal de un cuadrado cuyo lado mide 1 metro, mide $\sqrt{2}$ metros. Y este número, no es racional. Hacen falta entonces los números *reales.*

Y, a veces, tampoco alcanza con los enteros, los racionales o los reales. Por ejemplo, la ecuación $x^2 + 1 = 0$ no tiene solución en los números reales. Los números *complejos* se introdujeron, precisamente, para resolver este tipo de ecuaciones, aunque fueron mirados con mucha desconfianza durante tres siglos. Hizo falta que matemáticos de la talla de Leonhard Euler y Carl Friedrich Gauss los usaran para que la comunidad científica dejara de lado los prejuicios. Hoy en día, no sólo se usan para resolver este tipo de ecuaciones. Las ecuaciones de James Clerk Maxwell, por ejemplo, que explican los campos electromagnéticos, precisan de los números complejos.

Si bien las nociones de números naturales, enteros, racionales o reales eran saber popular en el siglo XVII, cuando Isaac Newton y Gottfried Leibniz introdujeron el cálculo infinitesimal, las fuertes críticas que recibió esta teoría, por el obispo George Berkeley en el siglo XVIII, entre otros, obligaron a sentar bases precisas para todos estos conjuntos numéricos. Ésta fue una empresa de grandes dimensiones: los reales se definieron a partir de los racionales, y estos a partir de los enteros, que a su vez salen de los naturales. ¿Y los naturales? La noción de número natural es tan . . . ¡natural! . . . que es sumamente difícil definirlos de manera formal y sin utilizar otros conjuntos anteriores. Fue finalmente Giuseppe Peano quien en 1889 los introdujo axiomáticamente en su libro *Arithmetices principia, nova methodo exposita.*

Una vez definidos los naturales, la definición de los enteros y los racionales es sencilla. Los reales, en cambio, son materia mucho más delicada. Hay distintas definiciones posibles de los números reales, con distintos grados de formalidad. Desde "los puntos de una recta" hasta las *cortaduras de Dedekind* (propuestas por Julius Dedekind a comienzos del siglo XX), pasando por definiciones axiomáticas, o más implícitas como "números con desarrollos decimales infinitos". Los introducimos como clases de equivalencias de sucesiones crecientes y acotadas de números racionales. Esta forma de hacerlo, aunque es técnica y requiere una gran capacidad de abstracción, permite definir las operaciones fácilmente. Para "suavizar" su introducción, primero se los presenta de manera algo más informal, utilizando la noción de límite. También se mencionan otras definiciones posibles, entre ellas la de los desarrollos decimales infinitos.

Si se cuenta con los reales, los números complejos se pueden presentar algebraicamente, como sumas $a + bi$, donde a y b son números reales e i es una solución de la ecuación $x^2 + 1 = 0$. Ésta es la forma en que los presentó William Rowan Hamilton en la primera mitad del siglo XIX, trescientos años después de que Gerolamo Cardano y Lodovico Ferrari los utilizaran por primera vez. Y ésta es la forma en que los conocemos hoy.

Los conjuntos de números que se usan hoy en día no se reducen a los que presentamos aquí: naturales, enteros, enteros modulares, racionales, reales y complejos. Dependiendo del problema que se intente resolver, se utilizan muchos otros. Como ejemplo, basta mencionar a los *cuaterniones* (introducidos por Hamilton en 1843, que se utilizan para describir de manera algebraica movimientos del espacio, como rotaciones, traslaciones u homotecias) y a los *surreales* (introducidos por John Conway y Donald Knuth en 1974, que se utilizan en teoría de juegos). No obstante, estos conjuntos se usan en medida mucho menor, y los que presentamos bastan para la gran mayoría de las aplicaciones.

0. Conjuntos y relaciones

En este capítulo presentamos las nociones elementales que utilizaremos a lo largo del libro.

□ 1. Conjuntos

La noción básica con la que vamos a trabajar es la de *conjunto*. A nuestros fines, un *conjunto* es una colección de objetos sin orden ni repeticiones. Por ejemplo:

- $\mathcal{A}_1 = \{1, 2, 3\}$.
- $\mathcal{A}_2 = \{\pi, e\}$.
- $\mathcal{A}_3 = \{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$.
- $\mathcal{A}_4 = \{1, \heartsuit, \pi\}$.

También hay conjuntos infinitos, como el conjunto de los *números naturales*, con el que trabajaremos en el capítulo 1. Este conjunto se suele llamar $\mathbb{N}$, y es el conjunto $\{1, 2, 3, 4, 5, \ldots\}$.

Al conjunto que no tiene ningún elemento lo llamamos *conjunto vacío* y lo representamos con el símbolo $\emptyset$.

Una propiedad importante que tienen los conjuntos es que dado un elemento cualquiera se puede saber si está en el conjunto o no. Si a está en el conjunto $\mathcal{A}$ decimos que a *pertenece* a $\mathcal{A}$ y escribimos $a \in \mathcal{A}$. En caso contrario decimos que a *no pertenece* a $\mathcal{A}$ y escribimos $a \notin \mathcal{A}$. Por ejemplo, $2 \in \mathcal{A}_1$ pero $2 \notin \mathcal{A}_2$; $17 \in \mathbb{N}$ y $\heartsuit \notin \emptyset$.

Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos, decimos que $\mathcal{A}$ está *incluido* en $\mathcal{B}$, y escribimos $\mathcal{A} \subset \mathcal{B}$, si todos los elementos del conjunto $\mathcal{A}$ pertenecen al conjunto $\mathcal{B}$. Por ejemplo, $\mathcal{A}_1 \subset \mathbb{N}$, pero $\mathcal{A}_2 \not\subset \mathcal{A}_4$ porque $e \notin \mathcal{A}_4$.

En los ejemplos anteriores, los conjuntos fueron definidos listando sus elementos. Esta manera de dar un conjunto se llama *definición por extensión*. Hay otra forma de hacerlo: por *comprensión*, que consiste en dar una propiedad que satisfacen sus elementos y sólo ellos. Por ejemplo: el conjunto $\{1, 2\}$ se puede también definir por $\{x \in \mathcal{A}_1 : x < 3\}$, que se lee "los x que pertenecen a $\mathcal{A}_1$ tales que $x < 3$", y define el conjunto de todos los elementos de $\mathcal{A}_1$ que son menores que 3; es decir, $\{1, 2\}$. Por supuesto, este conjunto se podría haber definido de otras maneras, como $\{x \in \mathcal{A}_1 : x \neq 3\}$, $\{x \in \mathbb{N} : x^2+2 = 3x\}$, etc. El conjunto $\{y \in \mathcal{A}_3 : y \text{ es negro}\}$ es el conjunto $\{\spadesuit, \clubsuit\}$.

Operaciones entre conjuntos. Los profesores de gimnasia de la Escuela 314 quieren armar, para una competencia, un equipo de fútbol de jugadores entre 14 y 16 años, y uno de básquet de jugadores entre 15 y 17. Para armar los equipos, la dirección del colegio les entregó una lista con los alumnos entre 14 y 16 años, y otra con los alumnos entre 15 y 17.

Para citar a los alumnos a que se prueben, los profesores quieren armar cuatro listas, formadas por los alumnos que pueden: (1) integrar ambos equipos, (2) integrar alguno de los equipos, (3) integrar sólo el equipo de fútbol, (4) integrar sólo el equipo de básquet.

Para resolver problemas como éste, se utilizan ciertas operaciones entre conjuntos.

Dados dos conjuntos A y B, se definen:

- la *unión* de A y B, que es el conjunto formado por los elementos que pertenecen a uno de ellos o a ambos, y se escribe $A \cup B$;
- la *intersección* de A y B, que es el conjunto formado por los elementos que pertenecen simultáneamente a A y a B, y se escribe $A \cap B$;
- la *diferencia* entre A y B, que es el conjunto formado por los elementos que pertenecen a A pero no a B, y se escribe $A \setminus B$ o $A - B$.

Dos conjuntos se dicen *disjuntos* si su intersección es el conjunto vacío. Se dice que un conjunto A es la *unión disjunta* de dos conjuntos B y C si es la unión de ellos ($A = B \cup C$) y además B y C son disjuntos. Un conjunto es la unión disjunta de varios si es la unión de ellos y los conjuntos son disjuntos dos a dos. Por ejemplo: {1,2,3,4,5,6} es la unión disjunta de {1,4}, {2,3,6} y {5}, pero no es la unión disjunta de {1,4}, {1,2,3,6} y {3,5}, pues por ejemplo {1,4} ∩ {1,2,3,6} = {1} y por lo tanto no son disjuntos.

Ejercicio 1. Siguiendo con el ejemplo anterior, si llamamos $\mathcal{A}$ al conjunto de alumnos entre 14 y 16 años y $\mathcal{B}$ al conjunto de alumnos entre 15 y 17, describir las listas (1), (2), (3) y (4) en términos de operaciones entre $\mathcal{A}$ y $\mathcal{B}$.

Producto cartesiano. Lorena irá al cine con un amigo. Quiere elegir qué ropa ponerse entre tres pantalones (un jean azul, un jean gris y un pantalón blanco), cuatro remeras (dos musculosas, una blanca y una negra, y dos remeras de manga corta, una rosa y la otra celeste) y dos pares de calzado (unas sandalias y unos zapatos). Para esto, invita a sus amigas y les muestra cómo le quedan todas las combinaciones posibles. La noción que necesitamos introducir en este caso es la de producto cartesiano.

Si A y B son conjuntos, definimos el *producto cartesiano* de A y B como el conjunto formado por los pares ordenados (a, b) donde a pertenece a A y b pertenece a B. Escribimos este conjunto como $A \times B$.

Por ejemplo:

$\mathcal{A}_1 \times \mathcal{A}_2 = \{(1, \pi), (1, e), (2, \pi), (2, e), (3, \pi), (3, e)\}$.
$\mathcal{A}_2 \times \mathcal{A}_2 = \{(\pi, \pi), (\pi, e), (e, \pi), (e, e)\}$.
{♢, ♡, ♠, ♣} × {A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J,Q,K} representa la baraja francesa.

De manera similar se define el producto cartesiano de varios conjuntos. Por ejemplo, $\{a, b, c\} \times \{1, 2\} \times \{\alpha, \beta\} = \{(a, 1, \alpha), (b, 1, \alpha), (c, 1, \alpha), (a, 2, \alpha), (b, 2, \alpha), (c, 2, \alpha), (a, 1, \beta), (b, 1, \beta), (c, 1, \beta), (a, 2, \beta), (b, 2, \beta), (c, 2, \beta)\}$.

Si definimos los conjuntos $H = \{0, 1, 2, \ldots, 22, 23\}$, $M = \{0, 1, 2, \ldots, 58, 59\}$ y $S = M$, la hora del día se puede representar por un elemento del conjunto $H \times M \times S$.

Ejercicio 2. Escribir el conjunto de combinaciones de ropa para Lorena como producto cartesiano de conjuntos y dar este conjunto por extensión.

2. Relaciones

Los profesores de gimnasia de la Escuela 314 van a probar a los alumnos para el equipo de fútbol. Los alumnos se pueden anotar para probarse como arquero, defensor, mediocampista o delantero (se pueden anotar en más de un puesto). Los profesores comenzaron a usar la palabra *versátil* para referirse a los alumnos: dicen que un alumno es más versátil que otro si el primero se anotó en todos los puestos en los que se anotó el segundo y por lo menos uno más. Por ejemplo, si Pablo se anotó como arquero y delantero, y Andrés se anotó como arquero, mediocampista y delantero, Andrés es más versátil que Pablo. La manera de formalizar esta situación, en matemática, es utilizando el concepto de *relación en un conjunto*.

Si A y B son conjuntos, una *relación* de A en B es un subconjunto del conjunto $A \times B$.

Si $\mathcal{R}$ es una relación de $\mathcal{A}$ en $\mathcal{B}$, dados $a \in \mathcal{A}$ y $b \in \mathcal{B}$ decimos que *a está relacionado con b* y escribimos $a\mathcal{R}b$ si el par $(a, b) \in \mathcal{R}$. Si el par $(a, b) \notin \mathcal{R}$ decimos que *a no está relacionado con b* y escribimos $a \not\mathcal{R} b$. Por ejemplo, $\mathcal{R} = \{(1, \pi), (1, e), (2, e)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ es una relación de $\mathcal{A}_1$ en $\mathcal{A}_2$. En este caso, 1 está relacionado con π y con e, pero 3 no está relacionado con ningún elemento de $\mathcal{A}_2$.

Relaciones en un conjunto. Si $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ decimos que $\mathcal{R}$ es una relación en $\mathcal{A}$. Por ejemplo, $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$ es una relación en $\mathcal{A}_1$. Observemos que esta relación puede definirse también como $\mathcal{R} = \{(a_1, a_2) \in \mathcal{A}_1 \times \mathcal{A}_1 : a_1 < a_2\}$.
Dado un conjunto $\mathcal{A}$ y una relación $\mathcal{R}$ en $\mathcal{A}$ decimos que:

- $\mathcal{R}$ es *reflexiva* si el par $(a, a) \in \mathcal{R}$ para todo $a \in \mathcal{A}$.
- $\mathcal{R}$ es *simétrica* si para todo par $(a, b) \in \mathcal{R}$ vale que el par $(b, a) \in \mathcal{R}$.
- $\mathcal{R}$ es *transitiva* si para todos los pares $(a, b) \in \mathcal{R}$, $(b, c) \in \mathcal{R}$ vale que $(a, c) \in \mathcal{R}$.
- $\mathcal{R}$ es *antisimétrica* si para todo par de elementos $(a, b) \in \mathcal{A}$ con $a \neq b$, si $(a, b) \in \mathcal{R}$ entonces $(b, a) \notin \mathcal{R}$.

Por ejemplo:

1. $\mathcal{R} = \{(\diamondsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\heartsuit,\diamondsuit), (\heartsuit,\spadesuit), (\spadesuit,\heartsuit), (\heartsuit,\clubsuit), (\clubsuit,\heartsuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit)\}$ en $\mathcal{A}_3$. Aunque $\diamondsuit \mathcal{R} \diamondsuit$, $\mathcal{R}$ no es reflexiva porque por ejemplo $\heartsuit \not\mathcal{R} \heartsuit$. Esta relación es simétrica porque para cada par de elementos que pertenece a $\mathcal{R}$, el par con los elementos en orden inverso también pertenece a $\mathcal{R}$ (convencerse). Esta relación no es transitiva porque $\diamondsuit \mathcal{R} \heartsuit$, $\heartsuit \mathcal{R} \spadesuit$ pero $\diamondsuit \not\mathcal{R} \spadesuit$.

Observemos que para afirmar que una relación es transitiva es necesario considerar todas las posibilidades (en este ejemplo, si bien $\heartsuit \mathcal{R} \spadesuit$, $\spadesuit \mathcal{R} \clubsuit$ y $\heartsuit \mathcal{R} \clubsuit$, la relación no es transitiva). Esta relación no es antisimétrica porque $(\diamondsuit, \heartsuit) \in \mathcal{R}$ y $(\heartsuit, \diamondsuit) \in \mathcal{R}$.

2. La relación "ser más versátil que", ideada por los profesores de gimnasia de la Escuela 314, no es reflexiva ni simétrica, pero sí es transitiva y antisimétrica.

3. $\mathcal{R} = \{(\heartsuit,\heartsuit), (\heartsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\diamondsuit,\diamondsuit), (\spadesuit,\spadesuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit), (\clubsuit,\clubsuit)\}$ en $\mathcal{A}_3$. Esta relación es reflexiva, simétrica y transitiva pero no es antisimétrica. Observemos que $\mathcal{R}$ se puede definir por comprensión diciendo que dos elementos de $\mathcal{A}_3$ están relacionados si son del mismo color. Usando esta definición alternativa es más fácil verificar que valen las propiedades.

4. $\mathcal{R} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ en $\mathcal{A}_1$ es reflexiva, antisimétrica y transitiva.

Las relaciones que son reflexivas, simétricas y transitivas son importantes y tienen un nombre especial: se llaman relaciones de *equivalencia*. Otro tipo de relaciones importante es el de las relaciones de *orden*, que son las reflexivas, antisimétricas y transitivas.

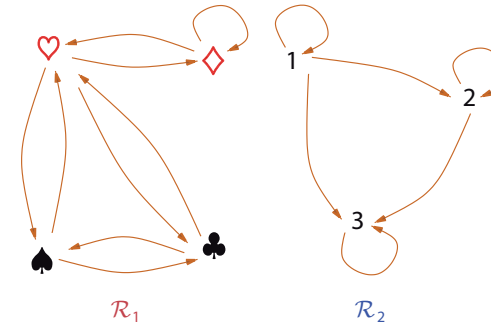


Figura 1. *Gráficos de relaciones.*

Ejemplos

1. Los profesores de gimnasia dicen que un alumno es "tan versátil como" otro si ambos se anotaron para probarse en los mismos puestos. Ésta es una relación de equivalencia.
2. Dos números naturales están relacionados si tienen la misma paridad (es decir, si son ambos pares o ambos impares). Esta es otra relación de equivalencia.
3. La relación $\mathcal{R}$ del ejemplo 4 de la lista anterior es una relación de orden.
4. La relación $a \leq b$ en los números naturales es una relación de orden.

Representación gráfica. A veces resulta cómodo representar una relación $\mathcal{R}$ en un conjunto $\mathcal{A}$ de manera gráfica. Para esto se ubican los elementos del conjunto $\mathcal{A}$ y se dibuja una flecha que sale de un elemento $a \in \mathcal{A}$ y llega a otro elemento $b \in \mathcal{A}$ para cada par de elementos tales que $a\mathcal{R}b$ (si $a\mathcal{R}a$ queda un "rulito" que sale de a y termina en a).

Por ejemplo, las relaciones
$\mathcal{R}_1 = \{(\diamondsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\heartsuit,\diamondsuit), (\heartsuit,\spadesuit), (\spadesuit,\heartsuit), (\heartsuit,\clubsuit), (\clubsuit,\heartsuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit)\}$ en $\mathcal{A}_3$ y
$\mathcal{R}_2 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ en $\mathcal{A}_1$ pueden representarse por los gráficos de la Figura 1.

3. Particiones

En un ejemplo anterior, consideramos la relación $\mathcal{R}$ en el conjunto $\mathbb{N}$ definida por $a\mathcal{R}b$ si a y b tienen la misma paridad. Esta relación define dos clases de números naturales: los números pares y los números impares. A los números pares los podemos caracterizar por la propiedad de estar relacionados con el número 2, mientras que a los impares los podemos caracterizar por la propiedad de estar relacionados con el número 1. Así tenemos:

$$\mathbb{N} = \{n \in \mathbb{N} : n\mathcal{R}1\} \cup \{n \in \mathbb{N} : n\mathcal{R}2\}$$

También podemos definir los números pares como los números naturales relacionados con el número 4 o, más generalmente, con cualquier número natural par 2, 4, 6, ... Lo importante es que la relación de equivalencia partió al conjunto de números naturales como unión disjunta de dos subconjuntos. Además, todos los elementos de cada subconjunto están relacionados entre sí.

Veamos otro ejemplo de cómo una relación de equivalencia nos da una partición de un conjunto. Los docentes de la Escuela 314 deciden programar ciertas actividades extracurriculares. Para poder asignar a sus alumnos a cada una de estas actividades precisan saber cuán ocupado está cada alumno. Para ello, les entregan un formulario a los alumnos donde deben decir cuántas actividades extras ya realizan por cuenta propia (por actividad extra consideran deportes, idiomas, música y cualquier otra actividad que demande al menos 2 horas semanales). Definen en el conjunto de alumnos una relación diciendo que el alumno A está relacionado con el alumno B si ambos realizan el mismo número de actividades.
Verificar que ésta es una relación de equivalencia.

Se consideran los subconjuntos A_n = {alumnos que realizan n actividades}, para n = 0, 1, 2, ..., 12 (ninguno de los alumnos realiza más de 12 actividades). Es claro que estos conjuntos son disjuntos dos a dos (cada alumno desarrolla un único número de actividades y éste determina en qué conjunto está) y la unión de ellos da todo el conjunto de alumnos. Luego, el conjunto de alumnos se parte como una unión disjunta de los subconjuntos A_n.

Si $\mathcal{A}$ es un conjunto y $\mathcal{R}$ una relación de equivalencia en el conjunto $\mathcal{A}$, para cada elemento $a \in \mathcal{A}$ definimos su clase de equivalencia como $[a] = \{b \in \mathcal{A} : a\mathcal{R}b\}$.

Éste es un subconjunto del conjunto $\mathcal{A}$.

Por ejemplo, si $\mathcal{A} = \mathbb{N}$ y la relación es tener la misma paridad, [1] es el conjunto de los números naturales impares, es decir, [1] = {1, 3, 5, ...}. Las clases de equivalencia [3], [5], [7], etcétera, también son el conjunto de los números naturales impares. Por otro lado, [2] es el conjunto de los números naturales pares, y lo mismo ocurre con [4], [6], [8], etcétera. Así, $\mathbb{N}$ queda partido en dos clases de equivalencia con esta relación: [1] y [2].

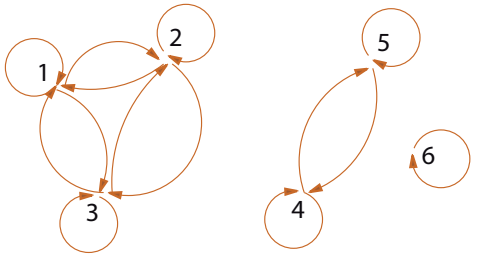


Figura 2. *Relación $\mathcal{R}$ en $\mathcal{A}$.*

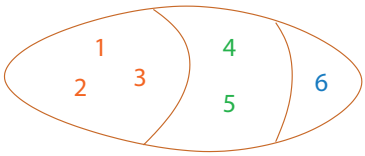


Figura 3. *Partición de {1, 2, 3, 4, 5, 6}.*

Veamos el siguiente ejemplo: consideremos en el conjunto $\mathcal{A} = \{1, 2, 3, 4, 5, 6\}$ la relación de equivalencia $\mathcal{R} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2), (4, 5), (5, 4)\}$. En la figura 2 se da la relación gráficamente.

Las clases de equivalencia para esta relación son:

$$[1] = [2] = [3] = \{1, 2, 3\}$$
$$[4] = [5] = \{4, 5\}$$
$$[6] = \{6\}$$

Así, el conjunto $\mathcal{A}$ se parte en los subconjuntos:

$$\mathcal{A} = \{1, 2, 3\} \cup \{4, 5\} \cup \{6\}.$$

donde para cada elemento de $\mathcal{A}$ consideramos todos los que están relacionados con él (ver figura 3).

En general, si $\mathcal{R}$ es una relación de equivalencia en el conjunto $\mathcal{A}$, si a y b son elementos de $\mathcal{A}$, sus clases de equivalencia son o bien iguales, o bien disjuntas. Es decir que: $[a] = [b]$ o $[a] \cap [b] = \emptyset$. El conjunto $\mathcal{A}$ se parte en las clases de equivalencia dadas por la relación $\mathcal{R}$.

□ 4. Funciones

Los profesores de gimnasia de la Escuela 314 definieron un equipo de fútbol titular. A los convocados les dieron las camisetas del 1 al 11. En términos matemáticos, a cada elemento del conjunto {1, 2, 3, ... , 10, 11} le asignaron un elemento del conjunto de alumnos.

Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos, una *función* de $\mathcal{A}$ en $\mathcal{B}$ es una relación $f \subset \mathcal{A} \times \mathcal{B}$ que satisface que para cada $a \in \mathcal{A}$ hay un único $b \in \mathcal{B}$, tal que $(a, b) \in f$. En este caso, usualmente se escribe $f(a) = b$. Si $f \subset \mathcal{A} \times \mathcal{B}$ es una función, también se escribe $f: \mathcal{A} \to \mathcal{B}$.

Ejemplos. Como antes, $\mathcal{A}_1 = \{1, 2, 3\}$ y $\mathcal{A}_2 = \{\pi, e\}$.

1. La relación $f = \{(1, \pi), (2, e), (3, e)\}$ es una función de $\mathcal{A}_1$ en $\mathcal{A}_2$. En este caso, $f(1) = \pi$, $f(2) = e$ y $f(3) = e$.
2. La relación $\{(1, \pi), (1, e), (2, e), (3, \pi)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ no es una función, porque $1 \in \mathcal{A}_1$ está relacionado con dos elementos de $\mathcal{A}_2$.
3. La relación $\{(1, \pi), (2, e)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ no es una función, porque $3 \in \mathcal{A}_1$ no está relacionado con ningún elemento de $\mathcal{A}_2$.
4. La asignación de las camisetas de fútbol a los alumnos de la Escuela 314 es una función.

En general, una función no se describe listando todos sus pares, sino dando una regla que permite obtener $f(a)$ en términos de a.

Ejemplos

1. La función $f: \mathcal{A}_1 \to \mathcal{A}_1$, $f = \{(1, 3), (2, 2), (3, 1)\}$ se puede describir por $f(a) = 4 - a$.
2. La función $g: \mathbb{N} \to \mathbb{N}$, $g(a) = 3a + 1$, está formada por los pares (1, 4), (2, 7), (3, 10), (4, 13), ...

□ 5. Operaciones

El equipo de fútbol de la Escuela 314 participa de un campeonato intercolegial. Una vez que todos los equipos jugaron dos partidos, los organizadores del torneo quieren armar las estadísticas. Para calcular la cantidad de goles a favor de cada equipo, deben sumar la cantidad de goles convertidos por el equipo en el primer partido con la de goles convertidos en el segundo. En este caso, la noción matemática involucrada es la de *operación*.

Una *operación en un conjunto* $\mathcal{A}$ es una función de $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$. Si $*: \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ es una operación, usualmente se escribe $a * b$ para el valor de $*$ en el par (a, b).

Ejemplos

1. La suma de números naturales es una operación. De hecho, cuando uno escribe por ejemplo 3 + 5 = 8, está diciendo que la función + le asigna el 8 al par (3, 5).
2. El producto de números naturales es otra operación.
3. La *potencia de números naturales*, que al par (a, b) le asigna a^b, es otra operación.

A veces es cómodo dar una operación mediante una tabla de doble entrada. A la izquierda se pone el primer elemento de cada par y arriba, el segundo. Por ejemplo, si $\mathcal{C} = \{0, 1, 2, 3, 4\}$, podemos definir las operaciones $\circ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ y $- : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ por

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$-$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

Esto quiere decir, por ejemplo, que $0 \circ 1 = 0$, que $2 \circ 3 = 1$, que $2 - 1 = 1$ y que $1 - 2 = 4$.

Si $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ es una operación, decimos que:

1. $*$ es *asociativa* si $a * (b * c) = (a * b) * c$ para todos los a, b, c en $\mathcal{A}$;
2. $*$ es *conmutativa* si $a * b = b * a$ para todos los a, b en $\mathcal{A}$;
3. un elemento $e \in \mathcal{A}$ es *un elemento neutro de* $*$ si $a * e = a$ y $e * a = a$ para todo a en $\mathcal{A}$.

La suma y el producto de números naturales son operaciones conmutativas y asociativas. El producto tiene un elemento neutro, que es el número uno. La suma, en cambio, no lo tiene, si se considera que el cero no pertenece al conjunto de los naturales. En cambio si agregamos el cero a los números naturales, éste resulta ser el elemento neutro de la suma.

La potencia de números naturales no es conmutativa porque, por ejemplo: $2^3 \neq 3^2$.

$$2^{(3^2)} \neq (2^3)^2$$

Tampoco es asociativa porque, por ejemplo:

Ejercicio 3. Explicitar el conjunto $\mathcal{A}$ y la operación utilizada para el cálculo de goles a favor planteado al comienzo de esta sección,

Ejercicio 4. Determinar si la operación $\circ$ en $\mathcal{C}$ definida en la tabla anterior es conmutativa, asociativa o tiene elemento neutro. Hacer lo mismo para $-$.

Cuando una operación $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ tiene un elemento neutro e, decimos que un elemento $a \in \mathcal{A}$ es un *inverso* de $b \in \mathcal{A}$ si $a * b = e$ y $b * a = e$. Por ejemplo, 1 es el elemento neutro de la operación $\circ$ en $\mathcal{C}$, y el inverso de 2 es 3 para esta operación. En este caso, 0 no tiene inverso.

□ 6. Sucesiones

Todos los días, Lorena y sus amigas Magalí y Natalia se reúnen en la casa de una de ellas: un día en lo de Lorena, al día siguiente en lo de Magalí, el tercero en lo de Natalia, y al cuarto día vuelven a empezar reuniéndose en lo de Lorena. Lorena quiere saber en qué casa se van a reunir el día del amigo (el 20 de julio), sabiendo que el día 1 de julio se

1 Lorena	6 Natalia	11 Magalí	16 Lorena
2 Magalí	7 Lorena	12 Natalia	17 Magalí
3 Natalia	8 Magalí	13 Lorena	18 Natalia
4 Lorena	9 Natalia	14 Magalí	19 Lorena
5 Magalí	10 Lorena	15 Natalia	20 Magalí

reunieron en su casa. Para esto, Lorena escribe:
Es decir, el día del amigo se reunirán en la casa de Magalí. Matemáticamente, lo que hizo Lorena es asignarle a cada número natural un elemento del conjunto {Lorena, Magalí, Natalia} (en realidad lo hace sólo para los primeros 20 números naturales, aunque podría extender la definición a todos ellos).

Si X es un conjunto, una *sucesión de elementos* de X es una función $f : \mathbb{N} \to X$.

En el ejemplo anterior X es el conjunto de Lorena y sus amigas. En el resto del libro las sucesiones con las que trabajaremos serán principalmente *sucesiones de números*, es decir,

el conjunto X será un conjunto de números.

Si $f: \mathbb{N} \to X$ es una sucesión y $n \in \mathbb{N}$, escribiremos a_n en lugar de $f(n)$. El elemento a_n se denomina el *enésimo término de la sucesión*. A partir de ahora, escribiremos $(a_n)_{n\geq 1}$ en lugar de f. Por lo tanto, los valores $f(1), f(2), \ldots, f(n), \ldots$ que toma la sucesión f serán expresados como $a_1, a_2, \ldots, a_n, \ldots$

Ejemplos

1. $a_n = n$.
2. $a_n = 1/n$.
3. $a_n = 2^n$.
4. $a_n = n^2$.
5. $a_n = (-1)^n$.

Es importante notar que en una sucesión dada los términos se pueden repetir. Esto sucede, por ejemplo, en la sucesión de Lorena. Las sucesiones de los ejemplos tienen la peculiaridad de que existe una *fórmula cerrada*; es decir, hay una *ley* o *fórmula q*ue dice cómo calcular a_n solamente en función de n.

Ejercicio 5. Encontrar una fórmula cerrada para la sucesión cuyos términos son 1, 2, 1, 2, 1, 2, 1, 2, . . .

1. Números naturales

□ 1. Nociones básicas

Los números naturales son, tal como los conocemos, 1, 2, 3, 4, 5, . . . Si bien todos tenemos esta idea intuitiva, más adelante, en la sección 4, daremos una definición precisa.

Llamamos $\mathbb{N}$ al conjunto de los números naturales, es decir:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

Estos números se usan a diario para contar. Matemáticamente, contar significa decir cuántos elementos tiene un conjunto. Por ejemplo, el conjunto {♢, ♡, ♠, ♣} tiene 4 elementos. ¿Cuántos elementos tiene el conjunto vacío?

Como el conjunto vacío no posee ningún elemento, necesitamos un símbolo nuevo que represente la cantidad de elementos de este conjunto. Este símbolo es el 0. Llamamos $\mathbb{N}_0$ al conjunto de los números naturales con el cero, o sea:

$$\begin{aligned} \mathbb{N}_0 &= \mathbb{N} \cup \{0\} \\ &= \{0, 1, 2, 3, 4, 5, \ldots\}. \end{aligned}$$

El conjunto de los números naturales tiene dos operaciones importantes: *suma y producto*. Como mencionamos en el capítulo anterior, la suma y el producto de números naturales son operaciones asociativas y conmutativas. El 1 es el neutro para el producto, y la suma no tiene elemento neutro en $\mathbb{N}$, pero sí en $\mathbb{N}_0$: el 0.

Además, estas dos operaciones están relacionadas por la siguiente propiedad: para toda terna de números naturales *a, b, c,* vale que:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Esta propiedad se llama *distributiva* del producto sobre la suma.

Veamos cómo se pueden usar estas propiedades para calcular el cuadrado de la suma de dos números naturales:

$$\begin{aligned} (a + b)^2 &= (a + b) \cdot (a + b) \\ &= (a + b) \cdot a + (a + b) \cdot b \\ &= a \cdot a + b \cdot a + a \cdot b + b \cdot b \\ &= a^2 + a \cdot b + a \cdot b + b^2 \\ &= a^2 + 2 \cdot a \cdot b + b^2 \end{aligned}$$

Esto también puede verse geométricamente como muestra el dibujo de la figura 1.

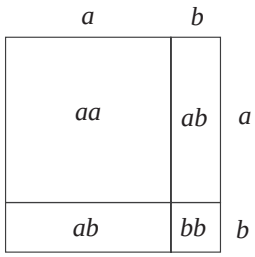


Figura 1. *El cuadrado de una suma.*

Ejercicio 1.1. Encontrar una fórmula para $(a + b)^3$.

□ 2. Inducción

Lorena y sus amigas se saludan en la puerta de la escuela con un beso. Un día, Lorena llega primera y quiere contar cuántos besos se dan en total todas las amigas (ella incluida). Cuando llega su primera amiga, Lorena la saluda y cuenta un beso. Cuando llega la segunda amiga, saluda a ambas, y Lorena cuenta dos besos más; en total, 3 besos. Cuando llega la tercera amiga, saluda a las tres y Lorena cuenta 3 besos más. En total, 6 besos. A medida que van llegando, Lorena descubre que si llegaron n amigas, la cantidad de besos es $1 + 2 + 3 + \ldots + n$. Esto nos lleva al siguiente problema: ¿cuánto da la suma de los primeros n números naturales?

A partir de la figura 2 podemos ver que:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Más adelante, daremos una demostración distinta de esta igualdad, que nos servirá para ilustrar el principio de inducción.

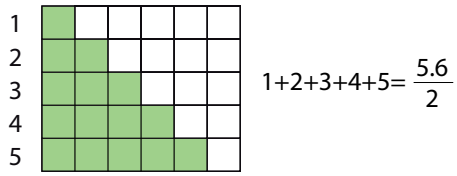


Figura 2. *La suma de los primeros números naturales.*

Consideremos ahora el siguiente problema: ¿cuánto es $1 + 2 + 2^2 + \ldots + 2^n$? Calculemos los primeros valores:

$$\begin{aligned} 1 &= 1 && n=0 \\ 1+2 &= 3 && n=1 \\ 1+2+4 &= 7 && n=2 \\ 1+2+4+8 &= 15 && n=3 \\ 1+2+4+8+16 &= 31 && n=4 \end{aligned}$$

Aunque a simple vista estos números no parecen conocidos, ¿qué pasa si a los resultados obtenidos les sumamos 1? Obtenemos que las primeras sumas, más 1, dan 2, 4, 8, 16, 32, que son potencias de 2. Parece ser que la suma $1+2+\ldots+2^n = 2^{n+1}-1$. ¿Cómo podemos convencernos de que esta fórmula vale?

Veamos qué pasa para $n = 5$:

$$\begin{aligned} \underbrace{1+2+4+8+16}_{2^5-1}+32 &= 2\cdot 2^5 - 1 \\ &= 2^6 - 1 \end{aligned}$$

Podemos repetir este razonamiento para $n = 6$, $n = 7$, ... O sea, si sabemos que vale:

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1,$$

entonces:

$$\underbrace{1 + 2 + \cdots + 2^n}_{2^{n+1}-1} + 2^{n+1} = 2 \cdot 2^{n+1} - 1$$
$$= 2^{n+2} - 1 \qquad (1)$$

Vemos así que si la fórmula es válida para un número natural n, también lo es para el siguiente número natural $n + 1$. ¿Alcanza esto para concluir que la fórmula vale para todos los números naturales?

La respuesta es sí. En la próxima sección vamos a formalizar este tipo de argumentos para poder aplicarlos en la demostración de propiedades sobre los números naturales.

□ 3. Principio de inducción

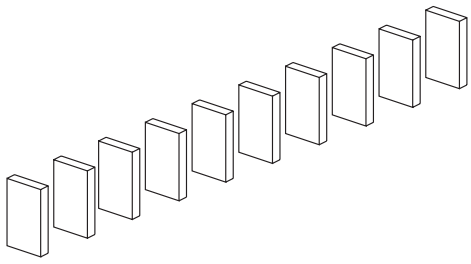


Figura 3. *Las fichas dispuestas para ser tiradas.*

Una herramienta muy usada para demostrar afirmaciones sobre los números naturales es el *principio de inducción*. Imaginemos una hilera de fichas de dominó paradas como en el dibujo de la figura 3.

Las fichas están dispuestas de manera que si cae una, tira a la siguiente. Entonces, podemos hacer que todas se caigan empujando solo la primera, como en la figura 4. Esta idea de las fichas cayendo es la base del principio de inducción.

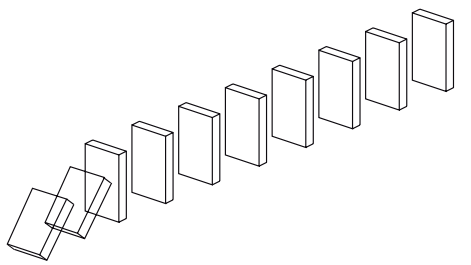


Figura 4. *Las fichas comienzan a caer.*

Principio de inducción. Supongamos que tenemos para cada número natural una afirmación $P(n)$ y queremos ver que todas estas afirmaciones son válidas. Si se puede demostrar que:

1. $P(1)$ es cierta,
2. si $P(n)$ es cierta,

entonces $P(n+1)$ también lo es, entonces $P(n)$ vale para todo $n \in \mathbb{N}$.

La parte 2. corresponde a que si una ficha de dominó cae, entonces tira la siguiente. La parte 1. corresponde a tirar la primera ficha. El hecho de que todas las fichas caigan es lo que explica que todas las afirmaciones $P(n)$ sean ciertas.

Veamos cómo funciona el principio de inducción en un ejemplo. De hecho, lo que hicimos al calcular la suma de las primeras potencias de 2 en la sección anterior fue aplicar, sin mencionarlo, el principio de inducción. Más precisamente, para cada $n \in \mathbb{N}$ afirmamos que $1 + 2 + ... + 2^n = 2^{n+1} - 1$. Esta afirmación es $P(n)$.

El principio nos dice que basta con verificar:

- $P(1) : 1 + 2 = 2^2 - 1$, lo cual es cierto.
- Supongamos que es cierto $P(n)$, es decir que $1 + 2 + \ldots + 2^n = 2^{n+1} - 1$. A partir de aquí debemos demostrar que $P(n + 1)$ es cierto, es decir que $1 + 2 + \ldots + 2^n + 2^{n+1} = 2^{n+2} - 1$. Esto es exactamente lo que hicimos en (1).

Apliquemos el principio de inducción al primer ejemplo de la sección anterior. En este caso $P(n)$ es la afirmación de que la suma de los primeros n números naturales es $\frac{n(n+1)}{2}$.

- $P(1) : 1 = \frac{1\cdot(1+1)}{2}$, lo cual es cierto.
- Supongamos que es cierto $P(n)$, es decir que $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. A partir de aquí, debemos demostrar que $P(n + 1)$ es cierto, es decir que $1 + 2 + \ldots + n + (n + 1) = \frac{(n+1)(n+2)}{2}$. Ahora:

$$\begin{aligned} \underbrace{1+2+\cdots+n}_{\frac{n(n+1)}{2}}+(n+1) &= \frac{n}{2}(n+1)+(n+1) \\ &= (n+1)\left(\frac{n}{2}+1\right) \\ &= (n+1)\left(\frac{n+2}{2}\right) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

Ejercicio 1.2. Probar que para todo número natural n vale que:

$$1 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Muchas veces se quiere probar la validez de afirmaciones $P(n)$ para los números naturales a partir de uno dado. Es decir, imaginemos que queremos probar que $P(n)$ es cierta para $n \geq M$, donde M es un número natural. El principio de inducción se aplica casi igual. La única diferencia es que en lugar de demostrar que $P(1)$ es cierta, demostramos que $P(M)$ es cierta.

Ejemplo. Probemos que la suma de los ángulos interiores de un n-ágono es $180^o(n - 2)$. Esta afirmación sólo tiene sentido si $n \geq 3$. En este caso, $M = 3$. Para probar la fórmula, debemos comenzar por ver que $P(3)$ es cierta. Es decir, que la suma de los ángulos interiores de un triángulo es $180^o(3 - 2) = 180^o$. Esta propiedad de los triángulos es bien conocida y no la demostraremos aquí. Debemos entonces demostrar que si la suma de los ángulos interiores de un n-ágono es $180^o(n - 2)$, entonces la de un $(n + 1)$-ágono es $180^o(n + 1 - 2) = 180^o(n - 1)$. Para ver esto, apelamos a la construcción de la Figura 5. Trazando la diagonal del dibujo, el $(n + 1)$-ágono se separa en un triángulo

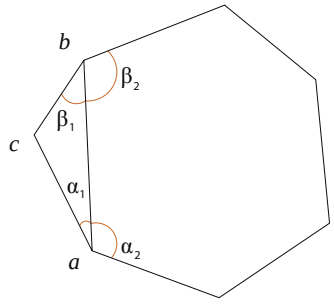


Figura 5. *Separación de un (n + 1)-ágono en un triángulo y un n-ágono.*

y un n-ágono. Observemos que la suma de los ángulos interiores del $(n + 1)$-ágono es la suma de los ángulos interiores del n-ágono más la del triángulo. El ángulo en el vértice a del $(n + 1)$-ágono se separa en α_1 (que es uno de los ángulos del triángulo) y α_2 (que es uno de los ángulos del n-ágono). Lo mismo ocurre con el ángulo en b, que se separa en β_1 y β_2. Como estamos suponiendo que $P(n)$ es cierta, la suma de los ángulos interiores del n-ágono es $180^o(n - 2)$. Por otra parte, la suma de los ángulos interiores del triángulo es 180^o. Entonces, la suma de los ángulos interiores del $(n + 1)$-ágono es $180^o(n - 2) + 180^o = 180^o(n - 2 + 1) = 180^o(n - 1)$.

Veamos otro ejemplo. Queremos probar que para todo $n \geq 8$ vale la desigualdad $2^n \geq 3n^2 + 3n + 1$. Para esto, probamos primero que vale para $n = 8$:

$$2^8 = 256, \quad 3 \cdot 8^2 + 3 \cdot 8 + 1 = 217, \text{ entonces } 2^8 \geq 3 \cdot 8^2 + 3 \cdot 8 + 1$$

Ahora, suponiendo que la desigualdad es válida para n, la probamos para $n+1$. Es decir, probamos que $2^{n+1} \geq 3(n + 1)^2 + 3(n + 1) + 1$. Por un lado:

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &= 2^n + 2^n \end{aligned}$$

Por otro lado:

$$3(n + 1)^2 + 3(n + 1) + 1 = 3n^2 + 6n + 3 + 3n + 3 + 1 = 3n^2 + 3n + 1 + 6n + 6$$

Como estamos asumiendo que $2^n \geq 3n^2+3n+1$, si probamos que $2^n \geq 6n+6$, para todo $n \geq 8$, tendremos que:

$$2^{n+1} = 2^n + 2^n \geq 3n^2 + 3n + 1 + 6n + 6 = 3(n + 1)^2 + 3(n + 1) + 1$$

Veamos, entonces, que $2^n \geq 6n + 6$ para todo $n \geq 8$. Nuevamente, esta propiedad la probamos por inducción. Si $n = 8$, nos queda $2^8 = 256$ y $6 \cdot 8 + 6 = 54$, por lo que la propiedad vale. Si asumimos ahora que vale para n, es decir, que $2^n \geq 6n + 6$, debemos probar que $2^{n+1} \geq 6(n + 1) + 6$. Como suponemos que $n \geq 8$, $2^n \geq 2^8 = 256 \geq 6$, y entonces $2^{n+1} = 2^n + 2^n \geq 6n + 6 + 6 = 6(n + 1) + 6$.

Ejercicio 1.3. Probar que $2^n \geq n^3$ para todo $n \geq 10$.

Ejercicio 1.4. Probar que $3^n \geq 2^{n+1} + n$ para todo $n \geq 3$.

□ 4. Axiomas de Peano

A fines del siglo XIX, Giuseppe Peano[1] dio una definición axiomática de los números naturales. La clave de la definición de Peano es la noción de *sucesor*: todo número natural tiene un sucesor, que se obtiene sumándole 1. Para entender los axiomas de Peano, observemos que el conjunto $\mathbb{N}$ cumple las siguientes propiedades:

[1] Matemático italiano que vivió entre 1858 y 1932. Enseñó en la Universidad de Turín y se dedicó a la investigación de, entre otras cosas, lógica, teoría de conjuntos y ecuaciones diferenciales.

1. El 1 es el único número natural que no es sucesor de ningún número natural.
2. Si a y b son dos números naturales distintos, el sucesor de a es distinto del sucesor de b.
3. Si K es un subconjunto de $\mathbb{N}$ tal que $1 \in K$ y vale que el sucesor de cualquier elemento de K también está en K, entonces $K = \mathbb{N}$.

Peano descubrió que estas propiedades alcanzan para definir a los números naturales, en el sentido de que cualquier conjunto con una función sucesor que satisfaga las 3 propiedades anteriores es "equivalente" al conjunto de números naturales. Formalmente, se puede dar la siguiente definición:

El conjunto de números naturales es un conjunto $\mathbf{P}$ con una función sucesor $S : \mathbf{P} \to \mathbf{P}$ que satisface los siguientes 3 axiomas:

1. $\mathbf{P}$ tiene un único elemento que no es sucesor de otro elemento de $\mathbf{P}$. Llamamos 1 a este elemento.
2. La función S es inyectiva. O sea, si a y b son elementos distintos de $\mathbf{P}$ entonces $S(a)$ es distinto de $S(b)$.
3. Si K es un subconjunto de $\mathbf{P}$ tal que $1 \in K$ y vale que el sucesor de cualquier elemento de K también está en K, entonces $K = \mathbf{P}$

El axioma 3 es equivalente al principio de inducción. Para verlo, supongamos que tenemos un subconjunto K de los números naturales que tiene al 1 y que cumple que si $n \in K$, su sucesor $n+1 \in K$. Llamemos $P(n)$ a la afirmación $n \in K$.

Sabemos que $P(1)$ es cierta y que si $P(n)$ es cierta, $P(n + 1)$ también lo es. Luego por el principio de inducción, $P(n)$ es cierta para todo $n \in \mathbb{N}$, o sea $n \in K$ para todo $n \in \mathbb{N}$. Luego $K = \mathbb{N}$.

Recíprocamente, supongamos que tenemos una afirmación $P(n)$ para cada número natural n que cumple que:

- $P(1)$ es cierta y,
- si $P(n)$ es cierta, $P(n + 1)$ también lo es.

Llamemos K al subconjunto de números naturales n para los que $P(n)$ es cierta.

Luego $1 \in K$. Por otra parte, si $n \in K$, su sucesor $n + 1 \in K$. Con todo esto, por el axioma 3, $K = \mathbb{N}$. Es decir, $P(n)$ es cierta para todo número natural n.

□ 5. Definiciones recursivas

Muchas veces uno necesita definir una sucesión de *manera recursiva*. Esto es, definir un elemento de la sucesión en términos de otros anteriores. Por ejemplo, consideremos la sucesión:

$$a_1 = 2, \quad a_{n+1} = a_n^2 + 1.$$

¿Cómo calculamos a_4? Por definición:

$$a_4 = a_3^2 + 1$$

Luego, conociendo el valor de a_3 podemos calcular a_4. De la misma manera, usando la definición para a_3, tenemos que:

$$a_3 = a_2^2 + 1$$

Repitiendo el proceso para a_2:

$$a_2 = a_1^2 + 1$$

Pero el valor de a_1 lo conocemos, lo que nos permite calcular:

$$\begin{array}{rcccc} a_2 & = & 2^2 + 1 & = & 5 \\ a_3 & = & 5^2 + 1 & = & 26 \\ a_4 & = & 26^2 + 1 & = & 677 \end{array}$$

Este tipo de definiciones, en la que el valor de cada término depende del valor de términos anteriores, se denomina *definición recursiva*. Usualmente, para que la definición esté bien, es necesario precisar el valor de los primeros términos de la sucesión. La cantidad de términos necesarios depende de la definición recursiva. Si cada término de la sucesión depende exclusivamente del término anterior, como en el ejemplo, entonces es necesario definir explícitamente un término (en el ejemplo, definimos $a_1 = 2$ de manera explícita). Si cada término depende de los dos anteriores, serán necesarios dos términos, etcétera. Consideremos otro ejemplo:

$$L_1 = 2, \quad L_2 = 1, \quad L_{n+2} = L_{n+1} + L_n$$

Los primeros términos de esta sucesión son:

$$L_1 = 2,\ L_2 = 1,\ L_3 = 3,\ L_4 = 4,\ L_5 = 7,\ L_6 = 11,\ L_7 = 18,\ L_8 = 29$$

Como se ve, con la información dada se pueden calcular todos los términos de la sucesión. Esta sucesión se conoce como "números de Lucas" (ya que fueron introducidos por Edouard Lucas), y está íntimamente relacionada con la sucesión de Fibonacci, que veremos en la sección siguiente. Como la fórmula recursiva $L_{n+2} = L_{n+1} + L_n$ da un término en función de los dos anteriores, son necesarios dos valores explícitos de la sucesión (L_1 y L_2). De hecho, si cambiásemos el valor de L_1 y L_2 dejando la fórmula recursiva intacta, los valores de la sucesión cambiarían. Si por ejemplo pusiésemos:

$$L'_1 = 1, \quad L'_2 = 5, \quad L'_{n+2} = L'_{n+1} + L'_n$$

Tendríamos:

$$L'_1 = 1,\ L'_2 = 5,\ L'_3 = 6,\ L'_4 = 11,\ L'_5 = 17,\ L'_6 = 28,\ L'_7 = 45,\ L'_8 = 73$$

Una sucesión muy usada en matemática es el factorial. El factorial de un número natural n se escribe $n!$ e, informalmente, se define como:

$$n! = 1 \cdot 2 \cdot 3 \ldots (n-1) \cdot n$$

Por ejemplo, 3! = 1 · 2 · 3 = 6, y 7! = 1 · 2 · 3 · 4 · 5 · 6 · 7 = 5.040.

La definición formal de factorial es:

$$1! = 1, \quad (n+1)! = (n+1) \cdot n!$$

Entonces, por ejemplo:

$$\begin{aligned} 4! &= 4 \cdot 3! \\ &= 4 \cdot 3 \cdot 2! \\ &= 4 \cdot 3 \cdot 2 \cdot 1! \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 24 \end{aligned}$$

Puede generar dudas que una definición recursiva esté bien hecha. El hecho de definir algo en términos de sí mismo no parece muy correcto. Sin embargo, las definiciones recursivas no sólo están bien, sino que muchas veces son necesarias. Y, además, son lo suficientemente formales como para hacerlas con una computadora. Como ejemplo, veamos dos definiciones posibles para el cálculo del factorial en lenguaje Python (elegimos el Python porque es muy sencillo, incluso para quien no lo conoce. De todas maneras, se puede reemplazar por una gran colección de lenguajes que permiten definiciones recursivas).

Una primera posible definición de factorial es:

```
def factorial(n):
    f = 1
    for i in range(1,n+1):
        f = f * i
    return f
```

La línea `f=1` pone en la variable *f* el valor 1. Luego, la instrucción: `for i in range(1,n+1):` ejecuta la línea que sigue para todos los valores de *i* entre 1 y *n*. Y la línea que sigue es poner en la variable *f* el valor que tenía *f* multiplicado por el valor de *i*.

Esta definición se parece a la primera que dimos. Dice que el factorial de un número *n* se calcula recorriendo todos los números de 1 a *n* y multiplicándolos entre sí. Vamos a ver otra definición, que se parece a la definición recursiva:

```
def factorial(n):
    if n == 1:
        return 1
    else:
        return n * factorial(n-1)
```

Aquí se dice que para calcular el factorial, hay dos posibilidades: si el número es 1, el factorial vale 1. Si no, el factorial vale *n* multiplicado por el factorial de *n* - 1.

Ejercicio 1.5. (Para el lector que sabe programar). Dar una definición de los números de Lucas L_n y de la variante L'_n en un lenguaje que permita definiciones recursivas.

□ 6. Principio de inducción global

Lorena decide participar en un concurso de juegos de ingenio. Llegado su turno, le dan el siguiente problema: dada la sucesión a_n definida por:

$$a_1 = 2, \quad a_2 = 8, \quad a_{n+2} = 4(a_{n+1} - a_n)$$

calcular el término 2.009 de la sucesión. Lorena calcula los primeros términos:

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 8 \\ a_3 &= 24 \\ a_4 &= 64 \\ a_5 &= 160 \\ a_6 &= 384 \end{aligned}$$

Observa que a_n es divisible por n para cada uno de los valores de la lista. Además, al dividir a_n por n, obtiene:

$$\begin{aligned} a_1 &= 1 \cdot 2 \\ a_2 &= 2 \cdot 4 \\ a_3 &= 3 \cdot 8 \\ a_4 &= 4 \cdot 16 \\ a_5 &= 5 \cdot 32 \\ a_6 &= 6 \cdot 64 \end{aligned}$$

Después de observar detenidamente la columna de la derecha, Lorena conjetura que $a_n = n \cdot 2^n$ para todo $n \in \mathbb{N}$, pero antes de contestar quiere estar segura de que su respuesta es correcta. Para probarlo, Lorena intenta recurrir al principio de inducción, pero se topa con una dificultad. Si llama $P(n)$ a la afirmación $a_n = n \cdot 2^n$, entonces vale $P(1)$ pero no puede demostrar que si $P(n)$ es cierta, entonces $P(n+1)$ es cierta.

Lo que sucede es que la fórmula $a_{n+2} = 4(a_{n+1} - a_n)$ involucra tres términos consecutivos. Por esto, el conocer un término no permite conocer el siguiente. Es para casos como éste que hace falta el *principio de inducción global*.

Principio de Inducción Global. Supongamos que tenemos para cada $n \in \mathbb{N}$ una afirmación $P(n)$ y queremos ver que todas estas afirmaciones son válidas. Si se puede demostrar que:

- $P(1)$ es cierta,
- si $P(k)$ es cierta para todo $k < n$, entonces $P(n)$ también lo es,

entonces $P(n)$ vale para todo $n \in \mathbb{N}$.

Veamos cómo puede utilizar Lorena el principio de inducción global. Probemos que $a_n = n \cdot 2^n$ para todo $n \in \mathbb{N}$. Primero, verificamos que $P(1)$ es cierta: $a_1 = 2 = 1 \cdot 2^1$. Ahora, suponemos que $P(k)$ es cierta para todo $k < n$. Por la definición de la sucesión, $a_n = 4(a_{n-1} - a_{n-2})$, pero esto vale solo para $n > 2$, ya que a_0 no está definido. Tenemos entonces dos casos: $n = 2$ y $n > 2$. Si $n = 2$, la afirmación $P(2)$ se verifica simplemente

observando que $a_2 = 8 = 2 \cdot 2^2$. Y si $n > 2$, como $n - 1 < n$ y $n - 2 < n$, nuestra hipótesis inductiva dice que valen las fórmulas para a_{n-1} y a_{n-2}, es decir:

$$a_{n-1} = (n-1) \cdot 2^{n-1}$$
$$a_{n-2} = (n-2) \cdot 2^{n-2}$$

Entonces:

$$\begin{aligned} a_n &= 4(a_{n-1} - a_{n-2}) \\ &= 4((n-1) \cdot 2^{n-1} - (n-2) \cdot 2^{n-2}) \\ &= 4 \cdot 2^{n-2}((n-1) \cdot 2 - (n-2)) \\ &= 2^2 \cdot 2^{n-2}(2n - 2 - n + 2) \\ &= 2^n \cdot n. \end{aligned}$$

Ahora sí Lorena contesta $a_{2.009} = 2^{2.009} \times 2.009$.

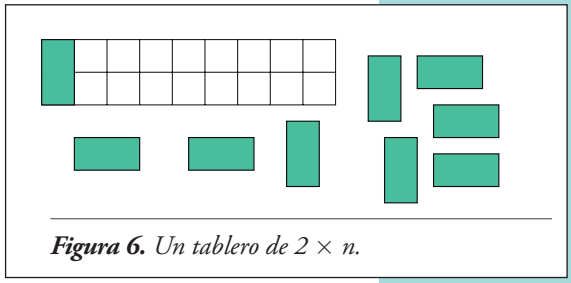


Figura 6. *Un tablero de 2 × n.*

Vamos a considerar un nuevo ejemplo, planteado por Fibonacci [2]. Tenemos un tablero de $2 \times n$, como en el dibujo de la Figura 6.

Queremos llenarlo con fichas de 2×1 con una regla: la ficha de la izquierda debe ir de manera vertical, como se muestra en la Figura 6.

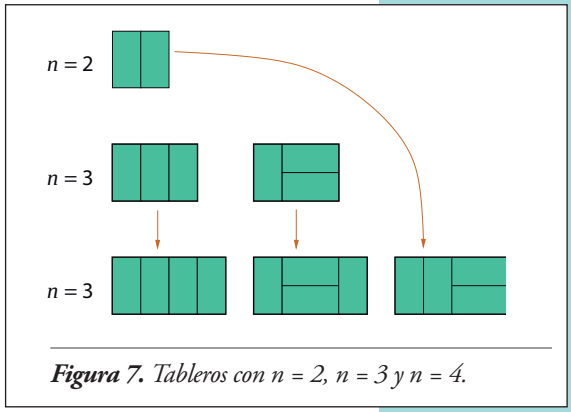


Figura 7. *Tableros con n = 2, n = 3 y n = 4.*

Llamamos F_n a la cantidad de formas de llenar el tablero de tamaño n con esta regla. Si queremos llenar un tablero, a la derecha hay dos posibilidades: o bien la última ficha la ponemos de manera vertical, o bien ponemos dos fichas de manera horizontal. En el caso vertical, al agregar esta ficha nos queda por llenar un tablero de tamaño $2 \times (n-1)$ que debe cumplir la regla. En el caso horizontal, al poner estas dos fichas, nos queda por llenar un tablero de tamaño $2 \times (n-2)$ que debe cumplir la regla. En la Figura 7, se ve cómo los tableros de tamaño 2×4 se forman a partir de los tableros de tamaño 2×3 y 2×2.

Esto dice que $F_n = F_{n-1} + F_{n-2}$ para todo $n \geq 3$. Por otra parte, $F_1 = 1$ y $F_2 = 1$. Veamos los primeros números de esta sucesión:

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_3 &= 2 \\ F_4 &= F_3 + F_2 = 2 + 1 = 3 \\ F_5 &= F_4 + F_3 = 3 + 2 = 5 \\ F_6 &= F_5 + F_4 = 5 + 3 = 8 \end{aligned}$$

y luego sigue con 13, 21, 34, 55, 89, etc. Es prácticamente imposible encontrar, a simple vista, una fórmula no recursiva para F_n. Sin embargo, se puede dar una:

[2] Fibonacci planteó este problema con conejos. Su libro "Liber Abaci" de 1202 dice textualmente: "Cierto hombre tenía una pareja de conejos juntos en un lugar cerrado y uno desea saber cuántos son creados a partir de este par en un año; cuando es su naturaleza parir otro par en un simple mes, y en el segundo mes, los nacidos parir también".

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Vamos a probar esta fórmula por inducción global. Para $n = 1$, tenemos que:

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1 &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2}\right)\\ &= \frac{1}{\sqrt{5}}\sqrt{5}\\ &= 1\\ &= F_1\end{aligned}$$

Para $n = 2$, tenemos:

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^2 &= \frac{1}{\sqrt{5}}\left(\frac{(1+\sqrt{5})^2-(1-\sqrt{5})^2}{4}\right)\\ &= \frac{1}{\sqrt{5}}\frac{(1+2\sqrt{5}+5)-(1-2\sqrt{5}+5)}{4}\\ &= \frac{1}{\sqrt{5}}\frac{4\sqrt{5}}{4}\\ &= 1\\ &= F_2\end{aligned}$$

Ahora, si $n \geq 3$, suponemos que vale la fórmula para todos los $k < n$. Entonces:

$$\begin{aligned}F_n = F_{n-1} + F_{n-2} &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}+1\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}+1\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}+2}{2}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}+2}{2}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{6+2\sqrt{5}}{4}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{6-2\sqrt{5}}{4}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}\right)^2\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n}\end{aligned}$$

Veamos un nuevo ejemplo de inducción global. Martín y Pablo, alumnos de la Escuela 314, compraron un chocolate que viene dividido en cuadraditos, y lo comen jugando un juego. El que pierde, va a pagar el próximo chocolate. El juego es así:

1. por turnos, Martín y Pablo cortan el chocolate en dos pedazos por una línea horizontal o vertical, como en la figura 8;
2. el que hizo el corte, elige el pedazo que quiere y deja el resto;

3. se van alternando en los cortes, hasta que queda un solo cuadradito, que ya no se puede cortar;
4. quien se queda con este último cuadradito, pierde el juego (y paga el chocolate que sigue).

La pregunta entonces es: ¿cuál es la mejor estrategia para no quedarse con el último cuadradito? Pensando en la estrategia ganadora, Martín observa que si le deja a Pablo un cuadrado de chocolate de 2×2, entonces Pablo va a perder seguro. Esto es porque con cualquier corte que haga Pablo deja un rectángulo de 2×1, y en la jugada siguiente Martín lo deja con el último cuadradito. Luego, observa que si le deja a Pablo un cuadrado de 3×3 también sabe cómo ganarle: en este caso Pablo puede dejar o bien un rectángulo de 3×2 o bien uno de 3×1. Si deja uno de 3×1, Martín le deja el último cuadradito y Pablo pierde. Si Pablo deja uno de 3×2, Martín le deja uno de 2×2 y como en el caso anterior Pablo pierde. Estudiando estos casos, Martín se da cuenta de cómo ganar si en algún momento a Pablo le queda para jugar un chocolate cuadrado de cualquier tamaño: cada vez que Pablo juega, Martín, en su turno, le deja nuevamente un chocolate cuadrado.

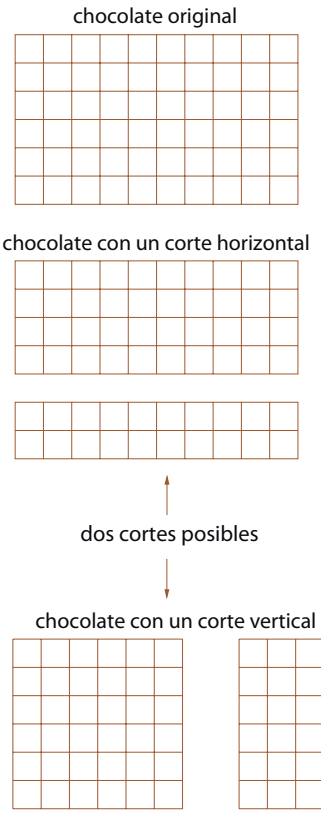


Figura 8. *El chocolate y dos cortes posibles.*

Probemos que Martín está en lo cierto. Para cada $n \in \mathbb{N}$ llamemos $P(n)$ a la afirmación siguiente: *si a Pablo le toca cortar un cuadrado de $n \times n$, Martín tiene una estrategia para ganar.*

Para $n = 1$, Martín no hace nada y gana. Supongamos que Martín tiene una estrategia para ganar si a Pablo le toca cortar un chocolate cuadrado de $k \times k$ para cualquier k menor que n (éstas son las afirmaciones $P(k)$ para $k < n$). Supongamos ahora que a Pablo le toca un chocolate cuadrado de $n \times n$. Pablo hace un corte, y le deja a Martín un chocolate rectangular de $k \times n$ para algún k menor que n. En su turno Martín corta el chocolate de manera de dejar a Pablo un cuadrado de $k \times k$ (ver Figura 9). Por hipótesis inductiva, a partir de aquí Martín tiene una estrategia para ganar.

Como conclusión, si el chocolate es cuadrado, siguiendo la estrategia de Martín el que comienza siempre pierde. Si el chocolate no es cuadrado, el que comienza siempre gana.

Ejercicio 1.6. Dada la siguiente sucesión definida recursivamente, conjeturar una fórmula para el término general y probarla:

$$a_1 = 1, \qquad a_2 = 4, \qquad a_{n+2} = 4\sqrt{a_{n+1}} + a_n \text{ para } n \in \mathbb{N}.$$

Ejercicio 1.7. Consideremos la sucesión definida recursivamente por:

$$a_1 = 2, \qquad a_2 = 3, \qquad a_{n+2} = 2a_{n+1} + a_n \text{ para } n \in \mathbb{N}.$$

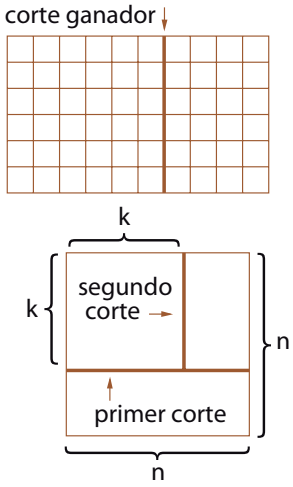


Figura 9. *Chocolate con cortes estratégicos.*

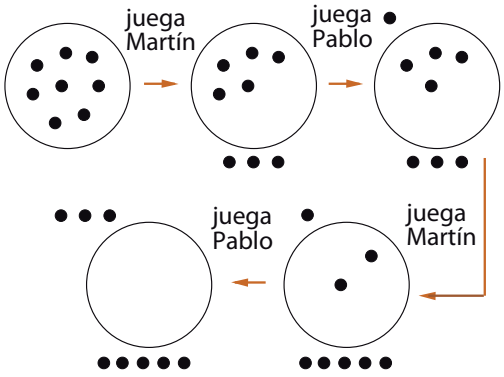


Figura 10. *Juegan Martín y Pablo.*

Probar que $a_n \leq 3^n$ para todo $n \in \mathbb{N}$.

Ejercicio 1.8. Martín y Pablo ahora juegan al siguiente juego: tienen un plato con piedritas. Por turnos, van sacando 1, 2, ó 3 piedritas. Quien vacía el plato gana. Por ejemplo, si hay 8 piedritas, Martín saca en su turno 3 y Pablo saca 1, y quedan 4. Ahora Martín saca 2 y Pablo saca las 2 que quedan. Gana Pablo. (ver figura 10)

¿Es cierto que si Martín empieza jugando con 8 piedritas, sin importar lo que haga, Pablo siempre tiene una manera de ganar? ¿Qué pasa si empieza con 9 piedritas? Para cada $n \in \mathbb{N}$, decidir quién tiene una estrategia ganadora si Martín empieza con n piedritas, y probarlo por inducción.

□ 7. Principio de buena ordenación

Con el orden usual, los naturales gozan de una propiedad importante: son bien ordenados.

Un conjunto A con una relación de orden $\leq$ se dice **bien ordenado** si todo subconjunto $B \subseteq A$ no vacío tiene un primer elemento (aquí "primer" elemento significa que es menor que todos los otros elementos de B).

Si consideramos A como el conjunto de los números enteros y B el de los enteros pares, entonces B no tiene primer elemento, porque para cualquier entero par m hay un entero par menor (por ejemplo m-2). Esto dice que el conjunto de los números enteros no es bien ordenado. Sin embargo, si ahora A es el conjunto de los números naturales y B es el de los naturales pares, entonces B sí tiene primer elemento: el 2, porque es el menor de los números naturales pares.

Gracias al principio de inducción global podemos probar el siguiente Teorema.

Teorema 1.1. *El conjunto de los números naturales es bien ordenado.*

Demostración. Vamos a demostrar que si $B \subseteq \mathbb{N}$ y B no tiene primer elemento, entonces B es vacío. Para esto, consideramos $P(n)$ como la afirmación "$n \notin B$", y vamos a probar por inducción global que $P(n)$ es verdadera para todo n. La afirmación $P(1)$ es verdadera porque si no lo fuera, 1 pertenecería a B y sería su primer elemento. Por otra parte, supongamos que $P(k)$ es cierta para todo $k < n$. Entonces, debemos probar que $P(n)$ también lo es. Como $P(k)$ es cierta para todo $k < n$, ninguno de los números $1, 2, \ldots, n-1$ pertenecen a B. Si $P(n)$ fuese

falsa, entonces n pertenecería a B y sería su primer elemento. Luego, n no puede pertenecer a B y $P(n)$ es verdadera.

En realidad, el principio de buena ordenación es *equivalente* al principio de inducción. Es decir, también podemos ver que el principio de inducción se deduce del principio de buena ordenación. De hecho, supongamos que para cada $n \in \mathbb{N}$, $P(n)$ es una afirmación tal que $P(1)$ es cierta y si $P(n)$ es cierta, entonces $P(n+1)$ también lo es. Podemos probar, gracias al principio de buena ordenación, que $P(n)$ es cierta para todos los números naturales. Para ello, consideramos B el conjunto de los n tales que $P(n)$ es falsa. Si B fuese no vacío, tendría un primer elemento, llamémoslo k. No puede ser $k = 1$ porque $P(1)$ es cierta. Entonces $k > 1$, y si $n = k - 1$, tenemos que $P(n)$ es cierta porque $k - 1 \notin B$. Pero esto dice que $P(n + 1)$ es cierta, es decir, $P(k)$ es cierta, y esto es un absurdo.

□ 8. Ejemplos surtidos

8.1. Torres de Hanoi o Torres de Brahma

El problema de las Torres de Hanoi fue inventado por el matemático francés Edouard Lucas en 1883. Tenemos tres grandes baldosas en el suelo, y un cierto número de discos de distinto tamaño apilados uno encima del otro en la primera baldosa ordenados por tamaño. El más pequeño está encima de la pila. El objetivo del juego es lograr mover toda la pila de discos a la tercera baldosa, con la condición de que:

- no se puede mover más de un disco a la vez;
- sólo se puede sacar el disco de la parte superior de cada pila de discos;
- en todo momento, en cada baldosa los discos deben estar ordenados por tamaño.

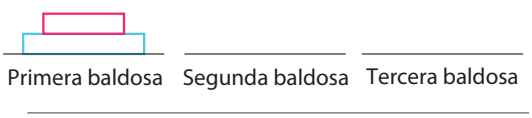


Figura 11. *Torre con 2 discos.*

Veamos cómo resolvemos este problema si tenemos simplemente dos discos:

- comenzamos con dos discos en la primera baldosa, como en la figura 11;
- en el primer paso solamente podemos quitar el disco pequeño y colocarlo en otra baldosa. Lo colocamos en la segunda baldosa;
- en el segundo paso, podemos mover el disco más grande para ubicarlo en la tercera baldosa;
- en el tercer paso, movemos el disco pequeño colocándolo encima del disco grande y conseguimos que quede la torre original en el tercer lugar.

Figura 12. *Resolución con 2 discos.*

Todo este proceso se ve en la figura 12.

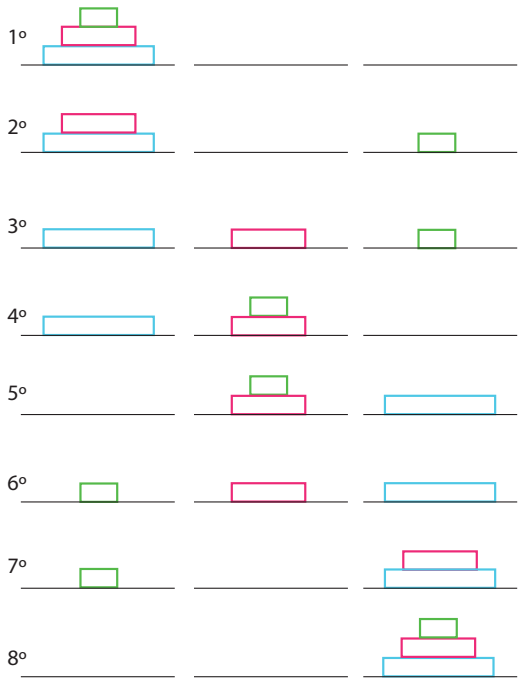


Figura 13. *Torre con 3 discos.*

Es bastante claro que no se puede hacer esto en menos de 3 pasos, dado que el primer paso es único (mover el disco pequeño). En el segundo paso tenemos dos opciones, pero si queremos lograr mover toda la torre, en algún momento deberá estar el disco grande en la tercera baldosa. Entonces, lo mejor es hacerlo en el segundo movimiento, y luego debemos colocar el disco pequeño sobre el grande.

La pregunta que hizo Lucas es si comenzamos con n discos: ¿cuál es el mínimo número de movimientos necesarios para pasar todos los discos de la primera baldosa a la tercera?

Invitamos a jugar un rato el juego, antes de continuar leyendo la respuesta. Existen versiones de plástico de este juego, que tienen tres postes tipo ábaco, y los discos están perforados para poder apilarlos de manera sencilla, aunque se puede jugar con monedas de distintos tamaños.

Llamemos H_n al número mínimo de movimientos para una torre de n discos. Sabemos que $H_1 = 1$ y $H_2 = 3$. Calculemos H_3. Como vemos en la Figura 13, alcanzan 7 movimientos. O sea: $H_3 \leq 7$.

Supongamos ahora que tenemos n discos. Para mover toda la torre a la tercera baldosa, en algún momento debemos colocar el disco más grande en la tercera baldosa. Dado que es el más grande de todos, si pensamos que este disco no existe y movemos los otros n - 1 discos de manera ordenada, los discos estarán ordenados en todo momento. Supongamos que sabemos cómo mover la torre de los n - 1 discos más pequeños a otra baldosa en H_{n-1} pasos de forma óptima. Entonces, podemos mover de esta forma los n - 1 discos más chicos a la segunda baldosa, luego mover el disco mayor hasta la tercera baldosa, y una vez hecho esto, mover los n - 1 discos menores para colocarlos de manera ordenada encima de él, nuevamente de forma óptima en H_{n-1} pasos (notar que esto fue lo hecho con 3 discos). En conclusión, probamos que

$$H_n = 2 \cdot H_{n-1} + 1.$$

Ejercicio 1.9. Probar por inducción que la sucesión dada por:

$$H_1 = 1, \qquad H_n = 2 \cdot H_{n-1} + 1 \text{ si } n \geq 1,$$

satisface $H_n = 2^n - 1$.

8.2. Algoritmo de ordenamiento (Sort)

Supongamos que tenemos una lista $[a_1, \ldots, a_n]$ de objetos que queremos ordenar con determinado criterio, por ejemplo números naturales para ordenar en forma creciente, o palabras para ordenar alfabéticamente.

Existe una gran variedad de algoritmos que permiten realizar esta tarea; vamos a analizar uno de ellos. La idea es la siguiente:

1. si la lista tiene uno o ningún elemento, no hay nada que hacer;
2. si la lista tiene dos o más elementos, se la subdivide en dos listas con la misma cantidad de elementos (o una con un elemento más que la otra si n es impar);
3. se ordena cada una de las dos listas nuevas y, a continuación, se las vuelve a unir, pero ordenando los elementos entre sí.

Para unir las dos listas ordenadas L_1 y L_2 y armar una única lista L, también ordenada, con los elementos de ambas, se utiliza el siguiente procedimiento:

- si alguna de las listas no tiene elementos, se agregan los elementos de la otra lista a L y se terminó el procedimiento;
- si ambas listas tienen elementos, se toma el primer elemento α de L_1 y se lo compara con el primer elemento β de L_2. Si $\alpha \leq \beta$, se agrega α a la lista L y se lo suprime de L_1 (L_2 no se modifica). Si $\alpha > \beta$, se agrega β a L y se lo suprime de L_2 (L_1 no se modifica). Luego, se repite el proceso con las nuevas listas.

Supongamos que queremos ordenar en forma creciente la lista $L = [4, 1, 2, 5, 7, 3, 6, 8]$. Consideramos las sublistas $L_1 = [4, 1, 2, 5]$ y $L_2 = [7, 3, 6, 8]$. Para ordenar L_1, la subdividimos nuevamente en dos listas $L_{11} = [4, 1]$ y $L_{12} = [2, 5]$.

Ordenamos L_{11} obteniendo $L'_{11} = [1, 4]$, y L_{12} obteniendo $L'_{12} = [2, 5]$. Ahora las volvemos a unir, ordenando los elementos: el primer elemento de L'_{11} es menor que el primero de L'_{12}, entonces ubicamos en primer lugar a 1. El segundo elemento de L'_{11} es mayor que el primero de L'_{12}; agregamos entonces el 2. Comparamos el segundo elemento de L'_{11} con el segundo de L'_{12}, y resulta menor, con lo que lo agregamos. Nos queda entonces la lista L_1 ordenada como $L'_1 = [1, 2, 4, 5]$.

Procediendo análogamente, se ordena la lista L'_2, obteniéndose $L'_2 = [3, 6, 7, 8]$. Para terminar, se unen las listas L'_1 y L'_2, comparando como antes uno a uno sus elementos:

L'	L'_1	L'_2	
$[\,]$	$[\underline{1}, 2, 4, 5]$	$[\underline{3}, 6, 7, 8]$	$1 < 3$
$[1]$	$[\underline{2}, 4, 5]$	$[\underline{3}, 6, 7, 8]$	$2 < 3$
$[1, 2]$	$[\underline{4}, 5]$	$[\underline{3}, 6, 7, 8]$	$4 > 3$
$[1, 2, 3]$	$[\underline{4}, 5]$	$[\underline{6}, 7, 8]$	$4 < 6$
$[1, 2, 3, 4]$	$[\underline{5}]$	$[\underline{6}, 7, 8]$	$5 < 6$
$[1, 2, 3, 4, 5]$	$[\,]$	$[6, 7, 8]$	$L'_1 = [\,]$
$[1, 2, 3, 4, 5, 6, 7, 8]$	$[\,]$	$[\,]$	

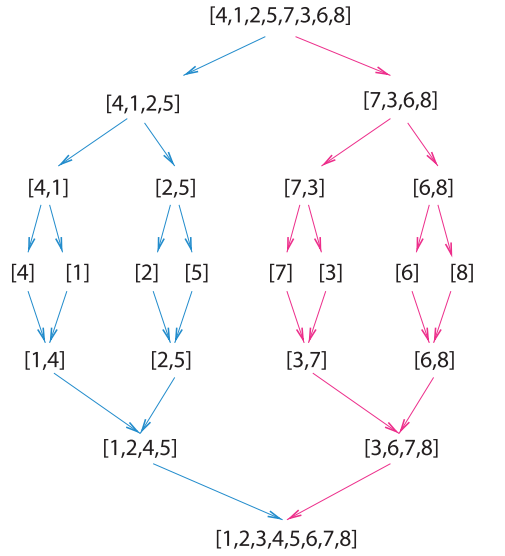


Figura 14. *El algoritmo de ordenamiento en la lista [4, 1, 2, 5, 7, 3, 6, 8].*

Se puede observar el procedimiento completo en la figura 14.

Queremos estimar la cantidad de comparaciones que realiza este algoritmo para ordenar una lista de longitud n. Supondremos que n es una potencia de 2, así al subdividir la lista sucesivamente siempre resultan dos sublistas de tamaño igual a la mitad de la anterior. Llamemos c_k a la cantidad máxima de comparaciones que realiza el algoritmo para ordenar una lista de $n = 2^k$ elementos.

Si $n = 2$, o sea $k = 1$, haciendo una sola comparación podemos ordenar la lista. Entonces $c_1 = 1$.

Si $n = 2^k$, con $k \geq 2$, en el primer paso del algoritmo vamos a partir la lista en dos sublistas de tamaño 2^{k-1}. La cantidad de comparaciones que haremos para ordenar cada una de las dos sublistas es como máximo c_{k-1}. Finalmente, debemos unir las dos listas ordenadas. En cada paso de esta unión se realiza una comparación y se ubica un elemento de alguna de las dos listas en la lista final, con lo que el algoritmo realiza menos de $n = 2^k$ comparaciones. Deducimos entonces, que $c_k < 2c_{k-1} + 2^k$.

Veamos que $c_k < k \cdot 2^k$ para todo $k \in \mathbb{N}$. Podemos probar esta propiedad por inducción:

- Si $k = 1$, vale $c_1 = 1 < 2 = 1 \cdot 2^1$.
- Supongamos que $c_k < k \cdot 2^k$ y acotemos c_{k+1}. Usando la desigualdad que probamos más arriba, junto con esta hipótesis, resulta que:

$$c_{k+1} < 2c_k + 2^{k+1} < 2 \cdot k \cdot 2^k + 2^{k+1} = k \cdot 2^{k+1} + 2^{k+1}$$
$$= (k+1) \cdot 2^{k+1}$$

Deducimos entonces que para ordenar una lista de $n = 2^k$ elementos, el algoritmo realiza menos de $k \cdot 2^k = \log_2(n) \cdot n$ comparaciones.

2. Números enteros

Patricia JANCSA

□ 1. Introducción

Estudiamos los números naturales y vimos que sirven para contar. Sin embargo, hay situaciones que para ser descriptas correctamente requieren de otro tipo de números. Los números enteros negativos se usan en diversos contextos, por ejemplo, para expresar o calcular:

- En geografía, profundidades o diferencias de altura:
  - *la capa más superficial de la estructura de la Tierra, llamada corteza terrestre, llega hasta los -30 km en el fondo oceánico;*
  - *la diferencia de altura que hay desde la cima del Aconcagua, que se halla a 6.959 metros sobre el nivel del mar, hasta el fondo de la laguna del Carbón, en la provincia de Santa Cruz, donde el altímetro marca 105 metros bajo el nivel del mar.* (Figura 1)

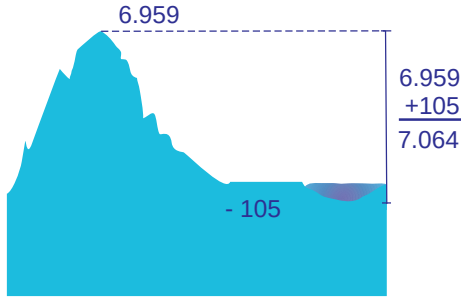


Figura 1.

- Temperaturas bajo cero: *el día más frío del año 2008 en Ushuaia fue el 16 de agosto, con una temperatura mínima de -5°C y una temperatura máxima de 7°C.*
- En contabilidad, los números negativos significan *deudas* y los positivos haberes o activos poseídos.
- Fechas en la antigüedad, años antes de Cristo: *Platón, el más importante filósofo de la antigüedad, fue alumno de Sócrates y maestro de Aristóteles; nació en Grecia en el año 427 a.C. y murió en el año 347 a.C.; por lo tanto, vivió 80 años.*

□ 2. Construcción de los números enteros

Para continuar el estudio de los números, consideremos $\mathbb{N}_0$ el conjunto de los números naturales y el cero, y pensemos en la siguiente situación. En el capítulo anterior, estudiamos operaciones de números naturales y vimos que dos números naturales se pueden sumar y se obtiene como resultado otro número natural; también se pueden multiplicar y el resultado es un número natural. Por ejemplo, $3+5 = 8 \in \mathbb{N}$ y $3 \cdot 5 = 15 \in \mathbb{N}$. Además, si quisiéramos restar uno de otro, por ejemplo, hacer 5 - 3 también se puede dentro del conjunto $\mathbb{N}$, es decir $5 - 3 = 2 \in \mathbb{N}$. Una situación cotidiana que refleja esta situación matemática es la siguiente: si Paula tiene 5 remeras, Lorena le puede pedir prestadas 3 remeras y a Paula todavía le quedan 2. En cambio, si Paula tuviera sólo 3 remeras, Lorena no debería esperar que le preste 5 porque no tiene más de 3.

Es decir, ¿qué ocurre si queremos efectuar la operación de resta en el otro sentido, o sea, 3-5? ¿A 3 se le puede restar 5? Veremos enseguida que, en realidad, sí se puede efectuar esta operación, pero el resultado ya no es un número natural.

Recordemos que la operación suma dentro de $\mathbb{N}_0$ tiene al cero como elemento neutro porque $a + 0 = a$ y $0 + a = a$ para todo número natural a. Pero ningún número natural tiene un **inverso** dentro de $\mathbb{N}_0$, respecto de la suma. La pregunta es qué tipo de números deberíamos agregarle a $\mathbb{N}_0$ para que todo elemento tenga inverso respecto de la operación suma. Es decir, si Paula tuviera 3 remeras, Lorena podría pedirle las 3 remeras (¡por lo menos para probárselas!) y en este caso, Paula no se quedaría con ninguna. Es decir, 3 - 3 = 0, o, mejor dicho, 3 + (-3) = 0 que no es un natural pero sí pertenece a $\mathbb{N}_0$.

En otras palabras, agreguémosle a $\mathbb{N}_0$ todos los "opuestos" de sus elementos, es decir, el -1, el -2, etcétera. Llamaremos al nuevo conjunto que construimos de esta forma *conjunto de los números enteros* y lo denotamos con la letra $\mathbb{Z}$. A partir de la construcción anterior:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$$

que, en particular, contiene a $\mathbb{N}$ y a $\mathbb{N}_0$. Así, dentro de $\mathbb{Z}$, cualquier $n \in \mathbb{N}$ tiene un inverso, respecto de la suma, que es su opuesto.

Veamos que la pregunta anterior también tiene respuesta dentro de $\mathbb{Z}$. Ahora, podemos realizar la operación "resta" o "diferencia" de cualquier par de enteros, por ejemplo, a 3 - 5 lo calculamos como 3 + (-5) = -2. Es decir, si Paula tuviera tres remeras, le faltarían dos para poder prestarle 5 remeras a su amiga.

Ejemplos

- *¿Qué diferencia de altura hay desde la cima del Aconcagua, que se halla a 6.959 metros sobre el nivel del mar, hasta el fondo de la laguna del Carbón, en la provincia de Santa Cruz, donde el altímetro marca 105 metros bajo el nivel del mar?*

  Para averiguarlo, necesitamos calcular 6.959 - (-105) = 6.959+105 = 7.064 metros.

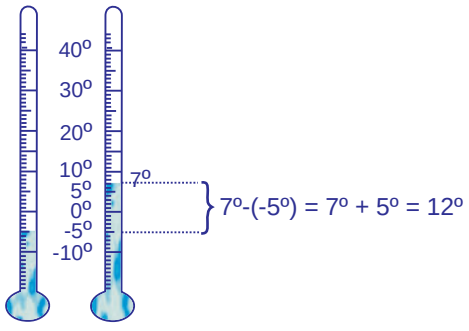


Figura 2. *En grados Celsius.*

- *¿Qué amplitud térmica hubo el 16 de agosto de 2.008 en Ushuaia?* (Figura 2)

  Dado que la temperatura mínima fue de -5°C y la máxima de 7°C, la amplitud térmica fue de 7°C -(-5°C)=12°C.

- *Si tenemos* $1.500 *en el banco, no podemos emitir un cheque por* $1.750*, salvo que el banco nos preste la diferencia, en cuyo caso generaríamos una deuda. Para informarnos de esta situación, el banco nos mandaría una carta donde explicaría que, en este caso, el saldo de nuestra cuenta sería de* $1.500 - $1.750 = -$250*, es decir que le deberíamos* $250 *al banco.*

- *Pitágoras, filósofo y matemático griego, nació aproximadamente en el año 582 a.C. y vivió 75 años; ¿en qué año murió?*

  Si Pitágoras nació en el año 582 a.C., es decir, 582 años antes del año cero, y vivió 75 años, entonces murió 75 años más tarde de su año de nacimiento, es decir que murió en el año:

$$-582 + 75 = -507$$

  La respuesta es que murió aproximadamente en el año 507 a.C.

2.1. Construcción formal de $\mathbb{Z}$

Notemos que un número entero negativo puede ser definido como la diferencia de dos números naturales. Por ejemplo -2 = 3 - 5, de donde puede asociarse el número -2 con el par ordenado (3 , 5). El problema es que (4 , 6), (11 , 13) y otros infinitos pares ordenados también dan como resultado -2 al restar sus componentes. ¿De qué forma podemos definir sin ambigüedad el número -2? Perfeccionemos la idea anterior, teniendo en cuenta a la vez *todos los pares ordenados de números naturales cuya diferencia es* -2. Es decir, dos pares ordenados (m , n) y (m', n') pueden asignarse al mismo número entero si:

$$m - n = m' - n' \quad (*)$$

El inconveniente es que las restas $(*)$ no pueden efectuarse en $\mathbb{N}$ si $m \leq n$. Pero este problema se puede solucionar si nos damos cuenta de que:

$$m - n = m' - n' \text{ es equivalente a } \quad m + n' = m' + n \quad (**)$$

y esta operación es correcta en $\mathbb{N}$, ya que la suma de cualquier par de naturales es un número natural. Entonces, estamos en condiciones de definir en $\mathbb{N} \times \mathbb{N}$ la relación ~ dada por:

$$(m\ ,\ n) \sim (m'\ ,\ n') \quad \text{si y sólo si } m + n' = m' + n$$

No es difícil ver que esta relación es de equivalencia; por lo tanto, produce en $\mathbb{N} \times \mathbb{N}$ una partición en clases de equivalencia, cada una de las cuales puede ser asociada a un único número entero y viceversa. Si denotamos por $[(m\ ,\ n)]$ la clase de equivalencia del par (m , n), para cada par de naturales m y n, resulta, por ejemplo:

$$\begin{aligned}[(3\ ,\ 5)] &\sim [(11\ ,\ 13)] \\ &\sim [(19\ ,\ 21)] \\ &\sim [(1\ ,\ 3)]\end{aligned}$$

Se define entonces m - $n \in \mathbb{Z}$ como cualquier representante de la clase $[(m\ ,\ n)]$. Explícitamente, se define el opuesto de cada número natural n como:

$$-n = [(1\ ,\ n + 1)]$$

Además, el cero puede obtenerse como:

$$0 = [(n\ ,\ n)] \text{ para cualquier } n \in \mathbb{N}.$$

2.2. La suma y la resta de números enteros

Formalmente, podemos definir la suma de dos números enteros a partir de sus clases de equivalencia $[(m\ ,\ n)]$ y $[(m',\ n')]$, con $m, m', n, n' \in \mathbb{N}$:

$$[(m\ ,\ n)] + [(m'\ ,\ n')] = [(m + m'\ ,\ n + n')]$$

Esto se interpreta como:

$$(m - n) + (m' - n') = (m + m') - (n + n')$$

Debemos ver que esta operación está bien definida en clases de equivalencias, esto es, que si $(m_1, n_1) \sim (m_2, n_2)$ y $(m'_1, n'_1) \sim (m'_2, n'_2)$, entonces $(m_1 + m'_1, n_1 + n'_1) \sim (m_2 + m'_2, n_2 + n'_2)$. Ahora, al ser $(m_1, n_1) \sim (m_2, n_2)$ vale que:

$$m_1 + n_2 = m_2 + n_1$$

y análogamente, al ser $(m'_1, n'_1) \sim (m'_2, n'_2)$ vale que:

$$m'_1 + n'_2 = m'_2 + n'_1.$$

lo que claramente implica que:

$$m_1 + m'_1 + n_2 + n'_2 = m_2 + m'_2 + n_1 + n'_1$$

como queríamos ver.

Se define la resta como:

$$[(m\ ,\ n)] - [(m'\ ,\ n')] := [(m + n'\ ,\ n + m')]$$

que interpretamos:

$$\begin{aligned}(m - n) - (m' - n') &= m - n - m' + n' \\ &= m + n' - n - m' \\ &= (m + n') - (n + m').\end{aligned}$$

Esta operación también está bien definida en clases de equivalencia: si $(m_1, n_1) \sim (m_2, n_2)$ y $(m'_1, n'_1) \sim (m'_2, n'_2)$ entonces $(m_1 + n'_1, n_1 + m'_1) \sim (m_2 + n'_2, n_2 + m'_2)$, pues:

$$\begin{aligned}m_1 + n'_1 + n_2 + m'_2 &= (m_1 + n_2) + (n'_1 + m'_2) \\ &= (m_2 + n_1) + (n'_2 + m'_1) \\ &= n_1 + m'_1 + m_2 + n'_2\end{aligned}$$

Veamos cómo resultan estas operaciones en la práctica: ya sabíamos cómo sumar dos números naturales y, en la sección anterior estudiamos que la resta de un natural de otro es un número entero. Por ejemplo, 5 - 3 = 2 y 3 - 5 = -2; podemos pensar esta operación como la suma de dos enteros, cada uno con su signo:

$$\begin{aligned} 3-5 &= 3+(-5) \\ &= -2 \end{aligned}$$

La manera más fácil de efectuar esta operación es la siguiente:

$$\begin{aligned} 3-5 &= -(5-3) \\ &= -2 \end{aligned}$$

En general, para m y $n \in \mathbb{N}$, si $m \geq n$ entonces m - n es la resta usual, y el resultado es un número natural o cero. Si $m < n$, el resultado de la resta m - n es un número entero negativo, y puede calcularse como:

$$m-n = -(n-m)$$

En cualquier caso, podemos pensar la resta de dos números naturales como una suma de dos enteros, cada uno con su signo:

$$m+(-n) = m-n$$

Luego, podemos sumar y restar dos números enteros de la siguiente manera:

- si m y $n \in \mathbb{Z}$ son positivos, entonces $m + n$ es la suma usual de números naturales, y m - n está definida arriba;
- si uno es positivo y otro negativo, digamos $m > 0$ y $-n < 0$, con $n \in \mathbb{N}$, entonces su suma es

$$m+(-n) = m-n \in \mathbb{Z}$$

y su resta o diferencia es:

$$m-(-n) = m+n \in \mathbb{N} \subset \mathbb{Z}, \qquad (-n)-m = -(n+m) \in \mathbb{Z}$$

- si ambos son negativos, digamos $-m$ y $-n$ con m y $n \in \mathbb{N}$, su suma es:

$$(-m)+(-n) = -m-n = -(m+n) \in \mathbb{Z}$$

y su diferencia es:

$$(-m)-(-n) = -m+n = n-m \in \mathbb{Z}$$

- si alguno de los dos es cero y $m \in \mathbb{Z}$, entonces:

$$m+0 = m, \quad m-0 = m \quad \text{y} \quad 0-m = -m$$

Por lo tanto, en el conjunto de los enteros se puede sumar y restar sin salir de él.

Es decir que, si $a, b \in \mathbb{Z}$ entonces $a + b$ y $a - b \in \mathbb{Z}$.

Ejemplo. ¿Qué número hay que sumarle a 16 para obtener 5?

Solución. Buscamos $n \in \mathbb{Z}$ tal que $16 + n = 5$

Si sumamos -16 a cada miembro obtenemos:

$$(*)\ 16 + n + (-16) = 5 + (-16) \iff n = -11$$

Por lo tanto, el número buscado es -11. En efecto, si reemplazamos a *n* por -11 en la igualdad inicial, obtenemos:

$$\begin{aligned} 16 + (-11) &= 16 - 11 \\ &= 5 \end{aligned}$$

como queríamos.

Notación. En $(*)$ usamos el símbolo "$\iff$" para indicar que la igualdad que está a la izquierda es equivalente a la de la derecha; es decir, que la validez de la igualdad de la izquierda implica la validez de la igualdad de la derecha y, recíprocamente, la validez de la igualdad de la derecha implica la validez de la igualdad de la izquierda.

2.3. Valor absoluto

¿Qué tienen en común los enteros 5 y -5? Sabemos que uno es el opuesto del otro; esto significa que 5 y -5 **están a la misma distancia del cero**, exactamente a una distancia igual a 5 unidades. La distancia de un número cualquiera al cero se llama el *valor absoluto* del número.

En consecuencia, el hecho anterior se expresa diciendo que el *valor absoluto* de 5 y el de -5 son ambos iguales a 5. En otras palabras, enteros opuestos tienen el mismo *valor absoluto*. En símbolos, el valor absoluto de un número *n* cualquiera se expresa de manera abreviada usando barras verticales en la forma $|n|$. La manera correcta de definirlo en general es:

$$|n| = \begin{cases} n & \text{si } n \geq 0 \\ -n & \text{si } n < 0 \end{cases}$$

Por ejemplo, |5| = 5 y, de acuerdo a la definición, también | - 5| = -(-5) = 5.

2.4. La multiplicación

El ingrediente nuevo que aparece al multiplicar números enteros es el signo: ¿cómo calculamos 3 · (-2)?

Así como para los números naturales el producto 3 · 2 significa *sumar dos veces* 3, que es 3 + 3 = 6, el producto 3 · (-2) significa *restar dos veces* 3, o sea:

$$\begin{aligned} 3 \cdot (-2) &= -3 - 3 \\ &= -6 \end{aligned}$$

De aquí surge la regla para multiplicar un número positivo por otro negativo: el resultado es un número negativo.

¿Cómo calculamos (-3) · (-2)? En este caso, debemos *restar dos veces* -3, o sea:

$$\begin{aligned}(-3)\cdot(-2) &= -(-3)-(-3)\\ &= +6\end{aligned}$$

De esta manera se deduce que el producto de dos números negativos es un número positivo.

Regla de los signos. Para multiplicar "números con signo" hay que respetar las siguientes reglas:

- (+) · (+) = +
- (+) · (-) = -
- (-) · (-) = +

Ejemplos

- (-2) · 3 = -(2 · 3) = -6.
- (-2) · (-3) = +(2 · 3) = 6.
- -[(-1) · (-2)] = -[1 · 2] = -2.

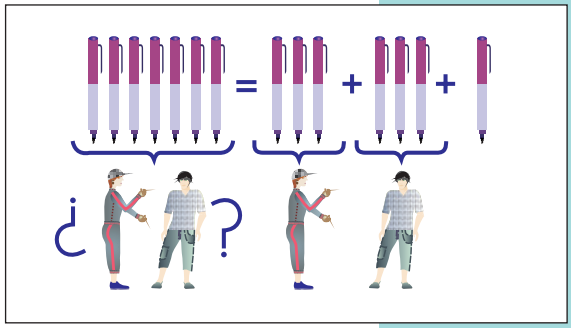
Observación. Sean b y $c \in \mathbb{Z}$ tales que $b \cdot c = 1$. Entonces $b = c = 1$ o $b = c = -1$.

En efecto, si $b \cdot c = 1$, entonces b y c son ambos positivos o ambos negativos. Si b y c son ambos positivos y ocurriera, por ejemplo, $b > 1$ entonces $b \cdot c$, que es igual a "b veces c", sería más grande que c, es decir que $b \cdot c > c \geq 1$; por lo tanto, tanto b como c deben ser 1.

Si b y c son ambos negativos, entonces $-b$ y $-c$ son positivos, y podemos usarlos para escribir el producto en la forma $b \cdot c = (-b) \cdot (-c)$ que sabemos que es igual a 1; por lo tanto, de nuevo $-b$ y $-c$ deben ser 1, o sea que b y c son iguales a -1.

□ 3. Divisibilidad y algoritmo de división

Imaginemos que tenemos una tableta de chocolate de **seis cuadraditos** que dos amigos quieren compartir por igual. Esta operación puede realizarse convenientemente, y a cada uno le tocan tres de las seis partes que tiene la tableta.



Ahora, imaginemos que tenemos 7 lapiceras que queremos repartir entre los dos amigos. Es claro que, para que a cada amigo le toque la misma cantidad, podemos darle tres lapiceras a cada uno pero *sobra una lapicera*, es decir, *la lapicera sobrante no puede partirse*.

La división es la operación que permite averiguar cuántas veces un número, el divisor, está contenido en otro número, el dividendo. Por ejemplo, el 2 está 3 veces en el 6, porque $3 \cdot 2 = 6$, entonces 6 *dividido* 2 *es igual a* 3. En este sentido, la división es la operación inversa de la multiplicación.

Se denomina *cociente* al resultado entero de la división. Si la división no es exacta, es decir, el divisor no está contenido un número exacto de veces en el dividendo, la operación tendrá un *resto*. En el caso de las lapiceras, se divide 7 por 2 y se obtiene un cociente de 3 unidades y un resto de 1 unidad, que también puede expresarse como:

Dividendo	=	**Cociente**	·	**Divisor**	+	**Resto**
7	=	3	·	2	+	1

Para obtener el cociente y el resto de efectuar la división de un número entero por otro, se efectúa el procedimiento conocido como **algoritmo de división**, que explicaremos más adelante.

3.1. Divisibilidad

Si $a, b \in \mathbb{Z}$ decimos que *a divide* a *b* si existe $q \in \mathbb{Z}$ tal que $b = q \cdot a$, donde q es el cociente de la división de b por a.

Para expresar simbólicamente este hecho, se escribe $a \mid b$. También se dice que *b es divisible por a,* o que *a es un divisor de b*.

Por ejemplo, 2 divide a 2 (en efecto, $2 = 1 \cdot 2$); 2 también divide a 4, a 6, a 8, a 20, y a todos los números pares. Justamente, un número es **par** si es divisible por 2.

Ejercicio 2.1. ¿Cómo podríamos describir a todos los números impares?

Observación. Propiedades de la noción de **divisibilidad**:

1. Para cada $n \in \mathbb{Z}$, $1 \mid n$, $n \mid n$, $-1 \mid n$ y $-n \mid n$.

   En efecto, $1 \mid n$ porque $n = 1 \cdot n$, es decir, en la división de n por 1, el cociente es n y la división es exacta. Por otra parte, en la división de n por el mismo n, el cociente es 1 y la división es exacta. Notemos, además, que $-1 \mid n$ y $-n \mid n$ porque $n = (-n) \cdot (-1)$.

2. Si $a, b \in \mathbb{Z}$, $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$.
3. Si $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.
4. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

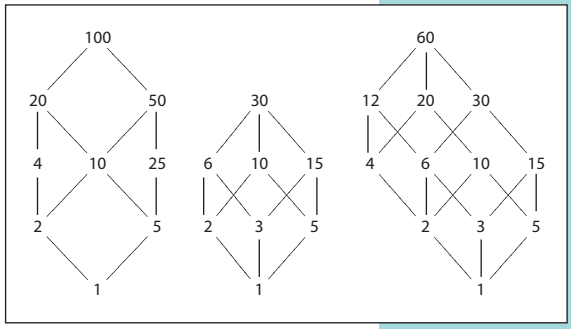
   En efecto, si $a \mid b$ existe $q \in \mathbb{Z}$ tal que $b = q \cdot a$. Si además $b \mid c$, existe $q' \in \mathbb{Z}$ tal que $c = q' \cdot b$. Entonces $c = q' \cdot (q \cdot a) = (q' \cdot q) \cdot a$.

5. Si $a \mid b$ y $a \mid c$ entonces $a \mid (h \cdot b + k \cdot c)$ para cualesquiera $h, k \in \mathbb{Z}$.

En efecto, si $a \mid b$ y $a \mid c$ existen enteros q_1 y q_2 tales que $b = q_1 \cdot a$ y $c = q_2 \cdot a$; entonces $h \cdot b + k \cdot c = h \cdot q_1 \cdot a + k \cdot q_2 \cdot a = (h \cdot q_1 + k \cdot q_2) \cdot a$.

El 1 tiene exactamente dos divisores, que son 1 y -1. Los demás enteros n distintos de 0, de 1 y de -1 tienen **por lo menos cuatro divisores**, que son el 1, el -1, el mismo n, y su opuesto $-n$, pueden tener más divisores. Un entero se dice *primo* si tiene exactamente cuatro divisores distintos. Los divisores de 6 son 1, 2, 3, 6 y sus opuestos, -1, -2, -3 y -6; es decir que 6 tiene ocho divisores en total (6 no tiene más divisores porque si $a \mid 6$ entonces $|a| \leq |6| = 6$). En particular, 6 no es primo. En cambio, los únicos divisores de 7 son 1, 7 y sus opuestos, -1 y -7; por lo tanto, 7 es primo.

Los divisores positivos de 100 son todos los números que aparecen en el primero de los diagramas siguientes. Para cada natural que aparece en el diagrama, sus divisores positivos son todos los que aparecen debajo de él, unidos a éste por un camino formado por una o más líneas. Los otros dos diagramas tienen, de la misma manera, los divisores de 30 y 60.



Notación. El símbolo "$\Rightarrow$" que utilizaremos en lo sucesivo indica que toda vez que vale el enunciado de la izquierda, como consecuencia vale el de la derecha. Es decir, que el enunciado de la izquierda implica el enunciado de la derecha.

Ejemplo. Determinar todos los $n \in \mathbb{Z}$ tales que $2 \cdot n - 1$ divide a $n^2 + 7$.

Solución: Supongamos que $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$, en símbolos escribimos $(2 \cdot n - 1) \mid (n^2 + 7)$, entonces divide también a cualquier múltiplo de él, por ejemplo:

$$(2 \cdot n - 1) \mid 2 \cdot (n^2 + 7) = 2 \cdot n^2 + 14$$

Por otra parte, es claro que:

$$(2 \cdot n - 1) \mid n \cdot (2 \cdot n - 1) = 2 \cdot n^2 - n$$

Ahora usamos la propiedad 5, que implica que $a \mid b$ y $a \mid c \Rightarrow a \mid (b - c)$, entonces:

$$(2 \cdot n - 1) \mid [2 \cdot n^2 + 14 - (2 \cdot n^2 - n)] \Longrightarrow (2 \cdot n - 1) \mid (14 + n)$$

Por lo tanto, si $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$ entonces $2 \cdot n - 1$ divide a $14 + n$. Nuevamente, en particular:

$$(2 \cdot n - 1) \mid 2 \cdot (14 + n) = 28 + 2 \cdot n$$

$$(2 \cdot n - 1) \mid (2 \cdot n - 1)$$

y entonces $2 \cdot n - 1$ divide a la diferencia de los dos, es decir, divide a $28 + 2 \cdot n - (2 \cdot n - 1) = 29$. Por lo tanto, si $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$, entonces $2 \cdot n - 1$ divide a 29.

Si pensamos un momento en el número 29, nos damos cuenta de que el conjunto de todos sus divisores es:

$$\mathcal{D}_{29} = \{1,\ -1,\ 29,\ -29\}$$

(En general, si n es un entero no nulo, llamamos $\mathcal{D}_n$ al conjunto de divisores de n, que sabemos que es finito por la segunda propiedad.)

En consecuencia, $2 \cdot n - 1$ no puede ser otro número más que alguno de los elementos del conjunto anterior. Analicemos caso por caso todas las posibilidades:

- Si $2 \cdot n - 1 = 1$, entonces $n = 1 \Rightarrow n^2 + 7 = 8$ y es cierto que $1 \mid 8$.
- Si $2 \cdot n - 1 = -1$, entonces $n = 0 \Rightarrow n^2 + 7 = 7$ y es cierto que $-1 \mid 7$.
- Si $2 \cdot n - 1 = 29$, entonces $n = 15 \Rightarrow n^2 + 7 = 232$ y es cierto que $29 \mid 232$ porque $232 = 29 \cdot 8$.
- Si $2 \cdot n - 1 = -29$, entonces $n = -14 \Rightarrow n^2 + 7 = 203$ y es cierto que $-29 \mid 203$ porque $203 = -29 \cdot (-7)$.

Por lo tanto, las soluciones al problema son los elementos del conjunto:

$$\{1,\ 0,\ 15,\ -14\}$$

3.2. Algoritmo de división

Si el divisor no está contenido un número exacto de veces en el dividendo, la operación tiene un **resto**, como en el ejemplo al comienzo de esta sección, en el que se reparten siete lapiceras entre dos personas. Este **resto debe ser menor que el divisor.** Para efectuar la división de un número natural por otro y obtener la expresión

$$\textbf{Dividendo} = \textbf{Cociente} \cdot \textbf{Divisor} + \textbf{Resto}$$

el procedimiento es el que aprendimos en la escuela primaria. Recordemos que se escribe el dividendo a la izquierda y el divisor a la derecha, contenido en dos caras adyacentes de un rectángulo abierto a la derecha: si, por ejemplo, consideramos la división de 4.712, el dividendo, por 23, el divisor, el proceso empieza así:

$$4.712 \quad \big|23$$

y continúa como hacíamos en la escuela.

El resultado es el siguiente: 4.712 dividido 23 da un cociente de 204 y un resto de 20, que verificamos así:

$$204 \cdot 23 + 20 = 4.712$$

Algoritmo de división para números enteros: consideraciones de signo. ¿Qué pasa si queremos dividir por un número negativo? Por ejemplo, si nos interesa calcular 4.712 dividido -23, utilicemos el cálculo anterior en el cual **dividendo y divisor eran ambos positivos** y obtengamos la expresión para este caso. En efecto, **multipliquemos dos veces por -1 el primer término** de la igualdad (notar que esta operación no altera el resultado); luego usemos convenientemente la conmutatividad y la asociatividad del producto:

$$\begin{aligned} 4.712 &= 204 \cdot 23 + 20 \\ &= [(-1) \cdot (-1) \cdot (204 \cdot 23)] + 20 \\ &= [(-1) \cdot 204 \cdot (-1) \cdot 23] + 20 \\ &= (-204) \cdot (-23) + 20. \end{aligned}$$

Por lo tanto, en la división de 4.712 por -23 el cociente es -204 y el resto es 20.

El algoritmo de división exige que el resto sea siempre no negativo, es decir, positivo o cero.

Por ejemplo, si nos interesa calcular -4.712 dividido 23 **multiplicamos toda la expresión anterior por** -1**:**

$$\begin{aligned} -4.712 &= -(204 \cdot 23 + 20) \\ &= -204 \cdot 23 - 20 \end{aligned}$$

que es correcto, pero no cumple con la condición de que el resto sea positivo o cero. Para solucionar este problema, lo que hacemos es **sumar y restar 23, y luego conmutar y asociar convenientemente** para obtener:

$$\begin{aligned} -4.712 = -204 \cdot 23 - 20 + 23 - 23 &= (-204 \cdot 23 - 23) + (-20 + 23) \\ &= (-205) \cdot 23 + 3 \end{aligned}$$

que dice que en la división de -4.712 por 23 el cociente es -205 y el resto es 3.

Finalmente, el caso que falta considerar es el de dividir un número negativo por otro negativo, por ejemplo, -4.712 dividido -23; para ello, empezamos como antes **multiplicando toda la expresión inicial por** -1:

$$\begin{aligned} -4.712 &= -(204 \cdot 23 + 20) \\ &= 204 \cdot (-23) - 20 \end{aligned}$$

y de nuevo necesitamos **sumar y restar** 23 para obtener un resto no negativo:

$$\begin{aligned} -4.712 = 204 \cdot (-23) - 20 &= 204 \cdot (-23) - 23 + 23 - 20 \\ &= 205 \cdot (-23) + 3 \end{aligned}$$

que dice que en la división de -4.712 por -23 el cociente es 205 y el resto es 3.

Dados los enteros n y d, con $d \neq 0$, el algoritmo de división es el procedimiento que permite escribir de manera única

$$n = q \cdot d + r$$

donde $0 \leq r < |d|$. Los números q y r se dicen el cociente y el resto, respectivamente, de la división de n por d.

Notar que si $n = 0$, el algoritmo de división vale con $q = 0 = r$; en efecto, $0 = 0 \cdot d + 0$ cualquiera sea d no nulo.

Este enunciado se demuestra a continuación:

Teorema 2.1. *Sean $n, d \in \mathbb{Z}$ y $d \neq 0$, entonces existen $q, r \in \mathbb{Z}$ tales que $n = q \cdot d + r$ y $0 \leq r < |d|$; además, q y r son únicos con esta propiedad.*

Demostración. ***Caso d > 0.*** Para cada par $n, d \in \mathbb{Z}$ con $d > 0$, definamos el conjunto de los *candidatos a resto en la división de n por d*:

$$R = \{r \in \mathbb{N}_0 : \ r = n - q \cdot d, \ \text{para algún } q \in \mathbb{Z}\}$$

Entonces $R \neq \emptyset$; en efecto, mostremos un elemento en el conjunto: sea $r_1 = n - (-d \cdot |n|) \cdot d$, y veamos que $r_1 \in R$. Si $n = 0$ entonces $r_1 = 0 \in R$. Si $n > 0$, tenemos que r_1 se puede escribir como producto de dos factores positivos:

$$\begin{aligned} r_1 &= n - (-d \cdot |n|) \cdot d \\ &= n + d^2 \cdot n \\ &= n \cdot (1 + d^2) > 0 \end{aligned}$$

y si $n < 0$ entonces $|n| = -n$ y obtenemos que r_1 es el producto de dos factores negativos o cero:

$$\begin{aligned} r_1 &= n - (-d \cdot |n|) \cdot d \\ &= n - (-d \cdot (-\ n)) \cdot d \\ &= n - (d \cdot \ n\ ) \cdot d \\ &= n - \ d^2 \cdot \ n \\ &= n \cdot (\ 1 - d^2\ ) \geq 0 \end{aligned}$$

donde n es negativo y el segundo factor es negativo o cero, dado que:

$$d \geq 1 \Longrightarrow d^2 \geq d \geq 1 \Longrightarrow d^2 - 1 \geq 0$$

Por lo tanto, cualesquiera sean $n, d \in \mathbb{Z}$, $d > 0$, R es un subconjunto no vacío de $\mathbb{N}_0$; entonces R tiene primer elemento. Denotemos por r_0 al primer elemento de R, que, como todos los elementos de R, es de la forma $r_0 = n - q_0 \cdot d$ para algún $q_0 \in \mathbb{Z}$; es decir, *existe un q_0 en $\mathbb{Z}$ tal que el primer elemento de R se escribe como $r_0 = n - q_0 \cdot d$*; además, $r_0 \geq 0$ por pertenecer a R.

Afirmamos que $r_0 < d$; en efecto, si ocurriera que $r_0 \geq d$ entonces $r_0 - d \geq 0$; por otra parte:

$$r_0 - d = (n - q_0 \cdot d) - d = n - (q_0 + 1) \cdot d$$

que implicaría que $r_0 - d \in R$, pero $r_0 - d < r_0$ y esto contradice el hecho de que r_0 sea el primer elemento de R. Por lo tanto, necesariamente $0 \leq r_0 < d$.

Así, hemos probado que existen q_0 y r_0 en $\mathbb{Z}$ tales que $n = q_0 \cdot d + r_0$ satisfaciendo la condición $0 \leq r_0 < d$. Esto concluye la prueba de la existencia de enteros q y r con las propiedades del enunciado.

Ahora, comprobemos que q y r son únicos satisfaciendo estas propiedades. Supongamos, por el contrario, que existen q y r y también q' y r' tales que:

$$\begin{aligned} n &= q \cdot d + r \quad 0 \leq r < d \\ n &= q' \cdot d + r' \quad 0 \leq r' < d \end{aligned}$$

Sin pérdida de generalidad, podemos suponer que alguno de los dos restos es el más grande, por ejemplo, $r' \leq r$; entonces,

$$0 \leq r - r' < d$$

Luego, restando miembro a miembro una igualdad de la otra, obtenemos:

$$0 = (q - q') \cdot d + (r - r')$$

que es equivalente a:

$$\begin{aligned} r - r' &= -(q - q') \cdot d \\ &= (q' - q) \cdot d \end{aligned}$$

Dado que $0 \leq r - r'$ y $d > 0$ obtenemos que $q' - q \geq 0$. Si $q' - q = 0$, entonces también $r - r' = 0$ y, necesariamente, $q' = q$ y $r' = r$. Si $q' - q > 0$, entonces $q' - q \geq 1$ porque es un entero; esto implica que $(q' - q) \cdot d \geq d$, pero el lado izquierdo de esta desigualdad es igual a $r - r'$ que sabíamos que era menor que d. Llegamos a una contradicción por haber supuesto que $q' \neq q$. Por lo tanto, debe ser $q' = q$ y $r' = r$.

Caso d < 0. Le aplicamos el caso anterior a $n \in \mathbb{Z}$ cualquiera y $-d > 0$; luego existen $q, r \in \mathbb{Z}$ tales que:

$$n = q \cdot (-d) + r, \quad 0 \leq r < (-d)$$

Notar que $|d| = -d$ pues $d < 0$, entonces la desigualdad anterior dice que $0 \leq r < |d|$. A la vez, podemos reescribir la igualdad anterior como:

$$\begin{aligned} n &= q \cdot (-d) + r \\ &= (-q) \cdot d + r, \quad 0 \leq r < |d| \end{aligned}$$

Por lo tanto, el cociente de la división de n por d es $-q \in \mathbb{Z}$ y el resto es r, que satisface $0 \leq r < |d|$ como acabamos de ver. La unicidad de q y r con estas propiedades se demuestra de manera análoga al caso $d > 0$ reemplazando d por $|d|$.

Algoritmo de división para calcular (q, r) donde q es el cociente y r es el resto de la división de n por $d \neq 0$.

- Si n ≥ 0 y d > 0:
  - tomar q = 0, r = n;
  - mientras que r ≥ d, reemplazar
    q ← q + 1,
    r ← r - d
  - dar como respuesta (q, r).

- Si n ≥ 0 y d < 0 aplicar el algoritmo a n y -d y dar como respuesta (-q, r).

- Si n < 0 y d > 0:
  - aplicar el algoritmo a -n y d;
  - si r = 0, dar como respuesta (-q, 0);
  - si no, dar como respuesta (-q - 1, d - r).

- Si n < 0 y d < 0:
  - aplicar el algoritmo a -n y -d;
  - si r = 0, dar como respuesta (q, 0);
  - si no, dar como respuesta (q + 1,-r - d).

□ 4. Desarrollos en base *b*

Para escribir los números, normalmente, usamos el *desarrollo decimal o desarrollo en base* 10, que se obtiene a partir del conjunto de los diez símbolos:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

Pero, a veces es útil conocer desarrollos en distintas bases de un número natural. Por ejemplo, las computadoras utilizan el *sistema binario* en el cual cualquier natural se expresa como una secuencia de unos y ceros.

En base 10, los números naturales se escriben como 1, 2, 3, 4, 5, 6, 7, 8, 9; para escribir el siguiente natural, el diez, se vuelve a empezar con el cero, pero anteponiendo un 1, o sea que el diez se expresa como 10, que es como lo conocemos.

De este modo, agotados los 10 símbolos empiezan los números de dos cifras. A partir del 9, los 10 siguientes naturales empiezan todos con un 1, es decir que hay 10 números que tienen al 1 en la cifra de las decenas; las unidades van siempre de 0 a 9; el veinte, que es el siguiente al 19, se obtiene sumando una unidad a la cifra 1 de las decenas, que entonces se convierte en un 2, y reemplazando el 9 de las unidades por un cero, es decir, 20; y así sucesivamente.

Notar que, como consecuencia, todo natural se expresa como una suma de múltiplos de potencias de 10. Por ejemplo, el número 5.607 es:

$$\begin{aligned} 5.607 &= 7 + 0 \cdot 10 + 6 \cdot 100 + 5 \cdot 1.000 \\ &= 7 + 0 \cdot 10 + 6 \cdot 10^2 + 5 \cdot 10^3 \end{aligned}$$

Si en lugar de usar diez símbolos, usamos solamente siete, 0, 1, 2, 3, 4, 5 y 6, obtenemos el *desarrollo en base* 7 de los naturales y el cero como secuencias de estos símbolos. En particular, el número siete se escribe en base 7 como un 10 porque es el siguiente al número seis que es el último de los siete símbolos a disposición:

$$(7)_{10} = (10)_7$$

El subíndice a la derecha indica la base en la cual está escrito el número entre paréntesis. Así, $(8)_{10} = (11)_7$; $(9)_{10} = (12)_7$; $(10)_{10} = (13)_7$; $(11)_{10} = (14)_7$; etcétera.

Entonces, el cero y los primeros naturales se escriben en base 7 así:

$$\{(0)_7, (1)_7, (2)_7, (3)_7, (4)_7, (5)_7, (6)_7, (10)_7, (11)_7, (12)_7, (13)_7, (14)_7, (15)_7,$$
$$(16)_7, (20)_7, (21)_7, (22)_7, (23)_7, (24)_7, (25)_7, (26)_7, (30)_7, (31)_7, (32)_7,$$
$$(33)_7, (34)_7, (35)_7, (36)_7, (40)_7, (41)_7, \ldots\}$$

Para obtener el desarrollo en base *b* de un número *n* expresado en el sistema decimal, aplicamos el algoritmo de división. El procedimiento consiste en dividir *n* sucesivamente por *b*.

Por ejemplo, para calcular el desarrollo en base 7 de 639, dividimos 639 por 7 y escribimos:

$$639 = 91 \cdot 7 + 2, \quad q_0 = 91, \ r_0 = 2$$

A continuación, dividimos a 91, el cociente de la división anterior, por 7; entonces:

$$91 = 13 \cdot 7 + 0, \quad q_1 = 13, \ r_1 = 0$$

Así siguiendo, dividimos por 7 los sucesivos cocientes; cuando se obtiene un cociente igual a cero, el proceso termina:

$$\begin{aligned} 13 &= 1 \cdot 7 + 6, \quad q_2 = 1, \ r_2 = 6 \\ 1 &= 0 \cdot 7 + 1, \quad q_3 = 0, \ r_3 = 1 \end{aligned}$$

Luego,

$$\begin{aligned} 639 &= 91 \cdot 7 + 2 \\ &= (13 \cdot 7 + 0) \cdot 7 + 2 \\ &= 13 \cdot 7^2 + 0 \cdot 7 + 2 \\ &= (1 \cdot 7 + 6) \cdot 7^2 + 0 \cdot 7 + 2 \\ &= 1 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 2 \end{aligned}$$

Los coeficientes del desarrollo en base 7 son los sucesivos restos:

$$\begin{aligned} 639 &= (r_3 r_2 r_1 r_0)_7 \\ &= (1.602)_7 \end{aligned}$$

Recíprocamente, si queremos recuperar el 639 de su escritura en base 7, desarrollamos la suma de las potencias de 7 de acuerdo a la expresión del número:

$$(r_3 r_2 r_1 r_0)_7 = r_3 \cdot 7^3 + r_2 \cdot 7^2 + r_1 \cdot 7 + r_0$$

En el ejemplo anterior:

$$\begin{aligned} (1.602)_7 &= 1 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 2 \cdot 7^0 \\ &= 343 + 6 \cdot 49 + 2 \\ &= 343 + 294 + 2 \\ &= 639 \end{aligned}$$

Para estudiar el *desarrollo binario o en base* 2, procedemos igual tomando el 2 como base. Por ejemplo: ¿cómo se expresa el 27 en base 2? Como antes, si aplicamos el algoritmo de división de 27 por 2, obtenemos 27 = 13 · 2 + 1. A continuación, dividimos el cociente, 13, por 2, y así se sigue:

$$\begin{aligned} 27 &= 13 \cdot 2 + 1, \quad q_0 = 13, \quad r_0 = 1 \\ 13 &= 6 \cdot 2 + 1, \quad q_1 = 6, \quad r_1 = 1 \\ 6 &= 3 \cdot 2 + 0, \quad q_2 = 3, \quad r_2 = 0 \\ 3 &= 1 \cdot 2 + 1, \quad q_3 = 1, \quad r_3 = 1 \\ 1 &= 0 \cdot 2 + 1, \quad q_4 = 0, \quad r_4 = 1 \end{aligned}$$

Luego 27 = $(11011)_2$. Recíprocamente, si queremos recuperar el 27 de su escritura en base 2, desarrollamos la suma de las potencias de 2 de acuerdo a la expresión del número:

$$(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1$$

$$(11011)_2 = 16 + 8 + 2 + 1$$
$$= 27$$

Algoritmo para calcular el desarrollo en base b de un número natural n.

- Comenzar con m = n, s = $(\ )_b$.
- Mientras que m ≠ 0:
  - hallar el cociente q y el resto r de la division de m por b;
  - agregar r como la cifra de más a la izquierda en s;
  - reemplazar m ← q.
- Dar como respuesta s.

Además de bases b donde b es un número de 2 a 10, en distintas situaciones de la ciencia y de la vida cotidiana se utilizan otras bases. ¡Veamos qué interesantes son los siguientes ejemplos!

Ejemplo. En ciencias de la computación se utiliza, además del sistema binario, el *sistema hexadecimal o en base* 16, que permite expresar cualquier número natural a partir de los siguientes símbolos:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F\}$$

En esta base, el símbolo A significa el número 10 en base diez, o sea:

$$(A)_{16} = (10)_{10}$$

Análogamente:

$$(B)_{16} = (11)_{10},\ (C)_{16} = (12)_{10},\ (D)_{16} = (13)_{10},\ (E)_{16} = (14)_{10},\ (F)_{16} = (15)_{10}$$

Para escribir el 16 en base 16, necesitamos dos símbolos, es decir:

$$(16)_{10} = (10)_{16}$$

A partir de este número, se tienen en total 16^2 números de dos dígitos o símbolos, lo que es muy económico en términos computacionales; esto justifica que el sistema hexadecimal sea muy utilizado en informática. En efecto, en computación se utiliza frecuentemente el byte como unidad de memoria; un byte representa 2^8 valores posibles, y este número se escribe en base 16 como $(100)_{16}$ pues:

$$2^8 = 2^4 \cdot 2^4 = 16 \cdot 16 = 1 \cdot 16^2 + 0 \cdot 16^1 + 0 \cdot 16^0 = (100)_{16}$$

Una unidad menos es $2^8 - 1 = (FF)_{16}$ que es el mayor número que puede representarse con solamente dos símbolos en base 16; por lo tanto dos dígitos hexadecimales corresponden exactamente a un byte.

Ejercicio 2.2. Comprobar que $(59792018174)_{10} = (\text{DEBE1CAFE})_{16}$

Ejemplo. La hora se expresa en horas, minutos y segundos, que en realidad sigue el esquema de numeración en base 60, conocida como *base sexagesimal*. En efecto, una hora tiene 60 minutos y un minuto tiene 60 segundos.

Para una duración desde 0 hasta 59 segundos, se utilizan los números naturales habituales. Pero ¿cómo se expresan duraciones de tiempo más largas? Por ejemplo, en lugar de decir

que un nadador olímpico completó la trayectoria de la prueba en 97 segundos, se dice que la recorrió en 1 minuto y 37 segundos, y se escribe 00:01:37.

Si observamos alguna vez un cronómetro o un reloj digital que expresa la hora en horas, minutos y segundos, veremos que pasa de 00:00:59 a 00:01:00, que significa una unidad de 60 segundos, o sea, 1 minuto. Si un reloj así marca 10:38:09, entendemos que son las diez de la mañana, treinta y ocho minutos y nueve segundos.

Si quisiéramos convertir esta expresión a un número en base diez, cuyo significado es el tiempo transcurrido desde las cero horas, medido en segundos, calculamos:

$$10:38:09 = 10 \cdot 60^2 + 38 \cdot 60 + 9 = 38.289 \text{ segundos}$$

Ejemplo. Veamos otro ejemplo en base sexagesimal. Conocemos en geometría el uso del número sesenta como base para la medición de ángulos. Cada ángulo puede describirse en grados, minutos y segundos. Un grado equivale a 60 minutos y un minuto a 60 segundos.

□ 5. Máximo común divisor

Además de poder averiguar todos los divisores de un número, a veces es importante conocer los divisores comunes de dos enteros para contestar la pregunta, ¿cuánto vale el divisor más grande de ambos?

Por ejemplo, los divisores *positivos* de 54 forman el conjunto:

$$\mathcal{D}_{54} = \{1,\ 2,\ 3,\ 6,\ 9,\ 18,\ 27,\ 54\ \}$$

Por otra parte, los divisores *positivos* de 60 son:

$$\mathcal{D}_{60} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60\ \}$$

Notemos que los naturales 1, 2, 3 y 6 están en ambos conjuntos, es decir, que son *divisores comunes de* 54 *y* 60, de los cuales el máximo es el 6. En otras palabras, 6 es el *máximo común divisor de* 54 *y* 60; lo denotamos así:

$$mcd\,(54\ ,\ 60) = 6 \text{ ó también } (54 : 60) = 6.$$

Precisemos la definición usando el concepto de divisibilidad:

Dados a y b en $\mathbb{Z}$, ambos distintos de cero, *el máximo común divisor* de a y b es un número natural d que verifica:

1) $d \mid a$ y $d \mid b$.
2) Si $c \in \mathbb{Z}$ es cualquier otro entero tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

La primera condición de la definición exige que *d* sea divisor de *a* y de *b*; la segunda, que sea el máximo entre todos los divisores comunes de *a* y *b*, ya que cualquier otro divisor común *c* divide a *d*.

Además, por definición, el máximo común divisor es positivo, aún si *a* y *b* no lo son. Por ejemplo, el máximo común divisor entre -54 y 60 es *d* = 6; más aún:

$$\begin{aligned} 6 &= mcd\,(54\ ,\ 60) \\ &= mcd\,(-54\ ,\ 60) \\ &= mcd\,(54\ ,\ -60) \\ &= mcd\,(-54\ ,\ -60) \end{aligned}$$

Una forma de calcular el máximo común divisor entre dos números es, como acabamos de ver, determinar todos los divisores de cada uno de los números y entre los divisores de ambos, tomar el máximo. Pero hay un procedimiento, llamado **algoritmo de Euclides**[3], debido al matemático griego homónimo, que es mucho más corto, se aplica a los valores absolutos de los enteros dados y se realiza del siguiente modo:

1) dividir el mayor de los dos números dados por el otro; en nuestro ejemplo, efectuamos *60 dividido 54* y obtenemos, por el algoritmo de división:

$$60 = 1 \cdot 54 + 6$$

2) dividir al segundo número por el resto anterior, o sea, *dividimos 54 por 6 y* obtenemos:

$$54 = 9 \cdot 6 + 0$$

3) el paso siguiente sería tomar el resto de la división anterior y dividirlo por el resto de ésta, y así sucesivamente hasta obtener resto 0. El **máximo común divisor es el último resto no nulo**.

En el ejemplo, el resto que obtuvimos en el paso anterior es cero y entonces el proceso termina acá, es decir, 6 = *mcd* (54, 60).

Notar que, si un entero *d* es un divisor tanto de 60 como de 54, entonces necesariamente *d* divide a 6. Más aún, para cada par de enteros *a* y *b*, **los divisores comunes de *a* y *b* son exactamente los mismos que los divisores comunes de *b* y *a* + *k.b* para cualquier entero *k*** por la propiedad 5 de divisibilidad. En particular, coinciden con los divisores comunes de *b* y el resto de la división de *a p*or *b*. Es por este motivo que el último resto no nulo en el algoritmo de Euclides resulta ser el máximo común divisor entre *a* y *b*. La comprobación precisa, en el caso general, está dada en la demostración del teorema.

Desarrollemos dos ejemplos más antes de plantear el teorema.

[3] Euclides fue un matemático griego que vivió alrededor del año 300 a.C. Estudió en Atenas y fundó una escuela de matemática en Alejandría (Egipto). Su obra Los Elementos es una de las obras científicas más conocidas del mundo. Este tratado de geometría ha sido utilizado como libro de texto durante 2.000 años y es, con algunas modificaciones, la base de los libros de texto de geometría plana de hoy, por lo cual se conoce a Euclides como al Padre de la Geometría. Euclides presentó el algoritmo que describiremos para resolver un problema geométrico: encontrar la medida más grande que puede utilizarse para medir, sin resto, dos segmentos de recta.

Ejemplos

a) Calcular el *mcd* (210, 99) usando el algoritmo de Euclides:

$$\begin{array}{rcll} 210 & = & 2 \cdot 99 + 12; & r_1 = 12 \\ 99 & = & 8 \cdot 12 + 3; & r_2 = 3 \\ 12 & = & 4 \cdot 3 + 0; & r_3 = 0 \end{array}$$

Entonces, el *mcd* (210, 99) = 3. En efecto, 210 = 3 · 70 y 99 = 33 · 3, ó sea que 3 es un divisor común. Más aún, como 70 y 33 no tienen divisores comunes salvo el 1, deducimos que 3 es el **máximo** de los divisores comunes.

b) Calcular el mcd (630, 50) usando el algoritmo de Euclides:

$$\begin{array}{rcll} 630 & = & 12 \cdot 50 + 30; & r_1 = 30 \\ 50 & = & 1 \cdot 30 + 20; & r_2 = 20 \\ 30 & = & 1 \cdot 20 + 10; & r_3 = 10 \\ 20 & = & 2 \cdot 10 + 0; & r_4 = 0 \end{array}$$

Entonces, el *mcd* (630, 50) = 10. En efecto, 630 = 63 · 10 y 50 = 5 · 10, entonces 10 es un divisor común. Como 5 y 63 no tienen divisores comunes salvo el 1, deducimos que 10 es el **máximo** de los divisores comunes.

Observación. ¿Cuánto vale el *mcd* (0, *a*) para $a \neq 0$? La respuesta es que:

$$mcd\,(0\ ,\ a) = a \quad \text{para todo } a > 0$$

dado que $a \mid a$, también $a \mid 0$ y $a \geq 1 > 0$. Si $a < 0$,

$$mcd\,(0\ ,\ a) = |a| = -a \in \mathbb{N}$$

El máximo común divisor de *a* y *b* no está definido si *a* = 0 y *b* = 0.

5.1. Algoritmo de Euclides

A continuación enunciamos y demostramos el teorema que justifica la existencia del máximo común divisor y provee el algoritmo que permite calcularlo.

Teorema 2.2 (Existencia y unicidad del máximo común divisor). *Dados $a, b \in \mathbb{Z}$, no simultáneamente nulos, existe un único $d \in \mathbb{N}$ que satisface las condiciones:*

1) $d \mid a$ y $d \mid b$.
2) Si $c \in \mathbb{Z}$ es cualquier otro entero tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

El número d se llama el máximo común divisor *de a y b.*

Demostración. Teniendo en cuenta la observación anterior, basta considerar el caso

$a \neq 0$ y $b \neq 0$. Además, como ya hemos observado en el ejemplo posterior a la definición de máximo común divisor es:

$$mcd\,(a\ ,\ b) = mcd\,(|a|\ ,\ |b|)$$

En consecuencia, basta probar el resultado para $a > 0$ y $b > 0$.

Existencia del máximo común divisor. Como ya hemos visto en los ejemplos, el algoritmo de Euclides se basa en el algoritmo de división. Supongamos que $a > b > 0$ y apliquémosle el algoritmo de división a a y b; entonces existen enteros q_1 y r_1 tales que:

$$a = q_1 \cdot b + r_1 \text{ y } 0 \leq r_1 < b$$

Si $r_1 = 0$, entonces $b \mid a$ y el $mcd\ (a, b) = b$. Si $r_1 \neq 0$, dado que $0 < r_1 < b$, podemos efectuar la división de b por r_1, entonces existen enteros q_2 y r_2 tales que:

$$b = q_2 \cdot r_1 + r_2 \text{ y } 0 \leq r_2 < r_1$$

Si $r_2 = 0$, el proceso termina. Si no, tenemos que $0 < r_2 < r_1$ y dividimos r_1 por r_2; existen q_3 y r_3 del algoritmo de división. Si $r_3 \neq 0$, dividimos r_2 por r_3, y así sucesivamente:

$$\begin{array}{rcll} a & = & q_1 \cdot b + r_1 & 0 \leq r_1 < b \\ b & = & q_2 \cdot r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_3 \cdot r_2 + r_3 & 0 \leq r_3 < r_2 \\ r_2 & = & q_4 \cdot r_3 + r_4 & 0 \leq r_4 < r_3 \\ & & \vdots & \end{array}$$

Pero estos restos se van haciendo cada vez más chicos y no pueden ser menores que cero; por lo tanto, en algún paso, el resto se hace cero y el algoritmo termina. Explícitamente, para algún n, obtenemos $r_n = 0$, es decir que en el paso n-ésimo ocurre lo siguiente:

$$\begin{array}{rcll} r_{n-3} & = & q_{n-1} \cdot r_{n-2} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = & q_n \cdot r_{n-1} & \end{array}$$

En particular, la última igualdad dice que $r_{n-1} \mid r_{n-2}$; pero entonces, la anterior implica que también $r_{n-1} \mid r_{n-3}$ por la propiedad 5 de divisibilidad. Así siguiendo, $r_{n-1} \mid r_{n-4}$, etcétera; obtenemos que $r_{n-1} \mid r_1$, $r_{n-1} \mid b$, y finalmente, $r_{n-1} \mid a$. Por lo tanto, r_{n-1} divide a ***a*** y a ***b***, es decir, es un **divisor común de *a* y *b*.**

Afirmamos que r_{n-1}, que es el último resto distinto de cero, es el máximo común divisor. Para probarlo, falta ver que si c es un divisor cualquiera de a y b, entonces $c \mid r_{n-1}$.

Sea c un divisor cualquiera de a y b; si recorremos de manera inversa el camino anterior, de la primera igualdad se desprende que $c \mid r_1$, ya que:

$$a = q_1 \cdot b + r_1,\ c \mid a,\ c \mid b \Longrightarrow c \mid r_1$$

Análogamente, usando la segunda igualdad, tenemos que como $c \mid b$ y $c \mid r_1$, entonces $c \mid r_2$.

Así siguiendo, obtenemos que c divide a todos los restos que van apareciendo. En particular, $c \mid r_{n-1}$. Por lo tanto, $r_{n-1} = mcd\,(a\,,\,b)$.

Unicidad del máximo común divisor. Supongamos que tenemos dos máximos comunes divisores, d_1 y d_2, es decir que d_1 y $d_2 \in \mathbb{N}$ verifican ambos las condiciones 1) y 2) del enunciado; entonces, dado que $d_1 \mid a$, $d_1 \mid b$ y d_2 cumple la condición 2), obtenemos que $d_1 \mid d_2$. Por el mismo razonamiento, $d_2 \mid d_1$. Luego, la propiedad 3 de divisibilidad dice que $|d_1| = |d_2|$ y al ser ambos positivos, $d_1 = d_2$.

Algoritmo de Euclides para calcular el máximo común divisor entre dos naturales no nulos a y b.

- Comenzar con $r_1 = a$, $r_2 = b$.
- Mientras que $r_2 \neq 0$:
  - hallar el resto r de la division de r_1 por r_2;
  - reemplazar
    $r_1 \leftarrow r_2$,
    $r_2 \leftarrow r$.
- Dar como respuesta r_1.

5.2. El máximo común divisor como combinación lineal entera de a y b

Una propiedad importante del máximo común divisor de a y b es que se lo puede escribir como **combinación lineal entera** de a y de b; más aún, el máximo común divisor es el natural más chico con esta propiedad.

Si $d \in \mathbb{Z}$, decimos que d es combinación lineal entera de a y b, si existen $m,\ n \in \mathbb{Z}$ tales que:

$$d = a \cdot m + b \cdot n$$

Veamos cómo calcular esta escritura para el máximo común divisor en un ejemplo. El $mcd\,(630,\ 50) = 10$. En efecto, por el algoritmo de Euclides:

$$\begin{array}{rcl@{\quad}rcl} 630 &=& 12 \cdot 50 + 30; & r_1 &=& 30 \\ 50 &=& 1 \cdot 30 + 20; & r_2 &=& 20 \\ 30 &=& 1 \cdot 20 + 10; & r_3 &=& 10 \\ 20 &=& 2 \cdot 10 + 0; & r_4 &=& 0 \end{array}$$

Para escribir a 10 como una combinación lineal entera de 630 y 50, recorremos en sentido inverso los pasos que efectuamos en el algoritmo y despejamos en cada nivel el resto, empezando por $d = 10$:

$$\begin{array}{rcl@{\quad}rcl} 30 &=& 1 \cdot 20 + 10 & \Longrightarrow & 10 &=& 30 - 20 \\ 50 &=& 1 \cdot 30 + 20 & \Longrightarrow & 20 &=& 50 - 30 \\ 630 &=& 12 \cdot 50 + 30 & \Longrightarrow & 30 &=& 630 - 12 \cdot 50 \end{array}$$

Luego, reemplazamos a cada resto por la expresión obtenida en cada uno de los pasos anteriores:

$$\begin{array}{rcl} 10 &=& 30 - 20 \\ &=& 30 - (50 - 30) \;=\; -50 + 2 \cdot 30 \\ &=& -50 + 2 \cdot (630 - 12 \cdot 50) \;=\; 50 \cdot (-25) + 630 \cdot 2 \end{array}$$

Obteniendo así la combinación lineal entera:

$$10 = 50 \cdot (-25) + 630 \cdot 2$$

Ejemplo. Probar que si $a, b \in \mathbb{Z}$ son tales que $mcd\,(a, b) = 5$, entonces $mcd\,(a + 2 \cdot b, 3 \cdot a + 4 \cdot b) = 5$ ó 10.

Solución. Llamemos $d = mcd\,(a + 2 \cdot b, 3 \cdot a + 4 \cdot b)$; entonces d divide a ambos números, en particular, divide a sus múltiplos y a la suma y a la diferencia de múltiplos de ellos, por ejemplo:

$$\begin{aligned} d \mid (a + 2 \cdot b) \quad &\Rightarrow d \mid 3 \cdot (a + 2 \cdot b) \\ d \mid 3 \cdot (a + 2 \cdot b) \text{ y } d \mid (3 \cdot a + 4 \cdot b) \quad &\Rightarrow d \mid [3 \cdot (a + 2 \cdot b) - (3 \cdot a + 4 \cdot b)] \end{aligned}$$

Entonces, d divide a $3 \cdot (a + 2 \cdot b) - (3 \cdot a + 4 \cdot b) = 6 \cdot b - 4 \cdot b = 2 \cdot b$

Análogamente:

$$\begin{aligned} d \mid (a + 2 \cdot b) \quad &\Rightarrow d \mid 2 \cdot (a + 2 \cdot b) = 2 \cdot a + 4 \cdot b \\ d \mid (2 \cdot a + 4 \cdot b) \text{ y } d \mid (3 \cdot a + 4 \cdot b) \quad &\Rightarrow d \mid [(3 \cdot a + 4 \cdot b) - (2 \cdot a + 4 \cdot b)] \end{aligned}$$

Entonces, d divide a $(3 \cdot a + 4 \cdot b) - (2 \cdot a + 4 \cdot b) = 3 \cdot a - 2 \cdot a = a$

En consecuencia:

$$\boxed{d \text{ divide a } a \text{ y } d \text{ divide a } 2 \cdot b}$$

Por otra parte, dado que $mcd\,(a, b) = 5$, existen $m, n \in \mathbb{Z}$ tales que:

$$5 = m.a + n.b$$

Si multiplicamos a ambos miembros por 2, obtenemos:

$$10 = (2 \cdot m) \cdot a + n \cdot (2 \cdot b)$$

Pero entonces, como consecuencia de este hecho y de la afirmación recuadrada, necesariamente d divide a 10. Por lo tanto:

$$\boxed{d \text{ es igual a } 1,\ 2,\ 5 \text{ ó } 10}$$

Sólo falta descartar que d sea 1 ó 2. Notar que $mcd\,(a, b) = 5$ implica que $5 \mid a$ y $5 \mid b$, entonces 5 divide a $a + 2 \cdot b$ y a $3 \cdot a + 4 \cdot b$. Entonces, por definición de d, obtenemos también que 5 divide a d. Por lo tanto, d no puede ser ni 1 ni 2.

Más aún, notar que si a es par, entonces $a+2 \cdot b$ y $3 \cdot a+4 \cdot b$ son ambos números pares, por lo tanto, $d = 10$, mientras que si a es impar, $a + 2 \cdot b$ también es impar y en este caso, $d = 5$.

Ejercicio 2.3. Probar que $mcd\,(2^n + 7^n, 2^n - 7^n) = 1$ para todo $n \in \mathbb{N}$.

Dos enteros a y b se dicen *coprimos,* si su máximo común divisor es igual a 1.

Notar que, en este caso, el número 1 se escribe como combinación lineal entera de a y b. En efecto, el $mcd\,(a\,,\,b)$ verifica siempre esta propiedad.

Recíprocamente, si existen $m,\ n \in \mathbb{Z}$ tales que:

$$1 = a \cdot m + b \cdot n$$

entonces, $mcd\,(a,\ b) = 1$. En efecto, si $d = mcd\,(a,\ b) \in \mathbb{N}$, dado que d divide a a y b, por la propiedad 5 de divisibilidad, d divide a $a \cdot m + b \cdot n = 1$. Pero el único divisor *positivo* de 1 es el mismo 1; por lo tanto, $d = 1$.

En resumen, el razonamiento anterior es la comprobación del siguiente enunciado:

Proposición 2.3. *Dos enteros a y b son coprimos si y sólo si existen* $m,\ n \in \mathbb{Z}$ *tales que* $1 = a \cdot m + b \cdot n$

Una propiedad importante que se deduce de ésta es la siguiente:

Proposición 2.4. *Dados enteros a, b, c tales que* $a \mid b \cdot c$, *si a y b son coprimos entonces* $a \mid c$.

Demostración. Como a y b son coprimos, existen m y $n \in \mathbb{Z}$ tales que $1 = a \cdot m + b \cdot n$. Multiplicando esta igualdad por c obtenemos que $c = a \cdot c \cdot m + b \cdot c \cdot n$. Claramente, a divide al primer término, y también divide al segundo porque divide a $b \cdot c$. Luego, a divide a c.

□ 6. Teorema fundamental de la aritmética

El teorema fundamental de la Aritmética, Teorema 2.6 de esta sección, afirma que todo entero, distinto de 0, 1 y -1, puede representarse como un producto de números primos. Su nombre está plenamente justificado por las consecuencias importantes que se desprenden de él y por sus innumerables aplicaciones. Antes de enunciarlo necesitamos recordar la noción de número primo y probar una propiedad que cumplen estos números.

Un número entero se dice *primo* si tiene exactamente cuatro divisores distintos; en otras palabras, $n \in \mathbb{Z}$ es primo si y sólo si sus únicos divisores son 1, -1, n y $-n$ y estos son todos distintos. Un número entero distinto de 1, -1 y 0 que no es primo se dice *compuesto*.

La razón del nombre "compuesto", como veremos enseguida, es que **si** $n \neq 1, -1, 0$ **no es primo, entonces** n **es un producto de primos.**

El 1 no es primo. Los primeros primos positivos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, etcétera.

Proposición 2.5. *Si un primo p divide a un producto de dos enteros, entonces p divide a alguno de los factores.*

Demostración. Sea p un primo positivo que divide a un producto de dos enteros $m \cdot n$. Si p dividiera a m valdría el enunciado. Supongamos que p no divide a m, entonces p y m son coprimos. Demostremos esta afirmación. Sea $d = mcd\,(p, m)$ entonces $d \mid p$ que es primo; luego $d = 1$ o $d = p$, pero en el último caso tendríamos que $p = d \mid m$, que contradice la hipótesis; por lo tanto, $d = 1$.

Tenemos entonces que $p \mid m \cdot n$, y p es coprimo con m, con lo cual, por la Proposición 2.4, necesariamente $p \mid n$.

Se prueba por inducción que el enunciado anterior se extiende a productos de una cantidad arbitraria de factores.

Observación. Para el teorema utilizaremos la siguiente notación: para indicar un producto de r factores, digamos $p_1 \cdot p_2 \ldots p_r$ se utiliza la escritura abreviada

$$p_1 \cdot p_2 \cdots p_r = \prod_{i=1}^{r} p_i$$

El símbolo de la derecha indica el producto de los factores p_i, donde el subíndice i toma los valores 1 a r, esto es, el producto de los números p_1, p_2, ... hasta p_r. Por ejemplo: si $r = 4$ y los cuatro factores son $p_1 = 2$, $p_2 = 5$, $p_3 = 7$ y $p_4 = 11$, entonces:

$$\begin{aligned}\prod_{i=1}^{4} p_i &= p_1 \cdot p_2 \cdot p_3 \cdot p_4 \\ &= 2 \cdot 5 \cdot 7 \cdot 11\end{aligned}$$

Teorema 2.6 (Teorema Fundamental de la Aritmética). *Todo $n \in \mathbb{Z}$, $n \neq 0$, 1,-1, se factoriza como producto de primos. Explícitamente, todo $n \in \mathbb{N}$, $n \neq 1$, se escribe como producto de primos positivos,*

$$\begin{aligned}n &= \prod_{i=1}^{r} p_i \\ &= p_1 \cdot p_2 \cdots p_r\end{aligned}$$

y esta factorización es única, salvo por el orden de los factores.

Todo $n \in \mathbb{Z}$, $n < -1$, se escribe como -1 por un producto de primos positivos,

$$\begin{aligned}n &= (-1) \cdot \prod_{i=1}^{r} p_i \\ &= (-1) \cdot p_1 \cdot p_2 \cdots p_r\end{aligned}$$

y esta factorización es única, salvo por el orden de los factores.

Demostración. Probemos primero el enunciado para $n \in \mathbb{N}$, $n \neq 1$. Consideremos el conjunto:

$$\mathcal{P} = \{n \in \mathbb{N} : n \neq 1 \text{ y } n \text{ no admite factorización en primos positivos}\}$$

Dado que $\mathcal{P} \subset \mathbb{N}$, si fuera no vacío, $\mathcal{P}$ tendría un primer elemento, digamos n_0. En particular, n_0 no sería primo (pues si lo fuera, n_0 sería igual a una factorización en primos de un único factor, el mismo n_0), entonces existirían $d, q \in \mathbb{N}$, distintos de 1 y de n_0, tales que $n_0 = d \cdot q$; más aún, d y q deberían ser menores que n_0 por ser divisores de n_0. Por lo tanto, ni d ni q pertenecerían a $\mathcal{P}$, y entonces serían factorizables en primos, en cuyo caso el mismo n_0 se factorizaría también, lo cual sería una contradicción. Por lo tanto, $\mathcal{P}$ es vacío, es decir, *todo natural salvo el* 1 *se factoriza como un producto de primos positivos*.

Si $n \in \mathbb{Z}$, $n < -1$, entonces $-n$ es positivo, distinto de 1 y se factoriza como un producto de primos positivos, digamos:

$$\begin{aligned} -n &= \prod_{i=1}^{r} p_i \\ &= p_1 \cdot p_2 \cdots p_r \end{aligned}$$

que implica:

$$\begin{aligned} n &= -\prod_{i=1}^{r} p_i \\ &= (-1) \cdot \prod_{i=1}^{r} p_i \\ &= (-1) \cdot p_1 \cdot p_2 \cdots p_r \end{aligned}$$

Por lo tanto, *todo entero negativo distinto de* -1 *se escribe como* -1 *por un producto de primos positivos*.

Veamos que la factorización es única, salvo por el orden de los factores. Para esto basta considerar el caso de números naturales. La prueba procede por inducción en r, la cantidad de factores primos en una descomposición.

Definamos la proposición $P(r)$: *Si un número natural admite una factorización como producto de r factores primos positivos, esta factorización es única, salvo por el orden de los factores.*

Si $r = 1$, el número en cuestión es producto de un único factor, es decir, es un primo p y, por lo tanto, no tiene divisores distintos de 1 y p. Entonces, si p admite una factorización $p = p_1 \cdots p_s$ como producto de primos positivos, debe ser $s = 1$ y $p_1 = p$ (de lo contrario, p_1 sería un divisor de p y $p_1 \neq 1, p$).

Probemos el paso inductivo. Sea n un natural que admite una factorización como producto de $r + 1$ factores primos y veamos que esta factorización es única.

Supongamos que:

$$\begin{aligned} n &= \prod_{i=1}^{r+1} p_i \\ &= p_1 \cdot p_2 \cdots p_r \cdot p_{r+1} \end{aligned}$$

y también, para algún $r' \in \mathbb{N}$:

$$\begin{aligned} n &= \prod_{j=1}^{r'} p'_j \\ &= p'_1 \cdot p'_2 \cdots p'_{r'} \end{aligned}$$

Todos los primos que aparecen en la factorización de *n*, dividen a *n*. Por ejemplo: el primo p_{r+1} divide a *n*, o sea que, en particular, divide al producto de primos que forman la segunda descomposición; por lo tanto, divide a alguno de los factores; pero como ellos son todos primos positivos, necesariamente coincide con alguno de estos factores, es decir que:

$$p_{r+1} = p'_{j_0} \text{ para algún subíndice } j_0$$

Luego, si excluimos este factor, obtenemos un número natural que admite una factorización con exactamente *r* factores primos:

$$\prod_{i=1}^{r} p_i = \prod_{j=1, j \neq j_0}^{r'} p'_j \quad (*)$$

Por lo tanto, como consecuencia de la hipótesis inductiva, la descomposición de este número es única, salvo el orden de los factores; pero entonces lo mismo vale para *n*, dado que el factor que les falta a ambas descomposiciones $(*)$ es p_{r+1} que es igual a p'_{j_0}.

Corolario 2.7. *Todo número natural compuesto n es divisible por algún número primo estrictamente menor que n.*

Ejemplo. ¿Cómo obtener la descomposición en factores primos de un entero dado?

Por ejemplo, calculemos la factorización de 360; el procedimiento consiste en **dividir sucesivamente por los primos positivos, en orden, empezando por el 2, tantas veces como sea posible**, o sea:

$$\begin{aligned} 360 &= 2 \cdot 180 \\ &= 2 \cdot (2 \cdot 90) \\ &= 2 \cdot (2 \cdot (2 \cdot 45)) \\ &= 2^3 \cdot 45 \end{aligned}$$

Como 45 no es divisible por 2, dividimos este factor por 3 y finalmente por 5,

$$\begin{aligned} 360 &= 2^3 \cdot 45 \\ &= 2^3 \cdot (3 \cdot 15) \\ &= 2^3 \cdot 3^2 \cdot 5 \end{aligned}$$

Por lo tanto, la factorización prima buscada es $360 = 2^3 \cdot 3^2 \cdot 5$

Recordemos que éste era el método que usábamos en la primaria; la representación gráfica que ayuda a aplicarlo es la siguiente:

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

La columna de la derecha nuevamente nos da la factorización $360 = 2^3 \cdot 3^2 \cdot 5$

Calculemos la factorización prima de -2.142: empezamos dividiendo a 2.142, su valor absoluto, por 2 y obtenemos:

$$2.142 = 2 \cdot 1.071$$

Como 1.071 no es par, continuamos dividiendo a 1.071 por 3; obtenemos:

$$\begin{aligned} 2.142 &= 2 \cdot 1.071 \\ &= 2 \cdot 3 \cdot 357 \end{aligned}$$

Dividimos a 357 por 3 y obtenemos un cociente entero, lo cual nos dice que hay otro factor 3, o sea:

$$\begin{aligned} 2.142 = 2 \cdot 1.071 &= 2 \cdot 3 \cdot 357 \\ &= 2 \cdot 3 \cdot (3 \cdot 119) \\ &= 2 \cdot 3^2 \cdot 119 \end{aligned}$$

Dado que 119 no es divisible por 3, verificamos si lo es por el primo siguiente, el 5, vemos que no. Así siguiendo, efectuamos la división por 7 y obtenemos un cociente entero, que además es primo, $119 = 7 \cdot 17$; entonces el proceso termina:

$$\begin{aligned} 2.142 &= 2 \cdot 3^2 \cdot 119 \\ &= 2 \cdot 3^2 \cdot 7 \cdot 17 \end{aligned}$$

Por lo tanto:

$$-2.142 = (-1) \cdot 2 \cdot 3^2 \cdot 7 \cdot 17$$

Es decir que **la factorización prima de un entero negativo es la de su valor absoluto multiplicada por** -1, como vimos en la demostración del teorema.

Si n es grande, puede ser difícil hallar su factorización, en particular, si el primo más chico que lo divide es un número grande. Por ejemplo, la factorización prima de 1.442.897 es:

$$1.442.897 = 113^3$$

En este ejemplo, el primo más chico que divide al número (y en realidad el único) es 113. Un ejemplo como éste requiere además la comprobación de que 113 es primo, que efectuaremos después.

Otro ejemplo que podemos considerar es n = 2.279.269, cuya factorización prima es:

$$2.279.269 = 127 \cdot 131 \cdot 137$$

Es decir, si empezamos a dividir por 2, por 3, por 5, por 7 ... etcétera, el proceso concluye en algún momento, pero es muy lento. Por otra parte, es necesario comprobar que estos tres factores son números primos.

Para comprobar que un número es primo, tenemos la siguiente herramienta:

Lema 2.8. *Un número natural n es compuesto si y sólo si existe un primo p que divide a n tal que* $1 < p \leq \sqrt{n}$.

Demostración. Sea n un número natural compuesto; dado que n no es primo, necesariamente admite algún divisor distinto de 1, -1, n y $-n$, digamos $d \in \mathbb{N}$. En particular, $1 < d < n$. Es decir que existen $d, q \in \mathbb{Z}$ que verifican:

$$n = d \cdot q \quad \text{y} \quad 1 < d, q < n$$

En efecto, si q fuera mayor o igual que n, el producto $d \cdot q$ sería mayor que n, porque $d > 1$; y si fuera $q = 1$, debería ser $d = n$, contradiciendo la elección de d.

Más aún, en realidad $d \leq \sqrt{n}$ o $q \leq \sqrt{n}$; en efecto, si ocurriera que ambos $d > \sqrt{n}$ y $q > \sqrt{n}$, obtendríamos:

$$d \cdot q > \sqrt{n} \cdot \sqrt{n} = n.$$

o sea, $d \cdot q > n$, hecho que contradice la igualdad $d \cdot q = n$ con la que empezamos.

Supongamos entonces que $d \leq \sqrt{n}$. Si d es primo, hemos terminado la demostración. Si no, se desprende del teorema fundamental que d, y por lo tanto n, admite un divisor primo, claramente menor que $\sqrt{n}$.

Recíprocamente, si existe un primo p que divide a n tal que $1 < p \leq \sqrt{n}$. entonces, como $\sqrt{n} < n$, obtenemos $p < n$, es decir que p es un primo que divide a n y no es igual a n; por lo tanto, n no es primo.

Ejemplo. Los números 109, 113, 127, 131 y 137 son primos. En efecto, dado que $13^2 = 169$, que es mayor que todos los anteriores, según el lema anterior es suficiente comprobar que no son divisibles por ningún primo positivo menor o igual que 11, es decir, que no son divisibles por 2, 3, 5, 7 ni 11.

Ejemplo. Comprobar que los siguientes números son primos: 1.009, 1.013, 1.021, 1.031, 1.033, 1.039, 1.049, 1.051. Probar que, en efecto, los anteriores no son divisibles por ningún primo menor o igual que 31, que es el máximo primo menor o igual que la raíz cuadrada de 1.051.

También 5.003 y 5.009 son primos, porque no son divisibles por ningún primo menor o igual que su raíz cuadrada. En efecto, no son divisibles por ningún primo menor que 71 y $71^2 = 5.041 > 5.009$.

Teorema 2.9. *Existen infinitos primos.*

Demostración. Vamos a comprobar que existen infinitos primos positivos. Supongamos que la afirmación no sea verdadera, sino que existan sólo una cantidad finita de primos positivos, digamos $p_1, p_2, \ldots, p_n$.

Consideremos el número entero $c = 1+p_1 \cdot p_2 \cdot \ldots \cdot p_n$, es decir, c es el *producto de todos los primos positivos más uno*. Notar que $c \neq 0, 1, -1$, porque, dado que el primo positivo más chico es 2, tenemos que $c \geq 1 + 2 = 3$. La afirmación es que c no es divisible por ningún primo positivo. En efecto, si algún primo dividiera a c, este primo debería ser alguno de los $p_1, p_2, \ldots, p_n$. Supongamos que p_1 divida a c; por otra parte es claro que p_1 divide al producto de todos los primos (pues p_1 es uno de los factores de este producto), es decir que:

$$p_1 \mid c \text{ y también } p_1 \mid p_1 \cdots p_n$$

Pero entonces p_1 dividiría a la diferencia de estos dos números, a saber, $c - p_1 \ldots p_n = 1$, ó sea que p_1 dividiría a 1; esto sería una contradicción con el hecho de que p_1 sea un número primo.

Pero entonces $c \neq 0, 1, -1$ es un entero no divisible por ningún primo, lo cual contradice el teorema fundamental; esta contradicción provino de haber negado el enunciado; por lo tanto, existen infinitos primos.

Ejemplo. Encontrar el menor número natural n tal que $2.200 \cdot n$ sea un cuadrado.

Solución. Como en numerosos ejemplos más, la herramienta esencial para este cálculo es el teorema fundamental.

Pensemos qué exponentes aparecen en la descomposición de un número natural mayor que 1 que es el cuadrado de algún otro, digamos k^2. Si escribimos en general $k = p_1 \ldots p_r$ como producto de primos y lo elevamos al cuadrado, obtenemos:

$$\begin{aligned} k^2 &= (p_1 \cdots p_r)^2 \\ &= p_1^2 \cdots p_r^2 \end{aligned}$$

Es decir que en la factorización en primos de un natural al cuadrado, los factores primos aparecen todos al cuadrado. Por ejemplo:

$$\begin{aligned} 50^2 &= (2 \cdot 5^2)^2 \\ &= (2 \cdot 5 \cdot 5)^2 \\ &= 2^2 \cdot 5^2 \cdot 5^2 \\ &= 2^2 \cdot (5^2)^2 \end{aligned}$$

El 5 ya estaba dos veces en el 50 y al elevarlo al cuadrado, aparece cuatro veces. Es decir que **en un cuadrado, todos los factores primos distintos deben estar una cantidad par de veces.**

Volviendo a nuestro problema, efectuemos la factorización de 2.200:

$$\begin{array}{r|l} 2.200 & 2 \\ 1.100 & 2 \\ 550 & 2 \\ 275 & 5 \\ 55 & 5 \\ 11 & 11 \\ 1 & \end{array}$$

Entonces:

$$2.200 = 2^3 \cdot 5^2 \cdot 11$$

Ahora pensemos en la condición de que 2.200 n sea un cuadrado, o sea, necesitamos que sea de la forma k^2 para algún $k \in \mathbb{N}$ que por el momento desconocemos.

¿Qué factores necesitamos agregarle a 2.200 para que todos los primos aparezcan elevados a un exponente par? Como el 2 está tres veces, necesitamos un 2 más; el 5 ya está una cantidad par de veces, así que no hacen falta más factores iguales a 5, el 11 está una vez, así que necesitamos al menos un 11 más. Es decir que si a 2.200 le agregamos estos dos factores cuyo producto llamamos n, o sea, $n = 2 \cdot 11$, tenemos:

$$\begin{aligned} 2.200 \cdot n &= (2^3 \cdot 5^2 \cdot 11) \cdot (2 \cdot 11) \\ &= 2^4 \cdot 5^2 \cdot 11^2 \\ &= (2^2 \cdot 5 \cdot 11)^2 \end{aligned}$$

que ya tiene la forma de un k^2, justamente, con $k = 2^2 \cdot 5 \cdot 11$. Por lo tanto, el n que buscábamos es el que construimos con los factores que agregamos, $n = 2 \cdot 11$.

6.1. El máximo común divisor a partir de la factorización prima

Una de las consecuencias del Teorema 2.6 es que podemos escribir el máximo común divisor d de dos números en términos de los primos que dividen a los números. La idea es que todo divisor primo de ambos números necesariamente también divide a d, es decir, que aparece en la factorización en primos de d y, recíprocamente, todo primo que aparece en la factorización de d debe dividir a los dos números, por propiedad del máximo común divisor.

Por ejemplo: $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ y $50 = 2 \cdot 5^2$

Observemos que 2 y 5 aparecen en la factorización tanto de 630 como de 50; por lo tanto, $10 = 2 \cdot 5$ divide a ambos números; más aún, 2 y 5 son los únicos primos que aparecen en la factorización de los dos enteros, 630 y 50. Por otro lado, recordemos que ya hemos calculado en un ejemplo anterior que:

$$\begin{aligned} mcd\,(630\ ,\ 50) &= 10 \\ &= 2 \cdot 5 \end{aligned}$$

Ejemplo. Estudiemos otro ejemplo: calcular d, el máximo común divisor de 252 y 360, a partir de sus descomposiciones primas.

Efectuemos las factorizaciones:

$$252 = 2^2 \cdot 3^2 \cdot 7 \quad \text{y} \quad 360 = 2^3 \cdot 3^2 \cdot 5$$

entonces 2 y 3 dividen a ambos números. Notar que, en realidad, 2^2 y 3^2 dividen a ambos, dado que aparecen en sus descomposiciones; no así 2^3, que está sólo en la factorización de 360 pero no en la de 252. Por lo tanto:

$$2^2 \cdot 3^2 \text{ divide a } d$$

Es decir que, dado que el 2 aparece en la descomposición prima de 252 con exponente 2, y el 2 aparece en la descomposición prima de 360 con exponente 3, el 2 aparece en la descomposición prima de d con exponente 2, que es el exponente más chico de los dos. Análogamente, 3^2 aparece en la factorización en primos de d. Más aún:

$$d = 2^2 \cdot 3^2 = 36$$

de lo contrario, debería haber algún otro primo que divida a d, pero como d divide a 252 y 360, un primo tal también dividiría a 252 y 360; pero ya vimos que los únicos primos que los dividen a ambos son 2 y 3 y vimos también cuál es la máxima potencia de cada uno de estos primos, que divide tanto a 252 como a 360.

Obtuvimos que:
el máximo común divisor es el producto de los primos comunes elevados a su menor exponente.

6.2. El mínimo común múltiplo

Para lograr un rendimiento óptimo, la fábrica X recomienda a los propietarios de sus autos cambiar el aceite cada 6.000 *km y el líquido refrigerante cada* 8.000 *km. ¿Cuál es la cantidad mínima de km al cabo de la cual hay que renovar los dos líquidos a la vez?*

La respuesta a esta pregunta es una cantidad n de km tal que coincida el cambio de aceite con el de líquido refrigerante; es decir que, en *miles de km*, n debe ser 6 ó 12 ó 18, etcétera para que toque hacer un cambio de aceite y, por otra parte, n debe ser 8 ó 16 ó 24, etcétera para que sea necesario efectuar un cambio de refrigerante. Es decir que:

n debe ser a la vez múltiplo de 6 y de 8.

¿Cuál es el natural que más fácilmente cumple esta condición? Seguramente 48, que es igual a 6 por 8, es el primer ejemplo que nos viene a la mente; claramente es un múltiplo tanto de 6 como de 8, pero no necesariamente es el más chico entre todos los múltiplos comunes.

En otras palabras, n debe ser *a la vez múltiplo de* 6 *y de* 8 y, entre todos los múltiplos de 6 y de 8, nos interesa *el mínimo.* Si pensamos cuidadosamente, nos damos cuenta de que el mínimo natural que satisface estas condiciones es $n = 24$, en unidades de miles de km. La respuesta es que cada 24.000 km corresponde renovar los dos líquidos para optimizar el rendimiento. Decimos que 24 *es el mínimo común múltiplo de* 6 *y* 8 y denotamos:

$$[6 : 8] = 24$$

Consideremos otro ejemplo. *En el campeonato interescolar, el equipo de voley femenino de la escuela tiene un partido cada* 10 *días y el de varones, cada* 12 *días. Si ambos equipos inauguran el campeonato jugando el mismo día, ¿cuántos días más tarde vuelven a coincidir?*

La respuesta es una cantidad m de días, a partir de la fecha inaugural, tal que les toque jugar a la vez a las chicas y a los varones; o sea que m debe ser a la vez múltiplo de 10 y múltiplo de 12. En otras palabras, m debe pertenecer al conjunto de los múltiplos de 10:

$$\mathcal{M}_{10} = \{10,\ 20,\ 30,\ 40,\ 50,\ \mathbf{60},\ 70,\ 80,\ 90,\ 100,\ 110\ldots\}$$

y a la vez al de los múltiplos de 12 que es

$$\mathcal{M}_{12} = \{12,\ 24,\ 36,\ 48,\ \mathbf{60},\ 72,\ 84\ldots\}$$

Si observamos los dos conjuntos, descubrimos que el número 60 está en ambos, y es el mínimo natural que es múltiplo de 10 y de 12 a la vez; es decir que *el mínimo común múltiplo de* 10 *y* 12 *es* 60 y escribimos:

$$[10 : 12] = 60$$

Dados enteros a y b, un número natural m se dice el *mínimo común múltiplo* de a y b si cumple las siguientes propiedades:

1) $a \mid m$ y $b \mid m$.
2) Si m' es otro entero tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

En otras palabras, el mínimo común múltiplo de a y b es el múltiplo positivo más chico de a y b. Lo denotamos por:

$$m = [a : b]$$

Teniendo a la vista los conjuntos de múltiplos de uno y otro número, es fácil deducir cuánto vale el mínimo común múltiplo entre ellos; pero en realidad, hay otras formas de calcularlo. Una muy eficiente se deduce del siguiente enunciado, donde debemos recordar la notación $(a : b)$ para el máximo común divisor de a y b.

Proposición 2.10. *Sean a y b números naturales, entonces el producto de a y b es igual al producto de su máximo común divisor y su mínimo común múltiplo. En símbolos, esta igualdad se expresa como:*

$$a \cdot b = (a : b) \cdot [a : b]$$

En el ejemplo previo para $a = 10$ y $b = 12$, estos números son:

$$(10 : 12) = 2 \quad \text{y} \quad [10 : 12] = 60$$

entonces la igualdad se expresa como:

$$\begin{aligned} 120 &= 10 \cdot 12 \\ &= 2 \cdot 60 \end{aligned}$$

Dados a y b, si lo que buscamos es el mínimo común múltiplo, se puede utilizar la igualdad anterior para despejarlo como el cociente entre el producto de a por b y su máximo común divisor. Es decir que, como consecuencia de la identidad anterior, tenemos que:

$$\begin{aligned} [10 : 12] &= \frac{10 \cdot 12}{(10 : 12)} \\ &= \frac{120}{2} \\ &= 60 \end{aligned}$$

Corolario 2.11. *Sean a y b números naturales, entonces el mínimo común múltiplo de a y b es igual al cociente entre el producto de a y b y su máximo común divisor. En símbolos, esta igualdad se expresa como:*

$$[a : b] = \frac{a \cdot b}{(a : b)}.$$

Si alguno de los dos números es negativo, el producto de ellos es negativo también. La relación anterior vale si corregimos el signo, es decir:

$$\text{si } a < 0 < b \quad \text{o} \quad b < 0 < a, \quad [a : b] = \frac{-a \cdot b}{(a : b)}$$

Recordemos que tanto $[a : b]$ como $(a : b)$ son naturales, cualesquiera sean los signos de a y b. Si tanto a como b son negativos, la igualdad vale sin cambiar signos.

Observación. En el caso en que a y b sean coprimos, $(a : b) = 1$, la igualdad anterior implica que $[a : b] = a \cdot b$, es decir que en este caso, el mínimo común múltiplo de a y b es igual al producto de a por b.

Por ejemplo, los múltiplos positivos de $a = 3$ son:

$$\mathcal{M}_3 = \{3,\ 6,\ 9,\ \mathbf{12},\ 15,\ 18,\ 21,\ \mathbf{24},\ 27,\ 30,\ 33,\ \mathbf{36},\ 39 \dots\}$$

y los múltiplos positivos de $b = 4$ son:

$$\mathcal{M}_4 = \{4,\ 8,\ \mathbf{12},\ 16,\ 20,\ \mathbf{24},\ 28,\ 32,\ \mathbf{36},\ 40 \dots\}$$

Entonces, el mínimo común múltiplo es:

$$\begin{aligned} [3 : 4] &= 12 \\ &= a \cdot b. \end{aligned}$$

Notar que hay infinitos múltiplos comunes de 3 y 4, que son todos múltiplos de 12, el mínimo común múltiplo.

Ejemplo. Los enteros $a = 275$ y $b = 327$ son coprimos; en efecto:

$$a = 275 \quad \text{y} \quad b = 327$$
$$= 5^2 \cdot 11 \qquad = 3 \cdot 109$$

no tienen primos comunes en sus descomposiciones; por lo tanto, su máximo común divisor es (275 : 327) = 1 y su mínimo común múltiplo es el producto de los dos números:

$$[a : b] = 275 \cdot 327$$
$$= 3 \cdot 5^2 \cdot 11 \cdot 109.$$

Como ya vimos en un ejemplo anterior, 109 es primo.

A partir de la factorización prima de los enteros *a* y *b*, es fácil obtener el mínimo común múltiplo. En efecto, si *a* = 10 y *b* = 12,

$$10 = 2 \cdot 5 \quad \text{y} \quad 12 = 2^2 \cdot 3$$

Notar que el 2 aparece en *a* = 10 y en *b* = 12, pero en el 12 el exponente es igual a 2, mientras que en el 10 el exponente es 1. Por otra parte, el 3 y el 5 no son primos comunes. Comparemos estas factorizaciones con la del mínimo común múltiplo de *a* y *b*:

$$[a : b] = 60 = 2^2 \cdot 3 \cdot 5$$

Observamos que en 60 aparecen todos los primos, tanto los de *a* como los de *b*, y el 2, que es común a *a* y a *b*, está elevado al cuadrado, que es el exponente máximo con el que aparece en *a* y en *b*. Este hecho vale en general:

El mínimo común múltiplo es el producto de los primos comunes y no comunes elevados a su mayor exponente.

Ejemplo. Hallar todos los pares de naturales *a* y *b* tales que su mínimo común múltiplo sea igual a 60 y su máximo común divisor sea igual a 15.

Solución: sabemos que si *a* y *b* son los números buscados:

$$15 \mid a, \quad 15 \mid b, \quad a \mid 60 \quad \text{y} \quad b \mid 60$$

Es decir que, en particular, *a* y *b* pertenecen al conjunto de los divisores positivos de 60 = $2^2 \cdot 3 \cdot 5$, que son:

$$\mathcal{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

Además, nos interesan sólo los que a la vez son múltiplos de 15, es decir que nuestros candidatos para *a* y *b* son:

$$15, \ 30 \ \text{y} \ 60$$

Entre ellos, hay que elegir los pares *a, b* tales que (*a* : *b*) = 15 y [*a* : *b*] = 60; esto implica que uno de ellos debe ser impar, y el otro debe ser divisible por 4. Luego las soluciones son:

$$a = 15 \text{ y } b = 60 \quad \text{o} \quad a = 60 \text{ y } b = 15$$

Ejemplo. Determinar todos los naturales n tales que el mínimo común múltiplo de n y 130 sea igual a 260.

Solución: Sea n un número que cumple la condición, entonces:

$$\begin{aligned}[n : 130] &= 260 \\ &= 2^2 \cdot 5 \cdot 13\end{aligned}$$

Por definición de mínimo común múltiplo, n divide a $260 = 2^2 \cdot 5 \cdot 13$, luego en la factorización en primos de n solo pueden aparecer los primos 2, 5 y 13 y elevados a potencias que son a lo sumo las que aparecen en 260. Por lo tanto, n es de la forma:

$$n = 2^r \cdot 5^s \cdot 13^t \quad \text{con } 0 \le r \le 2,\ 0 \le s \le 1,\ 0 \le t \le 1$$

Notar que 2^2 es la máxima potencia de 2 que divide a $260 = [n : 130]$, mientras que la máxima potencia de 2 que divide a 130 es 2^1; en consecuencia, 2^2 debe aparecer en n. Por lo tanto, r, el exponente de 2 en n, debe ser 2, es decir:

$$n = 2^2 \cdot 5^s \cdot 13^t \quad \text{con } 0 \le s \le 1 \text{ y } 0 \le t \le 1$$

Analicemos caso por caso:

1. si $s = 0$ y $t = 0$, entonces $n = 2^2 = 4$, que cumple $[n : 130] = [4 : 130] = 260$;
2. si $s = 0$ y $t = 1$, entonces $n = 2^2 \cdot 13 = 52$, que cumple $[n : 130] = [52 : 130] = 260$;
3. si $s = 1$ y $t = 0$, entonces $n = 2^2 \cdot 5 = 20$, que cumple $[n : 130] = [20 : 130] = 260$;
4. si $s = 1$ y $t = 1$, entonces $n = 2^2 \cdot 5 \cdot 13 = 260$, que cumple $[n : 130] = [260 : 130] = 260$;

por lo tanto, los n que verifican $[n : 130] = 260$ son $n = 4$, $n = 20$, $n = 52$ y $n = 260$.

Ejemplo. Hallar todos los pares de naturales a y b tales que su máximo común divisor sea igual a 10 y su mínimo común múltiplo sea igual a 1.500.

Solución: Sabemos que si a y b son los números buscados, entonces:

$$a \cdot b = (a : b) \cdot [a : b] = 10 \cdot 1.500 = 15.000$$

Como además $15.000 = 3 \cdot 5 \cdot 10^3 = 3 \cdot 5 \cdot (2 \cdot 5)^3 = 2^3 \cdot 3 \cdot 5^4$ es la factorización en primos del producto de a por b, tenemos que a y b deben tener en sus descomposiciones a estos y solo a estos primos, y en el producto de a y b los exponentes de 2, 3 y 5 deben ser los de la descomposición de 15.000, o sea:

$$a = 2^r \cdot 3^s \cdot 5^t \quad \text{y} \quad b = 2^{3-r} \cdot 3^{1-s} \cdot 5^{4-t} \quad \text{con } 0 \le r \le 3,\ 0 \le s \le 1,\ 0 \le t \le 4$$

Sólo nos queda averiguar las restricciones para los exponentes de estos primos en las factorizaciones de a y de b.

El hecho de que $(a : b) = 10$ implica que los primos 2 y 5 deben aparecer como mínimo una vez en a y en b, pero no pueden estar elevados al cuadrado o a potencias mayores en ambos. Notar que si $t = 2$, tanto en a como en b, el 5 aparecería elevado al cuadrado. Por lo tanto, las posibilidades para los exponentes son:

$$1 \leq r \leq 2, \quad 0 \leq s \leq 1, \quad 1 \leq t \leq 3, \ t \neq 2$$

Analicemos caso por caso:

1. si $r = 1$ y $s = 0$, $t = 1$ entonces $a = 2 \cdot 5 = 10$ y $b = 2^2 \cdot 3 \cdot 5^3 = 1.500$;
2. si $r = 1$ y $s = 1$, $t = 1$ entonces $a = 2 \cdot 3 \cdot 5 = 30$ y $b = 2^2 \cdot 5^3 = 500$;
3. si $r = 1$ y $s = 0$, $t = 3$ entonces $a = 2 \cdot 5^3 = 250$ y $b = 2^2 \cdot 3 \cdot 5^3 = 60$;
4. si $r = 1$ y $s = 1$, $t = 3$ entonces $a = 2 \cdot 3 \cdot 5^3 = 750$ y $b = 2^2 \cdot 5^3 = 20$;

y los pares obtenidos en estos cuatro casos cumplen que $(a : b) = 10$ y $[a : b] = 1.500$.

Los casos restantes coinciden con los anteriores, intercambiando el orden de a y b. Por lo tanto, los pares (a, b), soluciones a nuestro problema, son:

$$(10, 1.500), \ (20, \ 750), \ (30, \ 500), \ (60, \ 250)$$

3. Aritmética modular

□ 1. Ecuaciones diofánticas

Los alumnos de la Escuela 314 hacen una colecta para reunir fondos para ayudar a una escuela de frontera. Para esto, ofrecen bonos contribución de dos tipos: bonos de $15 y bonos de $8.

Martín se lleva un piloncito de bonos de $15 y otro de bonos de $8. Después de vender varios bonos recaudó $100, pero no recuerda cuántos bonos vendió de cada clase (ni sabe cuántos bonos tenía cada uno de sus piloncitos al comienzo). ¿Puede Martín determinar cuántos bonos vendió de cada tipo?

Para tratar de determinar estas cantidades, Martín observa que:

- si no hubiera vendido ningún bono de $15, los $100 provendrían de vender bonos de $8; es decir, si vendió una cantidad y de bonos de $8 sería $100 = $8 · y, pero esto no puede ser porque 100 no es múltiplo de 8;
- si hubiera vendido un solo bono de $15, entonces los $100 - $15 = $85 restantes provendrían de vender bonos de $8, pero 85 tampoco es múltiplo de 8;
- si hubiera vendido 2 bonos de $15, los $100 - 2 · $15 = $70 restantes provendrían de vender bonos de $8, pero 70 no es múltiplo de 8;
- no puede ser que haya vendido 3 bonos de $15, porque $100 - 3·$15 = $55 y 55 tampoco es múltiplo de 8;
- es posible que haya vendido 4 bonos de $15, ya que $100 - 4 · $15 = $40 = 5 · $8. Esto significa que además habría vendido 5 bonos de $8;
- razonando de la misma manera deduce que no puede ser que haya vendido ni 5 ni 6 bonos de $15. Además, seguro que no vendió más de 7 de estos bonos, pues 7 · $15 = $105 y sólo recaudó $100.

Martín concluye entonces que los $100 fueron recaudados mediante la venta de 4 bonos de $15 y 5 bonos de $8.

Podemos plantear el problema de Martín mediante una igualdad de números enteros: si Martín vendió x bonos de $15 e y bonos de $8, entonces la cantidad de dinero que recaudó es:

$$15 \cdot x + 8 \cdot y = 100$$

Esto es, las cantidades de bonos de cada tipo $x, y \in \mathbb{N}_0$ que puede haber vendido Martín son las soluciones en los números enteros no negativos para esta ecuación. A continuación vamos a ver cómo es posible resolver este tipo de ecuaciones sistemáticamente.

Más precisamente, *dados a, b, c ∈ ℤ, con a y b no nulos, nos interesa hallar las soluciones en los números enteros de la ecuación:*

$$a \cdot x + b \cdot y = c \tag{2}$$

es decir, los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ para los cuales se cumple la igualdad.

Estas ecuaciones son una clase particular de las que se conocen como ecuaciones diofánticas[4], que son ecuaciones con coeficientes enteros de las que se buscan soluciones en el conjunto de los números enteros.

Una ecuación de este tipo no siempre tiene solución; por ejemplo, la ecuación $12 \cdot x + 14 \cdot y = 123$ no tiene solución, porque para todo par de números $x, y \in \mathbb{Z}$, el resultado de $12 \cdot x + 14 \cdot y$ es un entero par:

$$12 \cdot x + 14 \cdot y = 2 \cdot (6 \cdot x + 7 \cdot y)$$

mientras que 123 es impar.

De la misma manera que en el ejemplo, vemos que si $d \in \mathbb{Z}$ es un divisor común de a y b, tenemos que $d \mid a \cdot x + b \cdot y$ para cualesquiera $x, y \in \mathbb{Z}$. Entonces, si $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación (2), resulta que $d \mid c$. Esto nos dice que para que la ecuación (2) tenga soluciones es necesario que todo divisor común de a y b sea también divisor de c.

Esta última condición es a su vez equivalente a que $(a : b)$ divida a c. En efecto, si todo divisor común de a y b divide a c, en particular lo divide su máximo común divisor $(a : b)$. Recíprocamente, si $(a : b)$ divide a c, como cualquier divisor común de a y b divide a $(a : b)$, por la transitividad de la divisibilidad, también divide a c.

Concluimos que:

> Si $(a : b) \nmid c$, la ecuación $a \cdot x + b \cdot y = c$ no tiene soluciones en $\mathbb{Z}$.

Analicemos ahora en detalle un ejemplo en el que $(a : b) \mid c$.

Ejemplo. Consideremos la ecuación $50 \cdot x + 630 \cdot y = 10$. Como vimos en la sección 5 del capítulo 2, esta ecuación tiene solución, ya que $10 = (50 : 630)$ es combinación lineal entera de 50 y 630:

$$50 \cdot (-25) + 630 \cdot 2 = 10$$

es decir $(x, y) = (-25, 2)$ es una solución.

A partir de esta solución podemos ver, por ejemplo, que la ecuación $50 \cdot x + 630 \cdot y = 20$ también tiene solución. Para obtener como resultado el doble de 10, basta duplicar los valores de x e y (o lo que es lo mismo, multiplicar por 2 la igualdad anterior):

$$50 \cdot (-25) \cdot 2 + 630 \cdot 2 \cdot 2 = 10 \cdot 2$$

[4] El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra Aritmética.

o sea, que $(x, y) = ((-25) \cdot 2, 2 \cdot 2) = (-50, 4)$ es solución de esta nueva ecuación. De la misma manera, para cualquier $q \in \mathbb{Z}$ resulta que la ecuación $50 \cdot x + 630 \cdot y = 10 \cdot q$ tiene como solución a $(x, y) = (-25 \cdot q, 2 \cdot q)$, ya que:

$$50 \cdot (-25) \cdot q + 630 \cdot 2 \cdot q = 10 \cdot q$$

En general, sabemos que para cualesquiera $a, b \in \mathbb{Z}$ no simultáneamente nulos, $(a : b)$ es combinación lineal entera de a y b, es decir, existen números enteros s y t tales que:

$$a \cdot s + b \cdot t = (a : b)$$

Esto nos dice que la ecuación $a \cdot x + b \cdot y = (a : b)$ siempre tiene solución. Más aún, a partir de la igualdad de arriba vemos que, si $c = (a : b) \cdot q$, la ecuación (2) tiene como una solución a $(x, y) = (s \cdot q, t \cdot q)$, ya que:

$$a \cdot \underbrace{s \cdot q}_{x} + b \cdot \underbrace{t \cdot q}_{y} = (a \cdot s + b \cdot t) \cdot q = (a : b) \cdot q$$

Tenemos entonces también que:

> Si $(a : b) \mid c$, la ecuación $a \,.\, x + b \,.\, y = c$ tiene soluciones en $\mathbb{Z}$.

Resumiendo, hemos probado la siguiente proposición:

Proposición 3.1. *Sean $a, b, c \in \mathbb{Z}$ con a y b no nulos. La ecuación diofántica $a \cdot x + b \cdot y = c$ tiene soluciones en $\mathbb{Z}$ si y solo si $(a : b)$ divide a c.*

Veamos cómo son **todas** las soluciones de (2) cuando $(a : b)$ divide a c. En primer lugar, podemos dividir ambos miembros de (2) por $(a : b)$, obteniendo la nueva ecuación:

$$\frac{a}{(a : b)} \cdot x + \frac{b}{(a : b)} \cdot y = \frac{c}{(a : b)}$$

Esta ecuación tiene las mismas soluciones en $\mathbb{Z} \times \mathbb{Z}$ que la original (se puede pasar de una ecuación a la otra simplemente multiplicando o dividiendo por $(a : b)$). Si llamamos $\alpha = \frac{a}{(a:b)}$, $\beta = \frac{b}{(a:b)}$ y $\gamma = \frac{c}{(a:b)}$, que son enteros, nos queda la ecuación:

$$\alpha \cdot x + \beta \cdot y = \gamma$$

donde ahora $(\alpha : \beta) = 1$ (observar que α y β son coprimos porque hemos suprimido todos los factores comunes de a y b). Supongamos que (x_0, y_0) es una solución de esta ecuación. Si (x, y) es otra solución, vale que $\alpha \cdot x + \beta \cdot y = \gamma = \alpha \cdot x_0 + \beta \cdot y_0$; entonces:

$$\alpha \cdot (x - x_0) = -\beta \cdot (y - y_0)$$

De esta igualdad deducimos que $\beta \mid \alpha \cdot (x - x_0)$ y, como $(\alpha : \beta) = 1$, entonces $\beta \mid x - x_0$ (ver la Proposición 2.4 del capítulo 2); luego, existe $k \in \mathbb{Z}$ tal que $x - x_0 = k \cdot \beta$. Reemplazando en la igualdad de arriba, nos queda que $\alpha \cdot k \cdot \beta = -\beta \cdot (y - y_0)$, de donde se desprende que $y - y_0 = -\alpha \cdot k$. En conclusión, toda solución (x, y) de la ecuación diofántica considerada es

de la forma $x = x_0 + k \cdot \beta$, $y = y_0 - k \cdot \alpha$, con $k \in \mathbb{Z}$.

Teorema 3.2. *Sean $a, b, c \in \mathbb{Z}$, con a y b no nulos. Si $(a : b) \mid c$, entonces las soluciones de la ecuación diofántica $a \cdot x + b \cdot y = c$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tales que*

$$x = x_0 + k \cdot \frac{b}{(a : b)}, \quad y = y_0 - k \cdot \frac{a}{(a : b)}, \quad \text{con } k \in \mathbb{Z}$$

donde (x_0, y_0) es una solución particular de la ecuación.

Ejemplo. Volvamos al problema planteado al comienzo de esta sección: Martín vendió x bonos de \$15 e y bonos de \$8, y busca determinar los valores de x e y sabiendo que recaudó \$100, es decir, que:

$$15 \cdot x + 8 \cdot y = 100$$

Como $(15 : 8) = 1$, sabemos que la ecuación tiene soluciones. Comenzaremos buscando todas las soluciones en $\mathbb{Z} \times \mathbb{Z}$, y luego determinaremos las soluciones en $\mathbb{N}_0 \times \mathbb{N}_0$, que son las que le interesan a Martín.

En primer lugar, escribimos $1 = (15 : 8)$ como combinación lineal entera de 15 y 8. Para esto, utilizamos la información dada por el algoritmo de Euclides:

$$\begin{array}{rcl@{\qquad}rcl} 15 &=& 1 \cdot 8 + 7 & \longrightarrow & 7 &=& 15 - 1 \cdot 8 \\ 8 &=& 1 \cdot 7 + 1 & \longrightarrow & 1 &=& 8 - 1 \cdot 7 \\ 7 &=& 7 \cdot 1 & & &=& 8 - 1 \cdot (15 - 1 \cdot 8) \\ & & & & &=& 15 \cdot (-1) + 8 \cdot 2 \end{array}$$

Ahora tomamos la identidad obtenida:

$$15 \cdot (-1) + 8 \cdot 2 = 1$$

y la multiplicamos por 100 para conseguir una solución de la ecuación original:

$$\begin{aligned} 15 \cdot (-1) \cdot 100 + 8 \cdot 2 \cdot 100 &= 100 \\ 15 \cdot (-100) + 8 \cdot 200 &= 100 \end{aligned}$$

Tenemos así una solución particular de la ecuación: $(x_0, y_0) = (-100, 200)$.

Por el Teorema 3.2, todas las soluciones enteras de la ecuación $15 \cdot x + 8 \cdot y = 100$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ donde:

$$x = -100 + k \cdot 8, \quad y = 200 - k \cdot 15, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, nos interesan aquellas soluciones en las cuales $x \geq 0$ e $y \geq 0$:

$$\begin{aligned} x \geq 0 &\iff -100 + k \cdot 8 \geq 0 \iff k \cdot 8 \geq 100 \iff k \geq 13 \quad (\text{porque } k \in \mathbb{Z}) \\ y \geq 0 &\iff 200 - k \cdot 15 \geq 0 \iff 200 \geq k \cdot 15 \iff 13 \geq k \quad (\text{porque } k \in \mathbb{Z}) \end{aligned}$$

De estas desigualdades deducimos que la única solución $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ se obtiene para $k = 13$:

$$x = -100 + 13 \cdot 8\,, \qquad y = 200 - 13 \cdot 15$$
$$= 4 \qquad\qquad = 5$$

con lo cual, si recaudó $100, Martín tiene que haber vendido 4 bonos de $15 y 5 bonos de $8.

Ejercicio 3.1. Hallar todas las soluciones enteras de la ecuación $84 \cdot x + 270 \cdot y = 66$

□ 2. Congruencias

En esta sección vamos a presentar una noción de congruencia[5] en el conjunto $\mathbb{Z}$, que resulta muy útil a la hora de trabajar con propiedades de divisibilidad sobre los números enteros.

Dado $m \in \mathbb{N}$, decimos que $a, b \in \mathbb{N}$ son *congruentes módulo m*, y escribimos $a \equiv b \pmod{m}$ o simplemente $a \equiv_{(m)} b$, si $m \mid a - b$. Si a y b no son congruentes módulo m, escribimos $a \not\equiv b \pmod{m}$.

Por ejemplo,

- $11 \equiv 5 \pmod 3$, pues $3 \mid 11 - 5 = 6$,
- $11 \not\equiv -2 \pmod 4$, pues $4 \nmid 11 - (-2) = 13$,
- $a \equiv b \pmod 1$ para cualesquiera $a, b \in \mathbb{Z}$, ya que todo número entero es múltiplo de 1.

Observemos que, cualquiera sea $m \in \mathbb{N}$, tenemos que:

$$a \equiv 0 \pmod m \iff m \mid a.$$

Antes de continuar, analicemos más en detalle el caso $m = 2$.

Tenemos que $a \equiv b \pmod 2$ si y sólo si $2 \mid a - b$. Si a es par, entonces $a = 2 \cdot \alpha$ para algún $\alpha \in \mathbb{Z}$, con lo cual $a - b = 2 \cdot \alpha - b$ es múltiplo de 2 si y sólo si b lo es, o sea, si y sólo si b es par. De la misma manera, si a es impar vemos que $2 \mid a - b$ si y sólo si b también es impar. En otras palabras:

$$a \equiv b \pmod 2 \iff a \text{ y } b \text{ son ambos pares o ambos impares.}$$

Esto nos dice que la congruencia módulo 2 *parte* al conjunto de los números enteros en dos subconjuntos: el de los enteros pares y el de los enteros impares. En cada uno de estos subconjuntos, dos elementos cualesquiera están relacionados, y un elemento de uno de estos conjuntos no está relacionado con uno del otro (es decir, un entero par es congruente a todo entero par y no es congruente a ningún impar, y un entero impar es congruente a cualquier impar, pero a ningún par). Podemos formalizar esto, mediante el concepto de relación de equivalencia.

Para $m \in \mathbb{N}$ fijo, consideremos la relación $\mathcal{R}$ en $\mathbb{Z}$ definida por

$$a \mathcal{R} b \iff a \equiv b \pmod m$$

[5] Esta noción fue introducida por Carl Friedrich Gauss en su libro Disquisitiones Arithmeticae publicado en 1801.

Esta relación satisface:

i) $\mathcal{R}$ es reflexiva: $a \equiv a$ (mód m) para todo $a \in \mathbb{Z}$, ya que $m \mid a - a = 0$.
ii) $\mathcal{R}$ es simétrica: si $a \equiv b$ (mód m), entonces $m \mid a - b = -(b - a)$, con lo que también vale que $m \mid b - a$, es decir, que $b \equiv a$ (mód m).
iii) $\mathcal{R}$ es transitiva: si $a\mathcal{R}b$ y $b\mathcal{R}c$, es porque $m \mid a - b$ y $m \mid b - c$; pero entonces $m \mid (a - b) + (b - c) = a - c$, lo que dice que $a \equiv c$ (mód m).

Por lo tanto, $\mathcal{R}$ es una relación de equivalencia. Como vimos en la sección 3 del capítulo 0, $\mathcal{R}$ nos da una partición del conjunto $\mathbb{Z}$ en subconjuntos disjuntos – las clases de equivalencia– tales que, dentro de cada uno de ellos, dos elementos cualesquiera están relacionados (en nuestro caso, son congruentes módulo m) y dos elementos de subconjuntos distintos no están relacionados.

Como vimos anteriormente, para $m = 2$ la relación de congruencia parte al conjunto $\mathbb{Z}$ en 2 subconjuntos, $\{a \in \mathbb{Z} \mid a \text{ es par}\}$ y $\{a \in \mathbb{Z} \mid a \text{ es impar}\}$. El primero de ellos es la clase de equivalencia [0] y el segundo, es la clase de equivalencia [1]. En el caso general, fijado $m \in \mathbb{N}$, la relación de congruencia módulo m parte al conjunto de los números enteros en m clases de equivalencia. La siguiente propiedad de la congruencia nos dice cómo son estas m clases.

Proposición 3.3. *Sea $m \in \mathbb{N}$. Para cada $a \in \mathbb{Z}$, si r es el resto de la división de a por m, vale $a \equiv r$ (mód m). Más aún, este resto es el único entero r tal que $0 \leq r < m$ que es congruente con a módulo m.*

Demostración. Si r es el resto de la división de a por m, existe un entero q tal que $a = m \cdot q + r$. Entonces $a - r = m \cdot q$, con lo que $m \mid a - r$ y, por lo tanto, $a \equiv r$ (mód m).

Por otro lado, si $a \equiv r$ (mód m), sabemos que $m \mid a - r$. Entonces existe $q \in \mathbb{Z}$ tal que $a - r = m \cdot q$; luego $a = m \cdot q + r$. Si vale $0 \leq r < m$, por la unicidad en el algoritmo de división, r es el resto de la división de a por m.

Como consecuencia de este resultado, fijado $m \in \mathbb{N}$, dos enteros distintos r_1 y r_2 con $0 \leq r_1, r_2 < m$ no son congruentes módulo m, es decir, las clases de equivalencia $[r_1]$ y $[r_2]$ son distintas. Además, todo entero a resulta congruente a su resto r en la división por m, y entonces $a \in [r]$. Luego, el conjunto de los enteros se parte como sigue:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

Volveremos sobre esta propiedad importante de la congruencia en la sección 4.

Algunas propiedades fundamentales de la congruencia son las siguientes:

Propiedades 3.4. Sea $m \in \mathbb{N}$. Entonces:

1. si $a_1 \equiv b_1$ (mód m) *y* $a_2 \equiv b_2$ (mód m), entonces $a_1 + a_2 \equiv b_1 + b_2$ (mód m);
2. si $a \equiv b$ (mód m), entonces $c \cdot a \equiv c \cdot b$ (mód m) para todo $c \in \mathbb{Z}$;

3. si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;
4. si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$ para todo $k \in \mathbb{N}$;
5. si $c \cdot a \equiv c \cdot b \pmod{m}$ y $(c : m) = 1$, entonces $a \equiv b \pmod{m}$;
6. si $d \mid m$ y $a \equiv b \pmod{m}$, entonces $a \equiv b \pmod{d}$.

Demostración. Para demostrar estas propiedades se usan básicamente las propiedades de la divisibilidad vistas en el capítulo 2.

1. Por la definición de congruencia, tenemos que $m \mid a_1 - b_1$ y $m \mid a_2 - b_2$. Entonces, $m \mid (a_1 - b_1)+(a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$; luego, $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
2. Tenemos que $m \mid a - b$, entonces también $m \mid c \cdot (a - b) = c \cdot a - c \cdot b$, con lo que $c \cdot a \equiv c \cdot b \pmod{m}$.
3. Por la propiedad anterior, como $a_1 \equiv b_1 \pmod{m}$, multiplicando por a_2, resulta que $a_1 \cdot a_2 \equiv b_1 \cdot a_2 \pmod{m}$; análogamente, multiplicando por b_1 la congruencia $a_2 \equiv b_2 \pmod{m}$, obtenemos que $b_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ y finalmente, por la transitividad, concluimos que $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.
4. Se prueba por inducción aplicando la propiedad 3.
5. Por hipótesis, $m \mid c \cdot a - c \cdot b = c \cdot (a - b)$. Y como c y m son coprimos, por la Proposición 2.4 del capítulo 2, resulta que $m \mid a - b$, es decir, que $a \equiv b \pmod{m}$.
6. Como $d \mid m$ y $m \mid a - b$, la transitividad de la divisibilidad implica que $d \mid a - b$, o sea que $a \equiv b \pmod{d}$.

Ejemplo. Veamos, utilizando la noción de congruencia y sus propiedades, que si $a, b, c \in \mathbb{Z}$ son tales que $a^2 + b^2 = c^2$, entonces $3 \mid a$ o $3 \mid b$.

Si 3 no divide a a ni a b, entonces tanto a como b tienen resto 1 ó 2 en la división por 3. Ahora bien, $1^2 = 1 \equiv_{(3)} 1$ y $2^2 = 4 \equiv_{(3)} 1$. Entonces, por la propiedad 4 anterior, tenemos que $a^2 \equiv 1 \pmod{3}$ y $b^2 \equiv 1 \pmod{3}$; luego, por la propiedad 1,

$$\begin{aligned} a^2 + b^2 &\equiv 1 + 1 \pmod{3} \\ &\equiv 2 \pmod{3} \end{aligned}$$

Esto implica que $c \in \mathbb{Z}$ debería cumplir que:

$$c^2 \equiv 2 \pmod{3}$$

Pero esto no puede ocurrir, puesto que si $c \equiv 0 \pmod{3}$, entonces $c^2 \equiv 0 \pmod{3}$ y, al igual que antes, si $c \equiv 1$ ó $2 \pmod{3}$, entonces $c^2 \equiv 1 \pmod{3}$.

Ejemplo. Calcular la cifra de las unidades en el desarrollo decimal de 33^{666}.

Calculando las primeras potencias de 33:

$$\begin{aligned} 33^0 &= \underline{1} \\ 33^1 &= 3\underline{3} \\ 33^2 &= 1.08\underline{9} \\ 33^3 &= 35.93\underline{7} \\ 33^4 &= 1.185.92\underline{1} \\ 33^5 &= 39.135.39\underline{3} \\ \dots &\quad \dots \quad \dots \end{aligned}$$

vemos que las cifras de las unidades son 1, 3, 9, 7, 1, 3, ... Uno podría conjeturar que seguirá siempre así, repitiéndose la secuencia 1, 3, 9, 7 sucesivamente y, a partir de esto, tratar de determinar la cifra de las unidades pedidas.

Para formalizar esta idea utilizaremos congruencias. La observación fundamental es que si el desarrollo decimal de 33^{666} es $(n_s \ldots n_1 n_0)_{10}$, entonces:

$$\begin{aligned} 33^{666} &= n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0 \\ &= 10 \cdot (n_s \cdot 10^{s-1} + \cdots + n_1) + n_0 \quad \text{y} \quad 0 \leq n_0 < 10 \end{aligned}$$

de donde deducimos que la cifra n_0 de las unidades es el *resto del número en la división por 10*. Para hallarlo, aplicaremos el resultado visto en la Proposición 3.3, o sea, buscaremos el único entero n_0 con $0 \leq n_0 < 10$ tal que $33^{666} \equiv n_0 \pmod{10}$.

Según los cálculos hechos al comienzo:

$$33^4 \equiv 1 \pmod{10}$$

Entonces, por la propiedad 4 de las Propiedades 3.4, para todo $k \in \mathbb{N}$, vale:

$$(33^4)^k \equiv 1^k \pmod{10}, \quad \text{o sea,} \quad 33^{4 \cdot k} \equiv 1 \pmod{10}$$

Dividamos entonces al exponente 666 por 4: como $666 = 4 \cdot 166 + 2$, deducimos que:

$$\begin{aligned} 33^{666} &= 33^{4 \cdot 166 + 2} \\ &= 33^{4 \cdot 166} \cdot 33^2 \\ &\equiv_{(10)} 1 \cdot 9 \\ &= 9 \end{aligned}$$

donde la congruencia es consecuencia de la propiedad 3 de las Propiedades 3.4. En consecuencia, la cifra de las unidades en el desarrollo decimal de 33^{666} es 9.
Observemos que, aplicando estas mismas propiedades, podemos determinar la cifra de las unidades de 33^n para $n \in \mathbb{N}$ arbitrario: dado $n \in \mathbb{N}$, por el algoritmo de división, existen enteros k y r tales que $n = 4 \cdot k + r$ y $0 \leq r < 4$, con lo cual:

$$\begin{aligned} 33^n &= 33^{4 \cdot k + r} \\ &= \underbrace{33^{4 \cdot k}}_{\equiv_{(10)} 1} \cdot 33^r \\ &\equiv_{(10)} 33^r \end{aligned}$$

Concluimos entonces que la cifra de las unidades de 33^n coincide con la de 33^r, donde r es el resto de la división de n por 4; por lo tanto, de acuerdo a los cálculos hechos al comienzo, esta cifra es 1, 3, 9, 7 si $r = 0, 1, 2, 3$ respectivamente.

Como aplicación de las propiedades de la congruencia podemos deducir los conocidos *criterios de divisibilidad*. Comencemos analizando el criterio de divisibilidad por 9 que nos dice que *"un número natural n es múltiplo de 9 si y sólo si la suma de todos sus dígitos es múltiplo de 9"*. Observamos que si el desarrollo decimal de n es $(n_s \ldots n_1 n_0)_{10}$, entonces

$$n = n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0$$

Queremos ver cuándo n es divisible por 9 o, equivalentemente, $n \equiv 0$ (mód 9). La clave para esto es observar que $10 \equiv 1$ (mód 9). Usando la propiedad 4 de las Propiedades 3.4, deducimos que $10^k \equiv 1$ (mód 9) para todo $k \in \mathbb{N}$ y, por lo tanto, de la escritura anterior de n, aplicando las propiedades 3 y 1, concluimos que:

$$\begin{aligned} n &= n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0 \\ &\equiv_{(9)} n_s \cdot 1 + \cdots + n_1 \cdot 1 + n_0 \\ &= n_s + \cdots + n_1 + n_0 \end{aligned}$$

En definitiva:

$$\text{si } n = (n_s \dots n_1 n_0)_{10}, \quad \text{entonces} \quad n \equiv n_s + \cdots + n_1 + n_0 \pmod 9$$

con lo cual, los enteros n y $n_s + \dots + n_1 + n_0$ tienen el mismo resto en la división por 9 (o sea, para conocer el resto de un número natural en la división por 9, basta sumar sus dígitos y calcular el resto en la división por 9 del número obtenido). En particular, n es múltiplo de 9 si y solo si $n_s + \dots + n_1 + n_0$ lo es.

Ejercicio 3.2. Enunciar y probar la validez de los criterios de divisibilidad por 3, 4, 5, 8 y 11.

Sugerencias para la divisibilidad por 4 y 8: observar que $10^2 \equiv 0$ (mód 4) y que $10^3 \equiv 0$ (mód 8).

Sugerencias para la divisibilidad por 11: tener en cuenta que $10 \equiv -1$ (mód 11) y que $(-1)^k$ es 1 si k es par o -1 si k es impar. Proceder luego en forma análoga a lo que hicimos para analizar divisibilidad por 9.

Una aplicación de la congruencia: el ISSN de las publicaciones. El ISSN (*International Standard Serial Number*) es un número de ocho dígitos que se usa para identificar publicaciones periódicas, tanto impresas como electrónicas. Cada publicación periódica (por ejemplo, las revistas) tiene asignado un ISSN único.

Los siete primeros dígitos de los ISSN son asignados secuencialmente a las publicaciones, independientemente del país de origen, el idioma, etc. (es decir, el ISSN no contiene información en sí mismo).

El octavo dígito de un ISSN es un *dígito de control* y para determinarlo se utiliza aritmética modular: Si los primeros siete dígitos del ISSN son $d_1 d_2 d_3 d_4 d_5 d_6 d_7$, el octavo dígito d_8 se determina de manera que:

$$8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7 + d_8$$

sea múltiplo de 11. Para esto, se calcula $8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7$ módulo 11 y se elige d_8 convenientemente.

Por ejemplo, la revista *Journal of Algebra* tiene ISSN: 0021-8693. Esto significa que se le asignaron los 7 dígitos 0021869 y luego el dígito de control. Teniendo en cuenta que:

$$\begin{aligned} 8\cdot 0+7\cdot 0+6\cdot 2+5\cdot 1+4\cdot 8+3\cdot 6+2\cdot 9 &= 0+0+12+5+32+18+18\\ &\equiv_{(11)} 1+5+(-1)+7+7\\ &\equiv_{(11)} 8 \end{aligned}$$

Si elegimos $d_8 = 3$, resulta que:

$$\begin{aligned} 8+d_8 &= 11\\ &\equiv 0 \pmod{11}. \end{aligned}$$

Sin embargo, el dígito de control no siempre es un número entre 0 y 9. Por ejemplo, para la revista *Trends in Microbiology* se tiene que ISSN: 0966-842X. ¿A qué se debe la "X"? Procediendo como en el ejemplo anterior, se calcula:

$$\begin{aligned} 8\cdot 0+7\cdot 9+6\cdot 6+5\cdot 6+4\cdot 8+3\cdot 4+2\cdot 2 &= 63+36+30+32+12+4\\ &\equiv_{(11)} (-3)+3+8+(-1)+1+4\\ &\equiv_{(11)} 1 \end{aligned}$$

con lo cual, d_8 debe cumplir:

$$1+d_8 \equiv 0 \pmod{11}$$

Ahora bien, el menor número natural que verifica esta igualdad es $d_8 = 10$. Cuando esto sucede, el dígito de control se escribe "X".

□ 3. Ecuaciones de congruencia

Martín compró unas cajas de chocolates para repartir entre sus 19 compañeros de división de la Escuela 314. Como eran menos de 19 cajas, para darle la misma cantidad de chocolates a cada uno, las abrió y repartió el contenido entre sus compañeros. Luego de hacer esto, le quedaron 5 chocolates. Sabiendo que cada caja tenía 12 chocolates, ¿cuántas cajas repartió Martín?

Para responder esta pregunta, observemos que si Martín repartió una cantidad x de cajas de chocolates, entonces la cantidad total de chocolates repartidos es $12 \cdot x$. Al repartir estos chocolates entre sus 19 compañeros le quedaron 5. En términos de divisibilidad, esto significa que $12 \cdot x$ tiene resto 5 en la división por 19 y, en términos de congruencias, que:

$$12 \cdot x \equiv 5 \pmod{19}$$

Como sabemos que $1 \leq x < 19$, podemos determinar la cantidad x de cajas repartidas por Martín verificando, para cada posible valor de x, si esta condición se cumple o no.

- Si $x = 1$, serían $12 \cdot 1 = 12$ chocolates, y $12 \not\equiv 5$ (mód 19). Concluimos que Martín no repartió una sola caja.
- Si $x = 2$, serían $12 \cdot 2 = 24$ chocolates, y $24 \equiv 5$ (mód 19). Entonces es posible que Martín haya repartido 2 cajas de chocolates.
- Si $x = 3$, serían $12 \cdot 3 = 36$ chocolates, y $36 \equiv 17 \not\equiv 5$ (mód 19). Entonces, Martín no repartió 3 cajas.
- ...

Haciendo esta misma verificación para $x = 4, 5, \ldots, 17, 18$, se ve que en ningún otro caso la cantidad total de chocolates resulta tener resto 5 en la división por 19. Concluimos entonces que Martín repartió 2 cajas de chocolates entre sus compañeros.

Para resolver el problema anterior, lo que hicimos fue buscar un entero x que sea solución de la ecuación $12 \cdot x \equiv 5 \pmod{19}$. Teniendo en cuenta que el valor buscado estaba comprendido entre 1 y 18, nos bastó con verificar cada uno de estos 18 casos. Pero esta verificación puede resultar ser muy larga si las cantidades involucradas son más grandes.

En lo que sigue estudiaremos *ecuaciones lineales de congruencia*. Se trata de ecuaciones del tipo:

$$a \cdot x \equiv b \pmod{m}$$

donde $m \in \mathbb{N}$ y $a, b \in \mathbb{Z}$, $a \neq 0$, están fijos y $x \in \mathbb{Z}$ es la incógnita.

Comencemos resolviendo la ecuación que apareció en el problema de las cajas de chocolates de Martín.

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que $12 \cdot x \equiv 5 \pmod{19}$.

La condición $12 \cdot x \equiv 5 \pmod{19}$ es equivalente a que $19 \mid 12 \cdot x - 5$, es decir, a que exista $y \in \mathbb{Z}$ tal que:

$$12 \cdot x - 5 = 19 \cdot y$$

o, lo que es lo mismo, tal que:

$$12 \cdot x - 19 \cdot y = 5$$

Ahora, ésta es una ecuación diofántica como las que estudiamos en la sección 1 de este capítulo y que ya sabemos resolver. Procediendo como vimos allí, resulta que $(40, 25)$ es una solución de esta ecuación y luego, todas sus soluciones son los pares de números enteros (x, y) de la forma $(x, y) = (40 + 19 \cdot k, 25 + 12 \cdot k)$ con $k \in \mathbb{Z}$.

En particular, lo que nos interesa para nuestro problema es que x es de la forma $x = 40 + 19 \cdot k$, que podemos reescribir usando la notación de congruencias como $x \equiv 40 \pmod{19}$, o bien (teniendo en cuenta que $40 \equiv 2 \pmod{19}$), como:

$$x \equiv 2 \pmod{19}$$

Observemos que esta ecuación tiene una única solución módulo 19, es decir, que existe un único x_0 solución de la ecuación que satisface $0 \leq x_0 < 19$ (en este caso $x_0 = 2$).

En el caso general, se puede proceder de la misma manera para llevar una ecuación de congruencias a una ecuación diofántica; para $x \in \mathbb{Z}$, vale que:

$$\begin{aligned} a \cdot x \equiv b \pmod{m} &\iff m \mid a \cdot x - b \iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - b = m \cdot y \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - m \cdot y = b \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } (x, y) \text{ es solución de } a \cdot x - m \cdot y = b \end{aligned}$$

Se resuelve la ecuación diofántica así obtenida y a partir de sus soluciones se obtienen, como en el ejemplo, las soluciones de la ecuación de congruencia original.

La equivalencia anterior entre ecuación de congruencia y ecuación diofántica nos provee un criterio para determinar cuándo una ecuación de congruencia tiene solución (ver en la Proposición 3.1 la condición que dedujimos para que la ecuación diofántica tenga soluciones):

$a \,.\, x \equiv b \pmod{m}$ tiene solución $\iff (a : m) \mid b$

En particular, *si a y m son coprimos*, la ecuación $a \cdot x \equiv b \pmod{m}$ tiene solución para todo $b \in \mathbb{Z}$. En este caso, las soluciones de la ecuación diofántica $a \cdot x - m \cdot y = b$ son de la forma $(x_0 + m \cdot k,\ y_0 + a \cdot k)$, donde (x_0, y_0) es una solución particular. Entonces las soluciones a la ecuación de congruencia son todos los x de la forma $x = x_0 + m \cdot k$ con $k \in \mathbb{Z}$, lo que podemos reescribir como:

$$x \equiv x_0 \pmod{m}$$

En el caso general, si $(a : m) \mid b$, las soluciones de $a \cdot x \equiv b \pmod{m}$ son las mismas que las de:

$$\frac{a}{(a : m)} \cdot x \equiv \frac{b}{(a : m)} \quad \left(\text{mód } \frac{m}{(a : m)}\right)$$

(Observar que ya vimos que las ecuaciones diofánticas asociadas a estas dos ecuaciones de congruencia tienen las mismas soluciones).

Ejemplo. Hallar todas las soluciones de la ecuación $24 \cdot x \equiv 10 \pmod{38}$.

Como $(24 : 38) = 2$ divide a 10, esta ecuación tiene soluciones en $\mathbb{Z}$. Para hallarlas, podemos resolver la ecuación de congruencia más simple que se obtiene dividiendo la ecuación dada por $2 = (24 : 38)$, es decir:

$$\frac{24}{2} \cdot x \equiv \frac{10}{2} \quad \left(\text{mód } \frac{38}{2}\right) \iff 12 \cdot x \equiv 5 \pmod{19}$$

Pero esta ecuación es la que resolvimos en el ejemplo anterior. Concluimos entonces que las soluciones de $24 \cdot x \equiv 10 \pmod{38}$ son los $x \in \mathbb{Z}$ tales que:

$$x \equiv 2 \pmod{19}$$

La ecuación planteada en el ejemplo que acabamos de resolver es una ecuación de congruencia módulo 38, mientras que la caracterización que dimos para sus soluciones es módulo 19, que es un *divisor* de 38. Esto ocurre en general: dada la ecuación de congruencia $a \cdot x \equiv b \pmod{m}$, si $(a : m) \mid b$, existe un único entero x_0, con $0 \leq x_0 < \frac{m}{(a:m)}$, tal que las soluciones de la ecuación son los enteros x que cumplen:

$$x \equiv x_0 \quad \left(\text{mód } \frac{m}{(a : m)}\right)$$

Ejercicio 3.3. Hallar, cuando existan, todas las soluciones a las siguientes ecuaciones lineales de congruencias:

(a) $17 \cdot x \equiv 20 \pmod{45}$
(b) $84 \cdot x \equiv 66 \pmod{270}$
(c) $28 \cdot x \equiv 30 \pmod{60}$

Ejercicio 3.4. Hallar todos los enteros a tales que el resto de dividir a $45 \cdot a$ por 27 es 9.

□ 4. El anillo de enteros módulo m

Como vimos en la sección 2 de este capítulo, la relación de congruencia módulo un número natural fijo m parte al conjunto de los enteros en m clases de equivalencia:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

donde, para cada $0 \leq r < m$, la clase $[r]$ contiene a todos los enteros que tienen resto r en la división por m.

Escribiremos el conjunto de clases de equivalencia en la congruencia módulo m como $\mathbb{Z}_m$, es decir:

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

Gracias a las propiedades 3.4, en particular a las propiedades 1 y 3, a partir de la suma y producto de números enteros se pueden definir dos operaciones en $\mathbb{Z}_m$, suma y producto, de la siguiente forma:

$$[a] +_m [b] = [a+b]$$
$$[a] \cdot_m [b] = [a \cdot b]$$

Observemos que la propiedad "$a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$" nos dice que el resultado de $[a]+_m[b]$ será el mismo sin importar qué elementos de las clases de equivalencia $[a]$ y $[b]$ consideremos para hacer la cuenta (y lo mismo nos dice la propiedad sobre el producto). En general, representamos cada clase de equivalencia módulo m por su único elemento comprendido entre 0 y m - 1 (como hicimos más arriba).

Por ejemplo:

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

Calculemos algunas sumas y productos en $\mathbb{Z}_6$.

- $[1] +_6 [3] = [1 + 3] = [4]$.
- $[2]+_6 [4] = [2+4] = [6] = [0]$. En consecuencia, $[4]$ es el inverso de $[2]$ para la suma en $\mathbb{Z}_6$.
- $[3] \cdot_6 [5] = [3 \cdot 5] = [15] = [3]$, ya que $15 \equiv 3 \pmod{6}$.
- $[5] \cdot_6 [5] = [25] = [1]$, ya que $25 \equiv 1 \pmod{6}$. Entonces, $[5]$ es inverso de sí mismo para el producto en $\mathbb{Z}_6$.

Podemos resumir las operaciones de suma y producto en $\mathbb{Z}_6$ por medio de las siguientes tablas:

$+_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\cdot_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Veamos algunas propiedades que cumplen las operaciones de suma y producto en $\mathbb{Z}_m$. En primer lugar, observamos que la asociatividad y conmutatividad de la suma y el producto en $\mathbb{Z}$ hacen que $+_m$ y $\cdot_m$ sean también *asociativas* y *conmutativas.* Por ejemplo:

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

(Análogamente se puede ver que $\cdot_m$ es asociativa y que $+_m$ y $\cdot_m$ son conmutativas).

Las clase [0] es el elemento neutro de $+_m$ y [1] es el elemento neutro de $\cdot_m$. Por otra parte, todo elemento de $\mathbb{Z}_m$ tiene un inverso para $+_m$, ya que $[a]+_m[-a] = [0]$; es decir, $[-a]$ es el inverso aditivo de $[a]$. Observemos que, sin embargo, no es cierto que todo elemento de $\mathbb{Z}_m$ tenga inverso para $\cdot_m$.Por ejemplo, mirando la tabla de $\cdot_6$, es claro que [2] no tiene inverso para $\cdot_6$, puesto que $[2] \cdot_6 [a] \neq [1]$ para todo a.

Finalmente, al igual que ocurre en $\mathbb{Z}$, las operaciones $+_m$ y $\cdot_m$ están relacionadas mediante la propiedad *distributiva* del producto sobre la suma:

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

Tenemos entonces que $\mathbb{Z}_m$ con las operaciones $+_m$ y $\cdot_m$ definidas arriba es un a*nillo conmutativo con unidad* [6] para cada $m \geq 2$.

Observación. El producto de números enteros tiene la propiedad de que si $a, b \in \mathbb{Z}$ y $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$. Esto no ocurre en general en $\mathbb{Z}_m$: mirando la tabla de $\cdot_6$ vemos que, en $\mathbb{Z}_6$, $[2] \cdot_6 [3] = [0]$, pero $[2] \neq [0]$ y $[3] \neq [0]$. Más aún, para cada $m \in \mathbb{N}$ compuesto, si $m = m_1 \cdot m_2$ con $m_1 > 1$ y $m_2 > 1$, resulta que
$[m_1] \neq [0]$, $[m_2] \neq [0]$, pero $[m_1] \cdot_m [m_2] = [m_1 \cdot m_2] = [0]$.

[6] El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra Aritmética.

La propiedad vale en $\mathbb{Z}_p$ si p es primo, ya que $[a] \cdot_p [b] = [a \cdot b] = [0]$ si y sólo si $p \mid a \cdot b$, y esto ocurre si y sólo si $p \mid a$ o $p \mid b$, o sea, si y sólo si $[a] = [0]$ o $[b] = [0]$ en $\mathbb{Z}_p$.

Ejercicio 3.5. Escribir las tablas de suma y producto en $\mathbb{Z}_2$, $\mathbb{Z}_4$ y $\mathbb{Z}_7$.

La "prueba del 9". Una herramienta que puede utilizarse para detectar errores cuando se efectúan operaciones con números enteros utilizando su desarrollo decimal es la llamada *prueba del* 9.

La idea básica consiste en reemplazar cada número natural involucrado en las operaciones por un único dígito, hacer luego la cuenta original con estos dígitos, y comparar el dígito así obtenido con el asociado al resultado original. El dígito que se le asigna a un número natural se obtiene por medio del siguiente procedimiento:

1. se calcula la suma de los dígitos del número sin tener en cuenta los 9;
2. si el resultado obtenido es mayor o igual que 9, se vuelve a sumar sus dígitos sin considerar los 9;
3. se sigue así reemplazando un número por la suma de sus dígitos hasta obtener un único dígito que, si es 9, se reemplaza por 0.

Este procedimiento se basa en la propiedad *"Si* $n = (n_s \ldots n_1 n_0)_{10}$, *entonces* $n \equiv n_s + \ldots + n_1 + n_0$ (mód 9)*"*. Utilizando esta propiedad, no es difícil convencerse de que el dígito asociado a cada número es simplemente su resto en la división por 9 y, por lo tanto, representa la misma clase de equivalencia en $\mathbb{Z}_9$. Al efectuar la operación indicada con los dígitos obtenidos y volver a transformar el resultado en un dígito, no estamos haciendo otra cosa que calcular el resultado de la operación en $\mathbb{Z}_9$.

Por ejemplo, si hacemos la suma 192.545+258.672 y el resultado nos da 451.217, para ver si hay un error calculamos:

- $192.545 \longrightarrow 1 + 2 + 5 + 4 + 5 = 17 \longrightarrow 1 + 7 = 8$
- $258.672 \longrightarrow 2 + 5 + 8 + 6 + 7 + 2 = 30 \longrightarrow 3$

Ahora efectuamos la suma de los dígitos obtenidos para los sumandos: 8 + 3 = 11, reemplazamos el resultado por un único dígito $11 \longrightarrow 1+1 = \boxed{2}$ y lo comparamos con el dígito asociado a la suma:

- $451.217 \longrightarrow 4 + 5 + 1 + 2 + 1 + 7 = 20 \longrightarrow 2 + 0 = \boxed{2}$

De esta manera obtenemos:

$$\begin{array}{rrcl} & 192.545 & \longrightarrow & 8 \\ + & 258.672 & \longrightarrow & + \quad 3 \\ \hline & 451.217 & \longrightarrow \boxed{2} & = \boxed{2} \end{array}$$

Como en este caso el resultado era el correcto, ambos dígitos coinciden. Sin embargo, el hecho de que la igualdad de los dígitos se cumpla no significa que la cuenta esté bien;

por ejemplo:

$$\begin{array}{rrcrcr} + & 192.545 & \to & & + & 8 \\ & 258.672 & \to & & & 3 \\ \hline & 451.\underline{12}7 & \to & \boxed{2} & = & \boxed{2} \end{array}$$

Tiene dos dígitos del resultado con errores.

Ahora, si los dígitos obtenidos en la prueba del 9 difieren, podemos asegurar que ha ocurrido un error, ya que lo que estamos haciendo es calcular de dos maneras distintas la suma en $\mathbb{Z}_9$.

$$\begin{array}{rrcrcr} + & 192.545 & \to & & + & 8 \\ & 258.672 & \to & & & 3 \\ \hline & 451.117 & \to & \boxed{1} & \neq & \boxed{2} \end{array}$$

En este caso, el haber obtenido como resultados $1 \neq 2$ nos dice que hemos cometido un error (aunque no podemos saber en cuál de los dígitos).

Análogamente, podemos aplicar el procedimiento en el caso del producto de números naturales. Si multiplicamos, por ejemplo, 192.545 x 258.672 y obtenemos por resultado 49.807.100.240, podemos darnos cuenta de que hay un error de la siguiente manera: el dígito asociado a 192.545 es 8 y el asociado a 258.672 es 3; haciendo la operación con estos dígitos obtenemos:

$$8 \cdot 3 = 24 \longrightarrow 2 + 4 = \boxed{6}$$

mientras que, para el resultado de la cuenta original, tenemos que:

$$49.807.100.240 \longrightarrow 4 + 8 + 7 + 1 + 2 + 4 = 26 \longrightarrow 2 + 6 = \boxed{8}$$

Como los dígitos calculados no coinciden, concluimos que hubo un error en la cuenta. (De hecho, el resultado correcto de esta multiplicación es 49.806.000.240.)

□ 5. Ecuaciones en $\mathbb{Z}_m$

Las ecuaciones de congruencia que estudiamos en la sección 3 pueden reinterpretarse como ecuaciones en $\mathbb{Z}_m$, simplemente observando que:

$$a \cdot x \equiv b \pmod{m} \iff [a] \cdot_m [x] = [b] \text{ en } \mathbb{Z}_m.$$

En lo que sigue, si queda claro en el contexto, escribiremos simplemente a para representar al elemento $[a] \in \mathbb{Z}_m$ y dejaremos de escribir los subíndices en la suma y el producto de $\mathbb{Z}_m$, es decir, escribiremos + en lugar de $+_m$ y $\cdot$ en lugar de $\cdot_m$

Ahora la ecuación $[a] \cdot_m [x] = [b]$ queda simplemente:

$$a \cdot x = b \text{ en } \mathbb{Z}_m$$

que tiene una forma más familiar. ¿Cómo resolvemos esta ecuación? En la sección 3 vimos cómo hacer esto en el caso general (resolvimos la ecuación de congruencia). Lo que pretendemos aquí es mostrar un camino alternativo utilizando las operaciones en $\mathbb{Z}_m$.

La idea para "despejar" x en una ecuación del tipo $a \cdot x = b$ es "pasar dividiendo" el coeficiente a. Formalmente, esto significa *multiplicar ambos miembros* de la ecuación por el *inverso multiplicativo* de a:

Si a^{-1} es un elemento tal que:

$$\begin{aligned} a \cdot a^{-1} &= a^{-1} \cdot a \\ &= 1 \end{aligned}$$

entonces:

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

O, equivalentemente:

$$x = a^{-1} \cdot b$$

Reemplazando este valor de x en la ecuación vemos que, en efecto, es una solución, ya que:

$$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$$

Así, si queremos resolver, por ejemplo, la ecuación $5 \cdot x = 4$ en $\mathbb{Z}_7$, como $3 \cdot 5 = 1$ en $\mathbb{Z}_7$ (o sea, 3 es el inverso multiplicativo de 5 en $\mathbb{Z}_7$), tenemos que:

$$5 \cdot x = 4 \text{ en } \mathbb{Z}_7 \implies \underbrace{3 \cdot 5}_{=1} \cdot x = 3 \cdot 4 \text{ en } \mathbb{Z}_7 \implies x = 5 \text{ en } \mathbb{Z}_7$$

y ésta es la (única) solución de la ecuación en $\mathbb{Z}_7$.

Esto nos dice que cuando $a \in \mathbb{Z}_m$ tiene inverso multiplicativo $a^{-1} \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene una única solución, $x = a^{-1} \cdot b$. En cambio, si $a \in \mathbb{Z}_m$ no tiene inverso multiplicativo, la ecuación $a \cdot x = b$ puede no tener soluciones o tener más de una solución. Por ejemplo, la ecuación $2 \cdot x = 1$ en $\mathbb{Z}_4$ no tiene solución, ya que es equivalente a la ecuación de congruencias $2 \cdot x \equiv 1$ (mód 4) y $(2 : 4) = 2$, que no divide a 1. Consideremos, por otro lado, la ecuación:

$$2 \cdot x = 2 \text{ en } \mathbb{Z}_4$$

A simple vista, deducimos que $x = 1 \in \mathbb{Z}_4$ es una solución de esta ecuación. Pero no es la única: $x = 3 \in \mathbb{Z}_4$ también lo es.

Ya vimos que, para un número natural m cualquiera, no todo elemento de $\mathbb{Z}_m$ tiene inverso multiplicativo. Por ejemplo: recién vimos que $2 \in \mathbb{Z}_4$ no tiene inverso multiplicativo. Tratemos de caracterizar los elementos que sí tienen inverso.

Sea $m \in \mathbb{N}$ fijo. Dado $a \in \mathbb{Z}_m$, un inverso multiplicativo para a en $\mathbb{Z}_m$ es un elemento $x \in \mathbb{Z}_m$ tal que:

$$a \cdot x = 1 \text{ en } \mathbb{Z}_m \text{ o, equivalentemente, } a \cdot x \equiv 1 \pmod{m}$$

Sabemos que esta última ecuación tiene solución si y sólo si $(a : m)$ divide a 1; pero para que esta condición valga, necesariamente debe ser $(a : m) = 1$. En definitiva:

$a \in \mathbb{Z}_m$ tiene inverso multiplicativo si y sólo si $(a : m) = 1$.

Por ejemplo:

- en $\mathbb{Z}_6$ los únicos elementos que tienen inverso multiplicativo son $a = 1$ y $a = 5$, ya que 1 y 5 son los únicos enteros comprendidos entre 0 y 5 que son coprimos con 6 (comparar con la tabla de $\cdot_6$ en la sección 4);
- todos los elementos de $\mathbb{Z}_7$, salvo el 0, tienen inverso multiplicativo, porque $(a : 7) = 1$ para todo $1 \leq a \leq 6$;
- en $\mathbb{Z}_8$, los elementos que tienen inverso multiplicativo son las clases de los números impares, es decir, 1, 3, 5 y 7.

Es claro que $0 \in \mathbb{Z}_m$ no puede tener inverso multiplicativo para ningún $m \geq 2$, puesto que $0 \cdot x = 0 \neq 1$ para cualquier $x \in \mathbb{Z}_m$. Pero, por ejemplo, en $\mathbb{Z}_7$, todo elemento $a \neq 0$ tiene inverso multiplicativo. Nos preguntamos, ¿cómo son los $m \in \mathbb{N}$ para los cuales todo elemento $a \in \mathbb{Z}_m$, $a \neq 0$, tiene inverso multiplicativo? Por lo que vimos antes, esto es equivalente a que $(a : m) = 1$ para todo a tal que $1 \leq a \leq m - 1$. Esto ocurre si m es *primo*: en este caso, los únicos divisores positivos de m son 1 y m, con lo cual, si $1 \leq a \leq m - 1$, el único posible divisor positivo común de a y m es 1; luego, $(a : m) = 1$. Por otro lado, si m no es primo, entonces m puede escribirse como un producto de dos números naturales menores que m, es decir, $m = a \cdot a'$ con $1 < a, a' < m$. Entonces $a \in \mathbb{Z}_m$ es no nulo y no tiene inverso multiplicativo, ya que $(a : m) = a \neq 1$.

Un anillo conmutativo con unidad en el que todo elemento no nulo tiene inverso multiplicativo se llama un *cuerpo*. El razonamiento anterior prueba que:

Teorema 3.5. *$\mathbb{Z}_m$ es un cuerpo si y sólo si $m \in \mathbb{N}$ es primo.*

Ejercicio 3.6.

1. Hallar los inversos multiplicativos de todos los elementos no nulos de $\mathbb{Z}_7$.
2. Determinar todos los elementos de $\mathbb{Z}_{14}$ que tienen inverso multiplicativo y hallar dichos inversos.

Volviendo a las ecuaciones lineales, el resultado anterior nos dice que, si m es primo y $a \neq 0 \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene un única solución en $\mathbb{Z}_m$. Cuando m no es primo, la ecuación $a \cdot x = b$ tiene solución en $\mathbb{Z}_m$ si y sólo si $(a : m) \mid b$. En caso que esto ocurra, existe un único entero x_0 con $0 \leq x_0 < \frac{m}{(a:m)}$ tal que las soluciones son todos los enteros x que cumplen $x \equiv x_0 \pmod{\frac{m}{(a:m)}}$, es decir, los enteros de la forma $x = x_0 + k \cdot \frac{m}{(a:m)}$ con $k \in \mathbb{Z}$. No es difícil ver que:

$$x_0,\ x_0 + \frac{m}{(a:m)},\ x_0 + 2 \cdot \frac{m}{(a:m)}, \ldots,\ x_0 + ((a:m) - 1) \cdot \frac{m}{(a:m)}$$

pertenecen a clases de equivalencia distintas en $\mathbb{Z}_m$ y que cualquier otro entero de la forma $x_0 + k \cdot \frac{m}{(a:m)}$ pertenece a la clase de alguno de ellos. Concluimos que:

Si $(a : m) \mid b$, la ecuación $a \,.\, x = b$ tiene exactamente $(a : m)$ soluciones distintas en $\mathbb{Z}_m$, que son de la forma

$$x_0 + k \cdot \frac{m}{(a : m)} \quad \text{con } 0 \leq k < (a : m)$$

para algún x_0 tal que $0 \leq x_0 < \frac{m}{(a:m)}$

Ejercicio 3.7. Para cada una de las siguientes ecuaciones, determinar si tiene soluciones y, en caso afirmativo, hallarlas:

- $5 \cdot x = 4$ en $\mathbb{Z}_{14}$
- $6 \cdot x = 10$ en $\mathbb{Z}_{21}$
- $20 \cdot x = 12$ en $\mathbb{Z}_{24}$

□ 6. Teorema chino del resto

Lorena y sus amigas juegan al *Corazones*, que es un juego de cartas que se juega con un mazo de cartas francesas, sin los comodines (son 52 cartas). No vamos a entrar en los detalles del juego, simplemente diremos que al comienzo de cada mano de *Corazones* se reparten las cartas de manera que todos los jugadores tengan la misma cantidad (eventualmente pueden sobrar algunas).

En el caso de Lorena y sus amigas, aunque ellas no lo saben, al mazo de cartas con el que están jugando le faltan algunas cartas. En la primera mano juegan 5 de las amigas; Lorena reparte todas las cartas que puede y le sobran 2. En la mano siguiente, juegan 4 y sobran 3 cartas (estaban un poco distraídas y no se dieron cuenta de que esto no puede ser). Finalmente, juegan una última mano entre 3 de las amigas y al repartir las cartas sobran 2. En este momento Lorena, que no estaba jugando porque había salido última en la mano anterior, se da cuenta de que no puede ser que sobren 2 cartas (¿cómo lo supo?).

Lorena se pregunta cuántas cartas faltan en el mazo y decide intentar calcular este número sin interrumpir el juego (o sea, ¡sin contar las cartas!). Haciendo memoria sobre lo que ocurrió en las manos anteriores, razona como sigue:

Si x es la cantidad de cartas que hay en el mazo, entonces

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3 \end{cases}$$

Como la cantidad de cartas es $x \leq 52$, por la condición $x \equiv 2 \pmod 5$, Lorena deduce que:

$$x \in \{2, \underline{7}, 12, 17, 22, \underline{27}, 32, 37, 42, \underline{47}, 52\}$$

De entre estos posibles valores, se queda con los que además cumplen que $x \equiv 3 \pmod 4$, es decir

$$x \in \{7, 27, \underline{47}\}$$

y de estos, busca los que cumplen que $x \equiv 2 \pmod 3$. El único valor con esta propiedad resulta ser:

$$x = 47$$

Lorena concluye que están jugando con 47 cartas, es decir, que faltan 5 en el mazo.

El problema general que trataremos en esta sección es el de la resolución de s*istemas de ecuaciones de congruencias.* Más precisamente, dados $m_1, m_2, \ldots, m_n \in \mathbb{N}$ y $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, se busca hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{3}$$

Un sistema de ecuaciones de este tipo no siempre tiene solución; por ejemplo, el sistema:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 4 \pmod 6 \end{cases}$$

no tiene soluciones. En efecto, la condición $x \equiv 4 \pmod 6$ implica que $x \equiv 4 \pmod 2$ (por la propiedad 6 de la Proposición 3.4). O sea, un entero x que satisface la segunda ecuación debe ser par. Pero la primera condición, $x \equiv 1 \pmod 2$, pide que x sea impar.

Una situación en la que podemos asegurar que el sistema de ecuaciones de congruencias sí tiene soluciones es cuando los módulos $m_1, \ldots, m_n$ son coprimos de a pares, es decir, si dos cualesquiera de ellos son coprimos.

Teorema 3.6 (Teorema chino del resto[7]). *Sean $m_1, m_2 \ldots, m_n \in \mathbb{N}$ coprimos de a pares, y sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Entonces existe un único $x_0 \in \mathbb{Z}$ con $0 \le x_0 < m_1 \cdot m_2 \ldots m_n$ que es solución del sistema de ecuaciones:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

y, además, un entero x es solución de las ecuaciones si y sólo si:

$$x \equiv x_0 \pmod{m_1 \cdot m_2 \cdots m_n}$$

Demostración. *Existencia.* Haremos la demostración por inducción en n, la cantidad de ecuaciones del sistema. Para $n = 1$ no hay nada que hacer, ya que el sistema es en realidad una única ecuación de congruencia.

Supongamos que el enunciado vale para sistemas de n ecuaciones y consideremos un sistema de $n + 1$ ecuaciones:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases}$$

[7] El origen de este teorema es un problema similar al que planteamos al comienzo de esta sección que aparece en el Manual Matemático escrito por Sun Zi alrededor del año 300. Un método para resolver este problema en el caso general fue dado en el Tratado de Matemática en Nueve Secciones, escrito por Qin Jiushao en 1247.

con $(m_i; m_j) = 1$ para todo $i \neq j$. Por la hipótesis inductiva, el sistema formado por las primeras n ecuaciones es equivalente a una única ecuación de congruencia:

$$x \equiv A \pmod{m_1 \cdots m_n}$$

para un (único) entero A con $0 \leq A < m_1 \ldots m_n$. Esto dice que los enteros x que cumplen las primeras n ecuaciones son aquéllos de la forma $x = M \cdot Q + A$ con $Q \in \mathbb{Z}$, donde $M = m_1 \ldots m_n$.

Las soluciones del sistema original son los x de esta forma que además cumplen la última ecuación; o sea $x = M \cdot Q + A$ para $Q \in \mathbb{Z}$ tal que $M \cdot Q + A \equiv a_{n+1} \pmod{m_{n+1}}$. Ahora, esta última condición es equivalente a la ecuación de congruencia:

$$M \cdot Q \equiv a_{n+1} - A \pmod{m_{n+1}}$$

Como por hipótesis $(m_i; m_{n+1}) = 1$ para cada $1 \leq i \leq n$, entonces $M = m_1 \ldots m_n$ resulta también coprimo con m_{n+1} y, por lo tanto, la ecuación anterior tiene solución. Más aún, las soluciones son de la forma:

$$Q \equiv q \pmod{m_{n+1}}$$

para un único q con $0 \leq q < m_{n+1}$, es decir, de la forma $Q = m_{n+1} \cdot k + q$ con $k \in \mathbb{Z}$. En definitiva, las soluciones del sistema son los $x \in \mathbb{Z}$ tales que:

$$\begin{aligned} x &= M \cdot Q + A \\ &= M \cdot (m_{n+1} \cdot k + q) + A \\ &= M \cdot m_{n+1} \cdot k + M \cdot q + A \\ &= (m_1 \cdots m_n \cdot m_{n+1}) \cdot k + (M \cdot q + A) \end{aligned}$$

Llamando $x_0 = M \cdot q + A$, esto es equivalente a la ecuación:

$$x \equiv x_0 \pmod{m_1 \cdots m_n \cdot m_{n+1}}$$

Como $0 \leq q \leq m_{n+1} - 1$ y $0 \leq A \leq M - 1$, resulta que

$$0 \leq x_0 \leq M \cdot (m_{n+1} - 1) + M - 1 = M \cdot m_{n+1} - 1 = m_1 \ldots m_n \cdot m_{n+1} - 1.$$

Unicidad. Supongamos que $0 \leq x_0 < x'_0 < m_1 \ldots m_n$ son dos soluciones del sistema dado. Entonces $x_0 \equiv x'_0 \pmod{m_i}$ para cada $1 \leq i \leq n$ (ya que ambos son congruentes a a_i); es decir, $m_i \mid x'_0 - x_0$ para todo $1 \leq i \leq n$. En otras palabras, $x'_0 - x_0$ es un múltiplo común de $m_1, \ldots, m_n$. Pero como $m_1, \ldots, m_n$ son coprimos de a pares, su mínimo común múltiplo es $m_1 \ldots m_n$; luego, $x'_0 - x_0$ es múltiplo de $m_1 \ldots m_n$. Como $0 \leq x'_0 - x_0 < m_1 \ldots m_n$, esto implica que necesariamente $x'_0 - x_0 = 0$, es decir, $x'_0 = x_0$.

El teorema nos asegura que, si los módulos son coprimos de a pares, vamos a encontrar una solución x_0 (y sólo una) para el sistema (3) que cumple $0 \leq x_0 < m_1 \cdot m_2 \ldots m_n$, y que *todas* las soluciones del sistema son los enteros de la forma $x = m_1 \cdot m_2 \ldots m_n \cdot k + x_0$ con $k \in \mathbb{Z}$.

Algoritmo para resolver el sistema (3) si $m_1, \ldots, m_n$ son coprimos de a pares.

- Definir $M_1 = m_1$ y $A_1 = a_1$. De la primera ecuación, $x \equiv a_1$ (mód m_1), se deduce que las soluciones son de la forma $x = M_1 \cdot Q_1 + A_1$ con $Q_1 \in \mathbb{Z}$.
- Para $i = 1, \ldots, n-1$:

  resolver $M_i \cdot Q_i + A_i \equiv a_{i+1} \pmod{m_{i+1}}$

  (donde la incógnita es Q_i). Sea $q_i \in \mathbb{Z}$ con $0 \le q_i < m_{i+1}$ tal que las soluciones de esta ecuación son $Q_i \equiv q_i \pmod{m_{i+1}}$:

  definir $M_{i+1} = M_i \cdot m_{i+1}, \quad A_{i+1} = M_i \cdot q_i + A_i$

  Entonces las soluciones del sistema formado por las primeras $i+1$ ecuaciones son de la forma $x = M_{i+1} \cdot Q_{i+1} + A_{i+1}$ con $Q_{i+1} \in \mathbb{Z}$.

- Dar como respuesta $x \equiv A_n \pmod{M_n}$.

Saber que hay una solución en un rango acotado nos permite hallarla por búsqueda exhaustiva (si es que el rango no es demasiado grande). Como Lorena en el ejemplo, buscamos todos los enteros x con $0 \le x < m_1 \cdot m_2 \ldots m_n$ tales que $x \equiv a_1 \pmod{m_1}$; de estos nos quedamos con aquellos que también cumplen que $x \equiv a_2 \pmod{m_2}$, y seguimos así, agregando en cada paso una restricción, hasta llegar a tener un único elemento en la lista. Sin embargo, para valores grandes de $m_1, \ldots, m_n$ esta búsqueda puede volverse tediosa. Resulta entonces más conveniente proceder resolviendo las ecuaciones sucesivamente.

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 14 \pmod{49} \\ x \equiv 17 \pmod{45} \end{cases}$$

Como $(49 : 45) = 1$, el Teorema chino del resto asegura que el sistema tiene soluciones y que tiene una única solución x_0 con $0 \le x_0 < 49 \cdot 45 = 2.205$. Buscaremos la solución resolviendo sucesivamente las ecuaciones.

Las soluciones de la primera ecuación, $x \equiv 14 \pmod{49}$, son todos los enteros x de la forma:

$$x = 49 \cdot q + 14, \quad \text{con } q \in \mathbb{Z}$$

De entre todos los posibles q, nos interesan aquéllos que hacen que se cumpla la segunda ecuación, $x \equiv 17 \pmod{45}$; en términos de q, esto es que $49 \cdot q + 14 \equiv 17 \pmod{45}$. En definitiva, nos queda una ecuación lineal de congruencia; basta determinar los $q \in \mathbb{Z}$ tales que:

$$49 \cdot q \equiv 3 \pmod{45}.$$

Acá vemos la importancia de que $(49 : 45) = 1$, que es lo que nos asegura que esta ecuación, y por lo tanto también el sistema original, tiene solución. Reduciendo módulo 45, la ecuación anterior queda $4 \cdot q \equiv 3 \pmod{45}$ y vemos que una solución es $q_0 = 12$ (en el caso general, resolvemos la ecuación de congruencia como vimos en la sección 3); luego todas sus soluciones son los $q \equiv 12 \pmod{45}$, es decir:

$$q = 45 \cdot k + 12, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, concluimos que las soluciones del sistema son todos los enteros x de la forma $x = 49 \cdot q + 14 = 49 \cdot (45 \cdot k + 12) + 14 = 49 \cdot 45 \cdot k + 602 = 2.205 \cdot k + 602$, con $k \in \mathbb{Z}$.

En el caso de un sistema de ecuaciones de congruencia en el que los módulos no son coprimos, lo que puede hacerse es tratar de reducirlo a otro en el que sí lo sean. Para hacer esto, la observación fundamental es que si $m = m_1 \cdot m_2 \ldots m_r$ con $m_1, \ldots, m_r$ coprimos de a pares, entonces:

$$x \equiv a \pmod{m} \iff \begin{cases} x \equiv a & (\text{mód } m_1) \\ \vdots & \\ x \equiv a & (\text{mód } m_r) \end{cases}$$

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 3 & (\text{mód } 12) \\ x \equiv 9 & (\text{mód } 14) \end{cases}$$

Tenemos que:

$$x \equiv 3 \pmod{12} \iff \begin{cases} x \equiv 3 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases} \iff \begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases}$$

$$x \equiv 9 \pmod{14} \iff \begin{cases} x \equiv 9 & (\text{mód } 2) \\ x \equiv 9 & (\text{mód } 7) \end{cases} \iff \begin{cases} x \equiv 1 & (\text{mód } 2) \\ x \equiv 2 & (\text{mód } 7) \end{cases}$$

Aquí los módulos no son coprimos de a pares, $(4 : 2) = 2$, pero vemos que la validez de la segunda ecuación implica la de la tercera. Luego, podemos suprimir esta última y resolver el sistema que queda:

$$\begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \\ x \equiv 2 & (\text{mód } 7) \end{cases} \iff x \equiv 51 \pmod{3 \cdot 4 \cdot 7}$$

Concluimos que las soluciones del sistema dado son los enteros de la forma $x = 84 \cdot k + 51$ con $k \in \mathbb{Z}$.

Ejercicio 3.8. Un grupo de amigos va a cenar a una pizzería. Cuando llega la cuenta, en la mesa son 10 personas; si todos ponen la misma cantidad (entera) de dinero, recolectan $6 más que lo que debían pagar. En ese momento vuelve a la mesa Martín (es decir, en realidad eran 11 amigos y no 10). Reparten entonces los gastos entre los 11, y sobran $10. Sabiendo que juntaron más de $100, ¿cuánto es lo mínimo que puede haberles costado la cena?

Ejercicio 3.9.

- Hallar todos los enteros que tienen resto 1 en la división por 3, resto 2 en la división por 5 y resto 5 en la división por 7.
- Hallar, si existen, todos los enteros que tienen resto 8 en la división por 12 y resto 6 en la división por 20.

□ 7. Pequeño teorema de Fermat

Como vimos en uno de los ejemplos de la sección 2, los restos de dividir las sucesivas potencias de un entero a por un entero m se repiten en algún momento (porque hay sólo una cantidad finita de restos posibles, mientras que consideramos infinitas potencias). Para simplificar los cálculos, es útil conocer un exponente donde ocurre esta repetición. El *pequeño teorema de Fermat*[8] es un

[8] Este teorema fue enunciado originalmente por Pierre de Fermat en una carta en 1640. Aunque se supone que Leibniz lo demostró unos pocos años después, fue recién en 1736 que Euler publicó la primera demostración. Más adelante, en 1760, Euler también probó una generalización del teorema.

resultado fundamental que nos da esa información.

Teorema 3.7 (Pequeño teorema de Fermat). *Sea $p \in \mathbb{N}$ un primo. Para cada $a \in \mathbb{Z}$ que no es múltiplo de p, vale que $a^{p-1} \equiv 1$ (mód p). Más aún, para todo $a \in \mathbb{Z}$ vale que $a^p \equiv a$ (mód p).*

Demostración. Sea $a \in \mathbb{Z}$ no divisible por p. Sea $[a] \in \mathbb{Z}_p$ la clase de equivalencia de a. Tenemos que $[a] \neq [0]$. Consideremos el conjunto $\mathbb{Z}_p^*$ de todos los elementos no nulos de $\mathbb{Z}_p$,

$$\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}$$

Vamos a multiplicar cada elemento de $\mathbb{Z}_p^*$ por $[a]$ y a mirar el conjunto obtenido de esta manera. Observemos que si $[b], [c] \in \mathbb{Z}_p$ y $[a] \cdot [b] = [a] \cdot [c]$, necesariamente $[b] = [c]$ porque podemos multiplicar ambos miembros de la primera igualdad por el inverso multiplicativo de $[a]$; en particular, $[a] \cdot [b] \neq 0$ si $[b] \neq 0$. Entonces, deducimos que el conjunto:

$$[a] \cdot \mathbb{Z}_p^* = \{[a] \cdot [1], [a] \cdot [2], \ldots, [a] \cdot [p-1]\}$$

está formado por p - 1 elementos del conjunto $\mathbb{Z}_p^*$ *distintos entre sí*. Como $\mathbb{Z}_p^*$ tiene a su vez p - 1 elementos, concluimos que $[a] \cdot \mathbb{Z}_p^*$ contiene a *todos* los elementos de $\mathbb{Z}_p^*$, es decir, que $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$.

Multiplicando los elementos de $[a] \cdot \mathbb{Z}_p^*$ obtenemos, por un lado:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \cdots \cdot ([a] \cdot [p-1]) &= [a]^{p-1} \cdot ([1] \cdot [2] \cdot \cdots \cdot [p-1]) \\ &= [a^{p-1}] \cdot [1 \cdot 2 \cdot \cdots \cdot (p-1)] \end{aligned}$$

Por otra parte, como $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$, el producto de estos elementos es el producto de los elementos de $\mathbb{Z}_p^*$ (eventualmente hecho en otro orden), o sea:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \cdots \cdot ([a] \cdot [p-1]) &= [1] \cdot [2] \cdot \cdots \cdot [p-1] \\ &= [1 \cdot 2 \cdot \cdots \cdot (p-1)] \end{aligned}$$

Igualando ambas expresiones para el producto, resulta que:

$$[a^{p-1}] \cdot [1 \cdot 2 \cdot \cdots \cdot (p-1)] = [1 \cdot 2 \cdot \cdots \cdot (p-1)]$$

Como p no divide a $1 \cdot 2 \cdot \ldots \cdot (p-1)$, puesto que es primo y no divide a ninguno de los factores, tenemos que $[1 \cdot 2 \cdot \ldots \cdot (p-1)] \neq [0]$, con lo que tiene inverso multiplicativo en $\mathbb{Z}_p$ y, multiplicando la igualdad anterior por dicho inverso, deducimos que:

$$[a^{p-1}] = 1$$

o, en términos de congruencias:

$$a^{p-1} \equiv 1 \pmod{p}$$

Para terminar, observemos que multiplicando ambos miembros de esta congruencia por a obtenemos que:

$$a^p \equiv a \pmod{p}$$

Pero esta igualdad vale también cuando $p \mid a$, ya que en este caso $a \equiv 0 \pmod{p}$ y también $a^p \equiv 0 \pmod{p}$.

Observación. Sea $p \in \mathbb{N}$ primo y sea $a \in \mathbb{Z}$ no divisible por p. Entonces $a^n \equiv a^m \pmod{p}$ si n y m son números naturales tales que $n \equiv m \pmod{p-1}$. En particular, si r_{p-1} es el resto en la división de n por $p-1$, entonces $a^n \equiv a^{r_{p-1}} \pmod{p}$.

En efecto, suponiendo que $n \geq m$, si $n \equiv m \pmod{p-1}$, tenemos que $n = m + k \cdot (p-1)$ para algún $k \in \mathbb{N}_0$; luego:

$$\begin{aligned} a^n &= a^{m+k\cdot(p-1)} \\ &= a^m \cdot (a^{p-1})^k \\ &\equiv a^m \cdot 1^k \\ &\equiv a^m \pmod{p} \end{aligned}$$

donde la anteúltima congruencia es consecuencia del pequeño teorema de Fermat.

Ejemplo. Hallar el resto en la división de $3^{1.423}$ por 11.

Por la Proposición 3.3, sabemos que el resto buscado es el único entero r con $0 \leq r < 11$ tal que $3^{1.423} \equiv r \pmod{11}$. Ahora, por la observación anterior, como $1.423 \equiv 3 \pmod{10}$ tenemos que:

$$\begin{aligned} 3^{1.423} &\equiv 3^3 \\ &\equiv 5 \pmod{11} \end{aligned}$$

Luego, $r = 5$.

Mencionemos, para concluir esta sección, que como consecuencia del pequeño teorema de Fermat podemos obtener una expresión explícita para los inversos multiplicativos de los elementos de $\mathbb{Z}_p$, si $p \in \mathbb{N}$ es primo: *el inverso multiplicativo de un elemento* $a \in \mathbb{Z}_p$, $a \neq 0$, *es* $a^{p-2} \in \mathbb{Z}_p$. En efecto, tenemos que $a \cdot a^{p-2} = a^{p-1} = 1$ en $\mathbb{Z}_p$, con lo que $a^{-1} = a^{p-2}$ en $\mathbb{Z}_p$.

Ejercicio 3.10. Hallar el resto en la división de a por m en los siguientes casos:

- $a = 129^{111}$, $m = 7$.
- $a = 129^{111}$, $m = 35$. (Sugerencia: calcular el resto en la división por 5 y por 7 y usar el teorema chino del resto).

□ 8. Aplicación: Tests de primalidad

Un *test de primalidad* es un procedimiento para determinar si un entero dado es primo o no lo es.

Dado $n \in \mathbb{N}$ un posible test de primalidad consiste en verificar si n es divisible por algún entero m tal que $2 \leq m \leq \sqrt{n}$. Si algún $m_0 \in \mathbb{N}$ con $2 \leq m_0 \leq \sqrt{n}$ divide a n, es claro que n es compuesto (hemos encontrado un divisor propio de n). De lo contrario, podemos asegurar que n es primo por el Lema 2.8 del capítulo 2. Este procedimiento nos permite decidir con certeza si n es primo.

Sin embargo, para valores grandes de n, la cantidad de operaciones a realizar (y por consiguiente, el tiempo que lleva hacerlas) puede resultar demasiado grande a los fines prácticos.

El pequeño teorema de Fermat ha dado lugar a tests de primalidad *probabilísticos* alternativos. La idea es que el método no nos permite determinar con certeza si n es primo, sino que podemos saberlo pero con cierta probabilidad de error.

8.1. Test de primalidad de Fermat

Este procedimiento funciona como explicamos a continuación:

- dado $n \in \mathbb{N}$, se elige al azar un entero a tal que $2 \leq a \leq n - 1$ y se calcula $a^{n-1} \pmod{n}$;
- si $a^{n-1} \not\equiv 1 \pmod{n}$, la respuesta es que *n es compuesto*;
- si $a^{n-1} \equiv 1 \pmod{n}$, la respuesta es que *n probablemente sea primo*.

Observemos que en caso que $a^{n-1} \not\equiv 1 \pmod{n}$, podemos estar seguros de que a **no** es primo, porque el pequeño teorema de Fermat nos dice que de serlo, debería ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ sin importar qué valor de a hayamos elegido.

Ahora bien, si n es compuesto puede ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ para algún a tal que $2 \leq a \leq n - 1$. Por ejemplo, para $n = 91 = 7 \cdot 13$ (¡que no es primo!) y $a = 3$ se tiene que $3^{90} = (3^6)^{15} = 729^{15} \equiv_{(91)} 1^{15} \equiv_{(91)} 1$. Es por este motivo que no podemos estar seguros de que n sea primo si la congruencia vale.

Sin embargo, si existe algún a coprimo con n tal que $a^{n-1} \not\equiv 1 \pmod{n}$, entonces lo mismo ocurre para al menos la mitad de los posibles $2 \leq a \leq n - 1$. Esto se debe a que, si $a_1, \ldots, a_s$ son todas las bases para las cuales $a_i^{n-1} \equiv 1 \pmod{n}$, entonces $(a \cdot a_i)^{n-1} = a^{n-1} \cdot a_i^{n-1} \equiv_{(n)} a^{n-1} \cdot 1 \equiv_{(n)} a^{n-1} \not\equiv_{(n)} 1$ y, además, $a \cdot a_1, \ldots, a \cdot a_s$ son todos distintos módulo n, ya que a es coprimo con n. Así, hay una probabilidad menor que $1/2$ de que eligiendo a al azar se verifique $a^{n-1} \equiv 1 \pmod{n}$. Si el proceso se repite k veces, la probabilidad de que en todos los casos resulte $a^{n-1} \equiv 1 \pmod{n}$ es $1/2^k$ (¡muy chica si k es grande!).

El problema es que hay enteros compuestos n para los cuales $a^{n-1} \equiv 1 \pmod{n}$ para *todo* a coprimo con n. Estos enteros se conocen como *números de Carmichael* y el hecho de que sean compuestos los hace difícil de detectar para el test de Fermat (sólo nos damos cuenta de que n es compuesto si justo elegimos un a tal que $(a : n) \neq 1$).

El menor de estos números[9] es $n = 561$; veamos que tiene la propiedad mencionada, es decir que:

$$a^{560} \equiv 1 \pmod{561}$$

[9] Este número fue encontrado por Carmichael en 1910, de ahí el nombre que reciben los enteros con esta propiedad.

para todo $a \in \mathbb{Z}$ con $(a : 561) = 1$. Como $561 = 3 \cdot 11 \cdot 17$, para probar lo anterior basta ver que:

$$\begin{cases} a^{560} \equiv 1 \pmod 3 \\ a^{560} \equiv 1 \pmod{11} \\ a^{560} \equiv 1 \pmod{17} \end{cases}$$

Estas congruencias son consecuencia del pequeño teorema de Fermat: en efecto, si $(a : 561) = 1$, tenemos que a no es múltiplo de 3 ni de 11 ni de 17, y el teorema asegura entonces que:

$$a^2 \equiv 1 \pmod 3, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}$$

con lo cual:

$$a^{560} = (a^2)^{280} \equiv 1 \pmod 3, \qquad a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}, \qquad a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$$

8.2. Test de primalidad de Miller-Rabin

Este procedimiento alternativo para determinar si un entero dado es primo o no se basa en el pequeño teorema de Fermat más el hecho fundamental de que:

$$x^2 \equiv 1 \pmod p \iff x \equiv 1 \pmod p \quad \text{o} \quad x \equiv -1 \pmod p.$$

Esta equivalencia vale ya que, si p es primo, entonces $p \mid x^2 - 1 = (x - 1) \cdot (x + 1)$ si y sólo si $p \mid x - 1$ o $p \mid x + 1$ (recordar que un número primo divide a un producto si y sólo si divide a alguno de los factores). Más precisamente, ambos resultados se combinan en la siguiente propiedad:

Proposición 3.8. *Sea p un primo positivo impar. Factoricemos $p - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar. Entonces, para cada $a \in \mathbb{Z}$ que no es múltiplo de p se tiene que:*

$$a^t \equiv 1 \pmod p \quad o \quad a^{t \cdot 2^k} \equiv -1 \pmod p \text{ para algún } 0 \le k < r$$

Demostración. Por el pequeño teorema de Fermat, sabemos que $a^{t \cdot 2^r} \equiv 1 \pmod p$. Como $r \ge 1$ porque $p - 1$ es par, podemos escribir $a^{t \cdot 2^r} = (a^{t \cdot 2^{r-1}})^2$ con $r - 1 \in \mathbb{N}_0$, y tenemos que:

$$(a^{t \cdot 2^{r-1}})^2 \equiv 1 \pmod p$$

Por lo que observamos más arriba, esto equivale a que:

$$a^{t \cdot 2^{r-1}} \equiv 1 \pmod p \quad \text{o} \quad a^{t \cdot 2^{r-1}} \equiv -1 \pmod p$$

Si $a^{t \cdot 2^{r-1}} \equiv -1 \pmod p$, se verifica la segunda condición del enunciado con $k = r - 1$. De lo contrario, resulta que $a^{t \cdot 2^{r-1}} \equiv 1 \pmod p$. Si $r - 1 = 0$, esto es simplemente la primera de las condiciones del enunciado. Finalmente, si $r - 1 \ge 1$, repitiendo el razonamiento anterior para $a^{t \cdot 2^{r-1}}$, deducimos que $a^{t \cdot 2^{r-2}} \equiv 1 \pmod p$ o $a^{t \cdot 2^{r-2}} \equiv -1 \pmod p$.

Siguiendo de la misma manera, o bien se llega en algún momento a un k con $0 \le k \le r - 1$ tal que $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, o bien resulta que $a^t \equiv 1 \pmod{p}$.

El *test de primalidad de Miller-Rabin* funciona entonces como sigue:

- dado $n \in \mathbb{N}$ impar, se escribe $n - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar;
- se elige a tal que $2 \le a \le n - 1$ al azar;
- se calcula $a^t \pmod{n}$. Si $a^t \equiv 1 \pmod{n}$ o $a^t \equiv -1 \pmod{n}$, decimos que *n probablemente sea primo*;
- si no, se calculan sucesivamente $a^{t \cdot 2} = (a^t)^2, a^{t \cdot 2^2} = (a^{t \cdot 2})^2, \ldots, a^{t \cdot 2^k} = (a^{t \cdot 2^{k-1}})^2, \ldots \pmod{p}$ hasta obtener como resultado -1, o bien hasta llegar a $a^{t \cdot 2^{r-1}}$. Si en algún paso el resultado es $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, decimos que *n probablemente sea primo*. De lo contrario, tenemos que:

$$a^t \not\equiv 1 \pmod{n} \quad \text{y} \quad a^{t \cdot 2^k} \not\equiv -1 \text{ para todo } 0 \le k \le r - 1$$

y, por la proposición anterior, podemos asegurar que *n es compuesto.*

Se puede ver que si n es compuesto, la propiedad:

$$a^t \equiv 1 \pmod{n} \quad \text{o} \quad a^{t \cdot 2^k} \equiv -1 \pmod{n} \text{ para algún } 0 \le k < r$$

se cumple a lo sumo para la cuarta parte de los a tales que $1 \le a \le n - 1$. Es decir, que la probabilidad de que para un n compuesto el test diga que n probablemente sea primo es a lo sumo $1/4$. Esto nos dice que repitiendo el test para distintos valores de a podemos hacer que la probabilidad de obtener una respuesta incorrecta sea muy chica.

Ejemplo. Apliquemos el test de Miller-Rabin a $n = 561$.

- Escribimos $n - 1 = 560 = 35 \cdot 2^4$.
- Elegimos a tal que $2 \le a \le 560$, por ejemplo, $a = 2$.
- Calculamos $2^{35} \equiv 263 \pmod{561}$. Como $2^{35} \not\equiv 1 \pmod{561}$ y $2^{35} \not\equiv -1 \pmod{561}$, continuamos.
- Elevamos al cuadrado sucesivamente:
  - $(2^{35})^2 \equiv 263^2 \equiv 166 \not\equiv -1 \pmod{561}$
  - $(2^{35})^{2^2} \equiv 166^2 \equiv 67 \not\equiv -1 \pmod{561}$
  - $(2^{35})^{2^3} \equiv 67^2 \equiv 1 \not\equiv -1 \pmod{561}$
- Concluimos que 561 es *compuesto*.

□ 9. Aplicación: criptografía

La *criptografía* se encarga de estudiar cómo enviar mensajes de manera *secreta*. El

objetivo es que solamente el receptor a quien queremos enviarle el mensaje pueda leerlo y entenderlo, es decir, que si otra persona (en particular, alguien que nosotros no queremos que lea el mensaje) logra acceder a la información, no pueda interpretarla.

Para esto se utilizan distintos *métodos de encriptación* y, esencialmente, el proceso funciona como explicamos a continuación:

- el emisor *encripta* el mensaje, es decir, convierte la información original o *texto plano* en *texto cifrado*, que en apariencia no tiene sentido,
- se transmite el texto cifrado,
- el receptor *desencripta* el mensaje recibido, es decir, lo vuelve a su forma original.

Lo importante en este esquema es que si el texto cifrado es interceptado por quien no es el receptor, sea muy difícil o mejor aún, imposible, de descifrar.

El texto plano del mensaje m es encriptado por el emisor usando un método **e**; el resultado es el texto cifrado c que se transmite al receptor, quien lo desencripta por medio de **d** para recuperar el mensaje original m.

$$m \longrightarrow \boxed{\mathbf{e}} \longrightarrow c \longrightarrow \boxed{\mathbf{d}} \longrightarrow m$$

Emisor *Receptor*

Procedimientos de este tipo se han utilizado desde la antigüedad: por ejemplo, se cuenta que Julio César utilizaba un esquema de encriptación basado en una tabla como la siguiente:

0	A	D
1	B	E
2	C	F
3	D	G
4	E	H
5	F	I
6	G	J
7	H	K
8	I	L
9	J	M
10	K	N
11	L	O
12	M	P

13	N	Q
14	O	R
15	P	S
16	Q	T
17	R	U
18	S	V
19	T	W
20	U	X
21	V	Y
22	W	Z
23	X	A
24	Y	B
25	Z	C

La segunda columna de estas tablas contiene, ordenadas, las 26 letras del alfabeto. La tercera columna, también contiene todo el alfabeto ordenado, pero comenzando desde la letra D y volviendo a comenzar con la A una vez que se termina. Para encriptar una palabra, se reemplaza cada una de sus letras por la ubicada a su lado en la tabla anterior. Por ejemplo, la palabra

ATAQUE

se codifica como

DWDTXH.

Para desencriptar se utiliza la tabla de manera inversa: se lee en la tercera columna y se busca su interpretación en la segunda.

El mecanismo para encriptar resulta ser simplemente reemplazar cada letra por la que está tres lugares más adelante en el alfabeto, leyéndolo en forma circular (o sea, "a b c ... x

y z a b ..."), y para desencriptar, reemplazar cada letra por la que está tres lugares antes.

Podemos interpretar esto en términos matemáticos como sigue: representamos cada letra por un elemento $x \in \mathbb{Z}_{26}$ (el número ubicado en la primera columna de las tablas) y para encriptarla calculamos:

$$\mathbf{e}(x) = x + 3 \quad \text{en } \mathbb{Z}_{26}$$

y escribimos la letra representada por el elemento obtenido. Por ejemplo:

- la letra Q corresponde al elemento $16 \in \mathbb{Z}_{26}$; para encriptar, calculamos 16 + 3 = 19 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde: la T;
- la letra Y corresponde a $24 \in \mathbb{Z}_{26}$; para encriptar, calculamos 24 + 3 = 1 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde el resultado: la B.

Para desencriptar, reemplazamos cada letra por el elemento correspondiente $y \in \mathbb{Z}_{26}$ y calculamos:

$$\mathbf{d}(y) = y - 3 \quad \text{en } \mathbb{Z}_{26}$$

Por ejemplo, para desencriptar la letra C, que corresponde al elemento $2 \in \mathbb{Z}_{26}$, calculamos 2 - 3 = 25 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde: la Z.

Es fácil generar nuevos métodos de encriptación que funcionen de esta manera, observando que **e** y **d** no son otra cosa que una función biyectiva $\mathbf{e} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ y su inversa $\mathbf{d} = \mathbf{e}^{-1}$. Por ejemplo, podríamos tomar $\mathbf{e}(x) = 3 \cdot x + 4$ y $\mathbf{d}(y) = 9 \cdot y + 16$.

El inconveniente de los métodos de encriptación como éste, en los que cada letra se reemplaza siempre por el mismo símbolo, es que son fácilmente vulnerables. Dado un texto encriptado de esta manera, si se analiza la frecuencia con que aparecen los distintos caracteres es posible descubrir qué letras representan (por ejemplo, las vocales A y E aparecen con mucha frecuencia en un texto; lo mismo ocurre con consonantes como la S o la T).

Por este motivo, para aplicaciones en las que la seguridad es muy importante, se utilizan otros métodos más sofisticados. En lo que sigue, introduciremos el *algoritmo RSA*, ideado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Este procedimiento hace uso de dos claves: una *clave pública*, que puede ser conocida por todos y se utiliza para encriptar, y una *clave privada*, que sólo debe conocer quien recibirá el mensaje, y que se usa para desencriptar. Al igual que el ejemplo básico que vimos antes, el algoritmo RSA se basa en cálculos de aritmética modular, en este caso, potenciación en lugar de suma.

Supongamos que Andrea le va a enviar un mensaje a Belén. Para armar las claves, Belén procede como sigue:

- genera dos primos grandes al azar $p \neq q$, aproximadamente del mismo tamaño;
- calcula $n = p \cdot q$ y $\varphi(n) = (p - 1) \cdot (q - 1)$;
- elige un entero e tal que:

$$1 < e < \varphi(n) \quad \text{y} \quad mcd(e, \varphi(n)) = 1$$

El par (*e, n*) es la clave pública que Belén da a conocer.

- calcula el inverso de *e* en $\mathbb{Z}_{\varphi(n)}$, es decir, obtiene el único *d* con:

$$1 < d < \varphi(n) \quad \text{y} \quad e \cdot d \equiv 1 \pmod{\varphi(n)}$$

El par (*d, n*) es la clave privada que Belén guarda en secreto.

Ahora, para mandar el mensaje, Andrea lo representa por un número *m* con $1 \leq m \leq n - 1$ y coprimo con *n* (si el mensaje es largo, lo separa en partes y lo representa por varios números), y luego lo encripta usando la clave pública de Belén:

$$\mathbf{e}(m) = m^e \quad \text{en } \mathbb{Z}_n$$

Finalmente, envía el resultado $c = \mathbf{e}(m)$ a Belén.

Belén recibe *c* y lo desencripta usando la clave privada que sólo ella conoce:

$$\mathbf{d}(c) = c^d \quad \text{en } \mathbb{Z}_n$$

Ejemplo. Supongamos que Andrea quiere mandarle el mensaje $m = 87$ a Belén. En primer lugar, Belén genera las claves:

- elige $p = 11$, $q = 17$;
- calcula $n = 11 \cdot 17 = 187$ y $\varphi(n) = 10 \cdot 16 = 160$;
- elige un entero *e* tal que $1 < e < 160$ y $mcd(e, 160) = 1$, por ejemplo $e = 7$. Hace pública la clave (7, 187);
- busca el inverso de $e = 7$ en $\mathbb{Z}_{160}$, es decir, resuelve:

$$7 \cdot d \equiv 1 \pmod{160}$$

obteniendo $d = 23$ (ya que $7 \cdot 23 = 161 \equiv 1 \pmod{160}$). Entonces (23, 187) es la clave que Belén se guarda para desencriptar el mensaje de Andrea.

Una vez que tiene la clave $(e, n) = (7, 187)$, Andrea encripta su mensaje $m = 87$ calculando:

$$m^e = 87^7 \quad \text{en } \mathbb{Z}_{187}$$

Para esto, haciendo las cuentas en $\mathbb{Z}_{187}$, calcula:

$$87^2 = 7.569 = 89$$
$$87^4 = (87^2)^2 = 89^2 = 7.921 = 67$$
$$87^7 = 87^{1+2+4} = 87^1 \cdot 87^2 \cdot 87^4 = 87 \cdot 89 \cdot 67 = 43$$

Envía entonces $\mathbf{e}(87) = 43$.

Finalmente, Belén desencripta la información recibida usando su clave privada $(d, n) = (23, 187)$, nuevamente calculando en $\mathbb{Z}_{187}$:

$$\begin{aligned}
&43^2 = 1.849 = 166\\
&43^4 = (43^2)^2 = 166^2 = 27.556 = 67\\
&43^8 = (43^4)^2 = 67^2 = 4.489 = 1\\
&43^{16} = (43^8)^2 = 1^2 = 1\\
&43^{23} = 11^{16+4+2+1} = 11^{16} \cdot 11^4 \cdot 11^2 \cdot 11 = 1 \cdot 67 \cdot 166 \cdot 43 = 87
\end{aligned}$$

Obtiene de esta manera, $\mathbf{d}(43) = 87$, que es el mensaje original que Andrea quería enviarle.

Veamos que en cualquier caso, si Belén recibe c, entonces $\mathbf{d}(c) = m$, el mensaje original. Es decir, Belén siempre descifra correctamente el mensaje. Recordando que $c = \mathbf{e}(m)$, esto es equivalente a verificar que:

$$\mathbf{d}(\mathbf{e}(m)) = m$$

Ahora bien, $\mathbf{d}(\mathbf{e}(m)) = (\mathbf{e}(m))^d = (m^e)^d = m^{e \cdot d}$ en $\mathbb{Z}_n$; con lo cual, debemos ver que:

$$m^{e \cdot d} = m \text{ en } \mathbb{Z}_n$$

o equivalentemente, que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

Para esto utilizaremos el pequeño teorema de Fermat. En primer lugar, recordemos que como $n = p \cdot q$ con p y q primos distintos (y por lo tanto, enteros coprimos), vale que:

$$m^{e \cdot d} \equiv m \pmod{n} \iff \begin{cases} m^{e \cdot d} \equiv m \pmod{p} \\ m^{e \cdot d} \equiv m \pmod{q} \end{cases}$$

La elección de las claves d y e se hizo de manera que $e \cdot d \equiv 1 \pmod{\varphi(n)}$, donde $\varphi(n) = (p - 1) \cdot (q - 1)$. Entonces, existe $k \in \mathbb{Z}$ tal que $e \cdot d = 1 + (p - 1) \cdot (q - 1) \cdot k$, y, por lo tanto:

$$m^{e \cdot d} = m^{1 + (p-1) \cdot (q-1) \cdot k} = m \cdot (m^{p-1})^{(q-1) \cdot k}$$

Mirando ahora módulo p y teniendo en cuenta que, por el pequeño teorema de Fermat, vale $m^{p-1} \equiv 1 \pmod{p}$ (observar que p no divide a m, ya que $(m : n) = 1$), resulta que $m^{e \cdot d} \equiv m \pmod{p}$. De la misma manera, $m^{e \cdot d} \equiv m \pmod{q}$. En consecuencia, tenemos que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

¿Por qué es difícil descifrar el mensaje para alguien que intercepta el envío de Andrea? Observemos que para hallar m a partir de $c = m^e$ es suficiente conocer d (así es como Belén descifrará el mensaje). Pero para calcular d, lo que se hizo fue buscar el inverso de e módulo $\varphi(n)$. Esto es fácil de hacer conociendo $\varphi(n)$, pero quien intercepte el mensaje, lo que conoce es la clave pública (e, n), es decir, conoce n, pero no $\varphi(n)$. Nuevamente, $\varphi(n) = (p - 1) \cdot (q - 1)$ es fácil de calcular una vez que conocemos p y q, es decir, una vez que factorizamos n. Y aquí está el problema: *factorizar números naturales grandes es difícil*. Por difícil entendemos que requiere de *mucho* tiempo: se cree que la cantidad de tiempo necesaria para factorizar un número natural crece casi exponencialmente a medida que

aumenta el tamaño de n. Por este motivo, en la actualidad se utilizan números de más de 300 dígitos en el algoritmo RSA.

No está probado que para ser capaz de desencriptar mensajes (es decir, recuperar m conociendo $c = m^e$ en $\mathbb{Z}_n$ y la clave pública (e, n)) sea necesario conocer la factorización de $n = p \cdot q$. Sin embargo, hasta el momento, no han surgido alternativas más eficientes y, más aún, existe un método probabilístico para factorizar $n = p \cdot q$ basado en poder descifrar mensajes de RSA. Por todo esto, el algoritmo RSA es uno de los métodos más utilizados en la actualidad en las aplicaciones donde realmente es necesario transmitir información de manera segura; de hecho, se usa a diario en Internet cuando se visita una página segura que requiere una clave para ingresar (como la de un banco).

4. Números racionales

Los alumnos Juan y Leandro de la Escuela 314 van a veranear a la costa atlántica. Una mañana deciden participar de un torneo de beach voley en el cual no tienen un buen desempeño. Por esto, les dan como premio consuelo un sandwich de milanesa para ambos. ¿Cómo hacen para repartir el premio entre los dos?

La respuesta resulta bastante simple si estamos acostumbrados a trabajar con números. Deberían tomar medio sandwich cada uno, pero ¿qué quiere decir la mitad?, ¿qué representa el número 1/2 ?

En el primer capítulo estudiamos los números naturales y vimos aplicaciones de los mismos a distintos problemas. En el segundo capítulo vimos la utilidad que presenta agregar al conjunto de los números naturales un elemento neutro (el cero) y un inverso aditivo por cada número natural y obtuvimos el conjunto de números enteros. Como el conjunto de números naturales tiene dos operaciones importantes, podemos tratar de agregar inversos para el producto.

Si comenzamos con los números enteros y estudiamos el producto en este conjunto nos encontramos con un problema importante: multiplicar por cero mata a todos los elementos. Así:

$$\begin{aligned} 0 \cdot 1 &= 0 \\ 0 \cdot 2 &= 0 \\ &\vdots \end{aligned}$$

Esto hace que, si queremos agrandar el conjunto de números enteros de forma tal que todo número tenga inverso, no vamos a poder hacerlo. Esto es porque el cero no puede tener inverso si queremos que el conjunto construido siga teniendo las propiedades que tiene el conjunto de números enteros, (a saber, que sea un grupo para la suma, y que valga la propiedad distributiva con respecto al producto). A pesar de parecer muy intuitivo que el cero no puede tener inverso, a veces la intuición nos falla, con lo cual precisamos dar una demostración de tal afirmación. Supongamos que agregamos un símbolo ♠ que sirve como inverso multiplicativo del cero, o sea:

$$0 \cdot \spadesuit = 1 \text{ y } \spadesuit \cdot 0 = 1$$

Usando la propiedad asociativa para el producto tenemos que:

$$\begin{aligned} 1 &= 0 \cdot \spadesuit \\ &= (2 \cdot 0) \cdot \spadesuit \\ &= 2 \cdot (0 \cdot \spadesuit) \\ &= 2 \cdot 1 \\ &= 2. \end{aligned}$$

Esto es una contradicción, dado que el número natural 1 y el número natural 2 son distintos.

Como no hay manera de construir un conjunto que contenga los enteros y en el cual el número cero tenga inverso multiplicativo, tratemos de agrandar el conjunto de números enteros de manera tal que en el conjunto construido todos los números enteros, salvo el cero, tengan inverso multiplicativo. La manera intuitiva de hacerlo es considerar fracciones, esto es cocientes de la forma *n/d* donde *n* y *d* son enteros y *d* no es cero (dado que el cero no puede tener inverso). En tal expresión, al número *n* se lo llama numerador y al número *d* se lo llama denominador de la fracción.

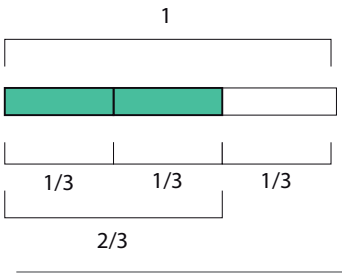


Figura 1. *El número 2/3.*

Tenemos una buena interpretación de las fracciones, la fracción 1/*d* representa tomar el elemento unidad 1 y partirlo en *d* pedazos iguales, como en el ejemplo del sandwich de milanesa. Siguiendo la definición de los números naturales, si *n* es positivo, la fracción *n/d* representa tomar *n* veces la fracción 1/*d*. La figura 1 muestra la manera de interpretar al número 2/3.

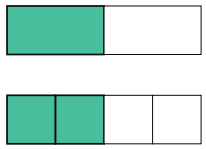


Figura 2. *Igualdad entre 1/2 y 2/4.*

Si nos detenemos a jugar con las fracciones, vemos que hay un problema en la definición que dimos. La fracción 1/2 representa tomar la mitad de la unidad, y la fracción 2/4 representa tomar dos veces la cuarta parte de la unidad. A pesar de que son dos fracciones distintas, ¡representan la misma cantidad!, como puede observarse en la figura 2.

A pesar de que la definición formal de número racional la daremos más adelante, los números racionales representan cantidades. Es por esto que la idea de que un número racional es una fracción no es del todo correcta, porque fracciones distintas pueden representar el mismo número racional. En la siguiente sección veremos cómo solucionar este problema, pero por ahora quedémonos con la idea de que a cada fracción le podemos asociar un número racional, aunque distintas fracciones pueden representar lo mismo.

Consideremos el conjunto de fracciones *n/d* con *n* un número entero y *d* un número entero no nulo. Podemos ver al conjunto de números enteros como un subconjunto del conjunto de fracciones, donde $2 = \frac{2}{1}$, $-1 = \frac{-1}{1}$, etc. Dado que sabemos sumar y multiplicar números enteros, nos gustaría hacer lo mismo con las fracciones. ¿Cómo multiplicamos 1/2 con 1/2 ?

El producto de números naturales se basa en la idea de tomar varias veces la misma cantidad. Así, multiplicar $2 \cdot 3$ representa tomar dos veces el número 3. Pensando que las fracciones representan tomar una cierta cantidad de una fracción del elemento unidad, multiplicar 1/2 con 1/2 representa tomar la mitad del elemento unidad 1 y a esto tenemos que tomarle la mitad nuevamente. Entonces, lo que queda será la cuarta parte de la unidad, con lo cual es natural definir el producto: $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Más generalmente, el producto de dos fracciones *a/b* y *c/d* lo definimos como:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Ejercicio 4.1. Verificar que el producto de números naturales adentro del conjunto de fracciones coincide con el producto usual.

Juan y Leandro, no contentos con el premio consuelo que les dieron por la mañana en el torneo de beach voley, deciden participar por la tarde en un torneo de tejos organizado en el mismo balneario. Como su desempeño fue otra vez bastante pobre, recibieron otro sandwich de milanesa. ¿Cuántos sandwiches de milanesa recibió cada uno?

Sabemos que ganaron 1/2 sandwich por la mañana y 1/2 sandwich por la tarde, con lo cual la respuesta esperada es que cada uno recibió un sandwich. Dicho de otro modo:

$$\frac{1}{2} + \frac{1}{2} = 1$$

La pregunta natural, es ¿cómo hacer para sumar dos fracciones cualesquiera?

Podemos deducirlo pensando las fracciones como partes de una unidad. Supongamos que queremos sumar las fracciones 1/3 y 1/2, ¿cuánto da?

El problema que tenemos es que estamos sumando partes del elemento unidad que están expresadas en escalas distintas. Consideremos el siguiente problema para entender qué está pasando: si caminamos dos kilómetros por la mañana y tres cuadras por la tarde (asumiendo que las cuadras tienen exactamente 100 metros cada una), ¿cuánto caminamos en todo el día?

Para poder dar una respuesta debemos usar la misma escala de distancia en ambos datos, ya sean cuadras, metros, etc. Si pensamos en cuadras, el resultado es fácil, porque caminamos 20 cuadras por la mañana y 3 por la tarde, en total caminamos 23 cuadras.

Al sumar fracciones pasa exactamente lo mismo, para poder sumar dos fracciones debemos tener los números en la misma escala. En nuestro problema queremos sumar 1/3 con 1/2, que dan escalas distintas. Si recordamos lo que dijimos antes de que las fracciones no tienen una representación única, podemos decir que da lo mismo 1/3 que 2/6 y 1/2 que 3/6. Al expresar los números en la misma escala sumar es fácil, así:

$$\begin{aligned} \frac{1}{3} + \frac{1}{2} &= \frac{2}{6} + \frac{3}{6} \\ &= \frac{5}{6} \end{aligned}$$

Más generalmente, si $\frac{a}{b}$ y $\frac{c}{d}$ son fracciones, podemos definir su suma como:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{a \cdot d}{b \cdot d} + \frac{b \cdot c}{b \cdot d} \\ &= \frac{a \cdot d + b \cdot c}{b \cdot d} \end{aligned}$$

Queremos ver que la suma en el conjunto de números racionales es asociativa, conmutativa, tiene un elemento neutro y que todo elemento tiene inverso. Además, el producto en el

conjunto de número racionales quitando el cero satisface las mismas propiedades, y que vale la propiedad distributiva de la suma con respecto al producto. Para poder probar esto, primero necesitamos tener una definición correcta de los números racionales.

□ 1. Definición formal

Al comenzar el estudio de los números racionales, vimos que las fracciones resultaban muy útiles. El problema que tenemos es que distintas fracciones pueden representar lo mismo. Por ejemplo: la fracción 1/2 y la fracción 2/4 representan la misma cantidad. Podemos pensar el conjunto de fracciones como:

$$\{(n, d) \in \mathbb{Z} \times \mathbb{Z} \ : \ d \neq 0\}$$

donde el par (*n, d*) representa la fracción $\frac{n}{d}$. ¿Cómo sabemos si dos fracciones representan la misma cantidad?

Si dos fracciones $\frac{a}{b}$ y $\frac{c}{d}$ representan la misma cantidad, vamos a escribir $\frac{a}{b} \sim \frac{c}{d}$.

Es fácil convencerse de que las fracciones 1/2 y 2/4 representan la misma cantidad, porque si partimos el elemento unidad en 4 y tomamos dos pedazos, terminamos tomando la mitad del elemento unidad. De igual modo, es claro que las fracciones 1/2 y 3/6 también representan la misma cantidad. Pero si nos dan las fracciones 2/4 y 3/6, a pesar de que representan la misma cantidad, no es tan claro el porqué. Nuevamente, tenemos el problema que las proporciones que consideramos no son las mismas, en un caso partimos la unidad en 6 y en el otro en 4.

Asumamos el siguiente principio: si $p \in \mathbb{N}$, las fracciones $\frac{n}{d}$ y $\frac{p \cdot n}{p \cdot d}$ representan la misma cantidad. Esto es bastante intuitivo, dado que lo que estamos haciendo es a cada parte *d*-ésima de la unidad la partimos en *p* pedacitos, y tomamos todos ellos.

Esto nos alcanza para determinar si dos fracciones $\frac{a}{b}$ y $\frac{c}{d}$ representan la misma cantidad o no. Simplemente, tomamos una escala que sirva para las dos (como hicimos al sumar fracciones). El denominador natural para considerar es $b \cdot d$, aunque el mínimo común múltiplo de *b* y *d* también sirve y, en varios casos, es más útil.

Ahora:
$$\frac{a}{b} \sim \frac{a \cdot d}{b \cdot d} \qquad \text{y} \qquad \frac{c}{d} \sim \frac{b \cdot c}{b \cdot d}$$

Pero las fracciones $\frac{a \cdot d}{b \cdot d}$ y $\frac{b \cdot c}{b \cdot d}$ representan el mismo número racional solamente cuando $a \cdot d = b \cdot c$. En conclusión, probamos que:

$$\frac{a}{b} \sim \frac{c}{d} \qquad \text{si y sólo si} \qquad a \cdot d = b \cdot c \tag{4}$$

Luego, en el conjunto $\{(n, d) \in \mathbb{Z} \times \mathbb{Z} : d \neq 0\}$ definimos la siguiente relación: decimos que el par (a, b) está relacionado con el par (c, d) (y escribimos $(a, b) \sim (c, d)$) solamente cuando $a \cdot d = b \cdot c$.

Veamos que la relación que acabamos de definir es una relación de equivalencia:

- **Reflexiva**: por definición, $(n, d) \sim (n, d)$ si $n \cdot d = d \cdot n$, lo que es cierto porque el producto es conmutativo.
- **Simétrica**: Si $(a, b) \sim (c, d)$, ¿vale que $(c, d) \sim (a, b)$? Por definición:

  $$(a, b) \sim (c, d) \text{ si y sólo si } a \cdot d = b \cdot c$$
  $$(c, d) \sim (a, b) \text{ si y sólo si } c \cdot b = d \cdot a$$

  Es claro que si $a \cdot d = b \cdot c$, entonces $c \cdot b = d \cdot a$ por ser conmutativo el producto de números enteros.
- **Transitiva**: Si $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, ¿vale que $(a, b) \sim (e, f)$? Por definición:

  $$(a, b) \sim (c, d) \text{ si y sólo si } a \cdot d = b \cdot c$$
  $$(c, d) \sim (e, f) \text{ si y sólo si } c \cdot f = d \cdot e$$
  $$(a, b) \sim (e, f) \text{ si y sólo si } a \cdot f = b \cdot e$$

  El dato es que valen las igualdades:

  $$a \cdot d = b \cdot c$$
  $$c \cdot f = d \cdot e$$

  Si multiplicamos la primera ecuación por f (que es $\neq 0$) y la segunda por b (que también es $\neq 0$), tenemos que:

  $$a \cdot d \cdot f = b \cdot c \cdot f$$
  $$b \cdot c \cdot f = b \cdot d \cdot e$$

  Luego: $a \cdot d \cdot f = b \cdot d \cdot e$, y como d es no nulo tenemos que $a \cdot f = b \cdot e$, o sea $(a, b) \sim (e, f)$.

Como vimos en el Capítulo 0, una relación de equivalencia en un conjunto parte al mismo en clases de equivalencia. Luego, definimos el **conjunto $\mathbb{Q}$ de números racionales** como el conjunto de clases de equivalencia del conjunto de fracciones por la relación $\sim$, o sea:

$$\mathbb{Q} = \{(n, d) \in \mathbb{Z} \times \mathbb{Z} : d \neq 0\}/\sim$$

Dentro de todas las fracciones que representan el mismo número, hay una que se destaca sobre las otras. Cuando vamos a comprar al supermercado pedimos medio kilogramo de pan, y no dos cuartos de kilogramo. Elegimos la fracción 1/2 por sobre la fracción 2/4 por tener denominador lo más chico posible. Esto hace que tengamos que partir la unidad lo menos posible.

Decimos que la fracción $\frac{a}{b}$ es **irreducible** si b es positivo y $mcd(a, b) = 1$.

¿Será cierto que toda fracción es equivalente a una única fracción irreducible?

La respuesta es *sí*, pero debemos demostrar este hecho formalmente. La mejor manera de demostrarlo es dar el algoritmo que lleva una fracción a su irreducible.

Supongamos que queremos hallar la fracción irreducible equivalente a la fracción 15/21, ¿qué hacemos?

Lo primero que uno se debe preguntar es si esta fracción ya es irreducible o no. Cumple que el denominador es positivo, con lo cual la primera condición se satisface. Luego debemos calcular *mcd* (15, 21). Si factorizamos ambos números, tenemos que $15 = 3 \cdot 5$ y $21 = 3 \cdot 7$, con lo cual $mcd(15, 21) = 3$.

Esto no sólo nos dice que la fracción no es irreducible, sino que además nos está diciendo que tanto el numerador como el denominador son múltiplos de 3. Si dividimos a ambos por 3, obtenemos la fracción 5/7 que es equivalente a 15/21 y es irreducible por ser $mcd(5, 7) = 1$. Luego, nuestro algoritmo de reducción es bastante simple: si b es positivo, la manera de obtener una fracción irreducible es:

$$\frac{a}{b} \longrightarrow \frac{a/\, mcd\,(a,b)}{b/\, mcd\,(a,b)}$$

Así, $\frac{35}{14} \sim \frac{5}{2}$, $\frac{18}{24} \sim \frac{3}{4}$, etc. ¿Qué pasa si b es negativo?

Este caso también es bastante conocido. Al pensar en números racionales, es normal considerar que 1/-2 representa lo mismo que -1/2 . Efectivamente ambas fracciones son equivalentes. En general, $\frac{a}{-b} \sim \frac{-a}{b}$. Luego, si el denominador es negativo, cambiando el signo del numerador y el denominador obtenemos una fracción equivalente, pero ahora con denominador positivo. Así, $\frac{33}{-121} \sim \frac{-3}{11}$.

Las fracciones irreducibles satisfacen dos propiedades importantes:

- toda fracción es equivalente a una única fracción irreducible;
- si $\frac{a}{b}$ es irreducible y $\frac{c}{d} \sim \frac{a}{b}$, entonces c y d son un múltiplo entero de a y de b, o sea hay un número entero m tal que $c = a \cdot m$ y $d = b \cdot m$.

Para ver la primera propiedad, ya dimos un algoritmo que a una fracción le asocia una fracción irreducible, con lo cual sabemos que toda fracción es equivalente a una fracción irreducible. Lo que falta ver es que hay una sola. Supongamos que tenemos dos fracciones irreducibles $\frac{a}{b}$ y $\frac{c}{d}$ equivalentes. Por definición esto quiere decir que:

$$ad = bc \tag{5}$$

En particular, d divide a bc. Como $mcd(c, d) = 1$ (por ser $\frac{c}{d}$ irreducible), tenemos que d divide a b. Análogamente, b divide a ad y es coprimo con a con lo cual b divide a d. Vimos que si dos números se dividen mutuamente, entonces son iguales o difieren en un signo. Al ser ambos positivos, tenemos que $b = d$. Luego (5) dice que $a = c$, porque b (y d) es $\neq 0$.

Ejercicio 4.2. Demostrar la segunda propiedad de las fracciones irreducibles.

Notemos la importancia de la primera propiedad. Nos dice que todo número racional se puede representar de forma única como una fracción irreducible. De ahí la importancia de las fracciones irreducibles, ellas son como los números racionales, ¡y sin ambigüedad!

Ahora que tenemos bien definidos a los números racionales, se nos presentan algunos problemas interesantes que a simple vista pasan desapercibidos. Por ejemplo:

$$\frac{1}{2} \sim \frac{2}{4} \quad \text{y} \quad \frac{1}{3} \sim \frac{2}{6}$$

o sea las primeras dos fracciones y las últimas dos representan el mismo número racional. ¿Cómo sumamos el número racional representado por 1/2 con el número racional representado por 1/3? Veamos:

$$\begin{cases} \frac{1}{2} + \frac{1}{3} & = \frac{2+3}{6} & = \frac{5}{6} \\ \frac{1}{2} + \frac{2}{6} & = \frac{6+4}{12} & = \frac{10}{12} \\ \frac{2}{4} + \frac{1}{3} & = \frac{6+4}{12} & = \frac{10}{12} \\ \frac{2}{4} + \frac{2}{6} & = \frac{12+8}{24} & = \frac{20}{24} \end{cases}$$

A pesar de que las fracciones que obtenemos son distintas, todas representan el mismo número racional, ya que:

$$5 \cdot 12 = 60 = 6 \cdot 10 \quad \text{con lo cual} \quad \frac{5}{6} \sim \frac{10}{12}$$

$$10 \cdot 24 = 240 = 12 \cdot 20 \quad \text{con lo cual} \quad \frac{10}{12} \sim \frac{20}{24}$$

Esta verificación no es suficiente, ya que hay infinitas fracciones que representan el mismo número racional. En este ejemplo:

$$\frac{1}{2} \sim \frac{2}{4} \sim \frac{3}{6} \sim \frac{4}{8} \sim \dots$$

y:

$$\frac{1}{3} \sim \frac{2}{6} \sim \frac{3}{9} \sim \frac{4}{12} \sim \dots$$

¿Será cierto que si sumamos una fracción cualquiera del primer renglón con una fracción cualquiera del segundo obtenemos fracciones equivalentes? Si este fuera el caso, entonces definimos la suma de la clase de la fracción 1/2 con la clase de la fracción $1/3$ como la clase de la fracción 5/6.

Como 1/2 es irreducible, las fracciones equivalentes a ella son de la forma $\frac{r}{2 \cdot r}$ con $r \in \mathbb{Z}$. Lo mismo sucede con 1/3, las fracciones equivalentes con ella son de la forma $\frac{s}{3 \cdot s}$, con $s \in \mathbb{Z}$. La suma de dos de ellas es:

$$\frac{r}{2 \cdot r} + \frac{s}{3 \cdot s} = \frac{r \cdot 3 \cdot s + s \cdot 2 \cdot r}{2 \cdot r \cdot 3 \cdot s}$$

$$= \frac{5 \cdot r \cdot s}{6 \cdot r \cdot s}$$

Como $\frac{5 \cdot r \cdot s}{6 \cdot r \cdot s} \sim \frac{5}{6}$ vemos que el resultado es siempre una fracción equivalente a 5/6. Resumiendo, hemos probado que definir la suma de 1/2 o cualquier fracción equivalente con 1/3 o cualquier fracción equivalente da fracciones equivalentes a 5/6.

El mismo argumento nos sirve para definir la suma de dos números racionales cualesquiera: si $\frac{a}{b}$ y $\frac{c}{d}$ representan dos números racionales, el número racional representado por la fracción $\frac{a\cdot d+b\cdot c}{b\cdot d}$ no depende de la fracción elegida en cada clase.

Dado que este punto es crucial para la suma de números racionales, veamos cómo se demuestra: supongamos que tenemos dos fracciones $\frac{\tilde{a}}{\tilde{b}}$ y $\frac{\tilde{c}}{\tilde{d}}$ equivalentes a $\frac{a}{b}$ y $\frac{c}{d}$ respectivamente. O sea:

$$a \cdot \tilde{b} = \tilde{a} \cdot b \tag{6}$$

$$c \cdot \tilde{d} = \tilde{c} \cdot d \tag{7}$$

Queremos ver que las fracciones $\frac{a\cdot d+b\cdot c}{b\cdot d}$ y $\frac{\tilde{a}\cdot\tilde{d}+\tilde{b}\cdot\tilde{c}}{\tilde{b}\cdot\tilde{d}}$ son equivalentes, o sea que:

$$\tilde{b}\cdot\tilde{d}\cdot(a\cdot d+b\cdot c) = b\cdot d\cdot(\tilde{a}\cdot\tilde{d}+\tilde{b}\cdot\tilde{c})$$

Haciendo las distributivas, lo que queremos ver es que:

$$a\cdot\tilde{b}\cdot d\cdot\tilde{d}+b\cdot\tilde{b}\cdot c\cdot\tilde{d} = \tilde{a}\cdot b\cdot d\cdot\tilde{d}+b\cdot\tilde{b}\cdot\tilde{c}\cdot d$$

Esta igualdad se deduce de multiplicar (6) por $d\cdot\tilde{d}$, (7) por $b\cdot\tilde{b}$ y sumarlas.

Ejercicio 4.3. Demostrar que si las fracciones $\frac{a}{b}$ y $\frac{c}{d}$ son equivalentes a las fracciones $\frac{\tilde{a}}{\tilde{b}}$ y $\frac{\tilde{c}}{\tilde{d}}$ respectivamente, entonces la fracción $\frac{a\cdot c}{b\cdot d}$ es equivalente a la fracción $\frac{\tilde{a}\cdot\tilde{c}}{\tilde{b}\cdot\tilde{d}}$

Luego la suma y producto usual de números racionales (haciéndolo con cualquier fracción que los represente) tiene sentido.

□ 2. Propiedades

La suma y el producto de números racionales son operaciones asociativas y conmutativas. El 1 es el neutro para el producto y el 0 es el neutro para la suma. La suma satisface que todo elemento tiene inverso, siendo el inverso del número racional representado por la fracción $\frac{a}{b}$ el número racional representado por la fracción $-\frac{a}{b}$. Además, todo número no nulo tiene inverso para el producto. Si $\frac{a}{b}$ representa un número racional no nulo, $a \neq 0$. Luego la fracción $\frac{b}{a}$ también representa un número racional, y por cómo definimos el producto, es claro que:

$$\frac{a}{b}\cdot\frac{b}{a} = 1$$

También vale la propiedad distributiva. Para toda terna de números racionales $\frac{a}{b}$, $\frac{c}{d}$, $\frac{e}{f}$ vale:

$$\begin{aligned}\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}\\ \left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f} &= \frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}\end{aligned}$$

Recordemos que un conjunto con dos operaciones que satisfacen todas las propiedades enunciadas anteriormente se llama un *cuerpo*. Por eso se suele hablar del *cuerpo de números racionales* más que del conjunto de números racionales.

Consideremos el siguiente problema: en una reunión de ex-alumnos de la Escuela 314, dos viejos conocidos rememoraban sus grandes logros de la época de estudiantes. En el medio de la conversación surgió la duda de quién había conseguido comer más cantidad de pizza en una sola noche. Uno de ellos afirmó haber comido 19 porciones en la pizzería del barrio, aclarando que cada pizza traía 8 porciones. El otro involucrado afirmó haberse comido 14 porciones en una pizzería donde cada pizza traía simplemente 6 porciones. Contando las anécdotas, coincidieron en que el tamaño total de cada pizza era el mismo en las dos pizzerías, cambiando simplemente el número de porciones. ¿Quién comió más?

Si la primera persona comió 19 porciones de pizza y cada pizza traía 8 porciones, entonces comió 19/8 de pizza. Con el mismo razonamiento vemos que la segunda persona comió 14/6 de pizza. La pregunta es entonces, ¿cuál de estos dos números es más grande, 19/8 o 14/6?

La forma de comparar números racionales es muy similar a cómo definimos la suma de ellos. Es bastante claro que si queremos comparar dos números racionales dados por fracciones **con el mismo denominador**, sólo tenemos que comparar los numeradores como números enteros. Así, 2/4 es menor que 3/4. Si los denominadores de las fracciones consideradas no son iguales, podemos encontrar un par de fracciones que representen el mismo número racional, y cuyos denominadores sí sean los mismos. Así, por ejemplo, si queremos comparar las fracciones $\frac{a}{b}$ y $\frac{c}{d}$ donde b y d son positivos, tenemos:

$$\frac{a}{b} \sim \frac{a \cdot d}{b \cdot d} \qquad \text{y} \qquad \frac{c}{d} \sim \frac{b \cdot c}{b \cdot d}$$

Decimos que $\frac{a}{b}$ **es menor** que $\frac{c}{d}$ (y escribimos $\frac{a}{b} < \frac{c}{d}$) si $a \cdot d < b \cdot c$.

Como queremos definir un orden en números racionales, debemos chequear que esta definición no depende de la fracción particular que elegimos para representar al número racional. Para simplificar la cuenta, supongamos que tenemos dos fracciones irreducibles $\frac{a}{b}$ y $\frac{c}{d}$ y dos fracciones cualesquiera $\frac{\tilde{a}}{\tilde{b}}$ y $\frac{\tilde{c}}{\tilde{d}}$ equivalentes a $\frac{a}{b}$ y $\frac{c}{d}$ respectivamente, con $\tilde{b}$ y $\tilde{d}$ positivos. Veamos que con la definición anterior es lo mismo pedir $\frac{a}{b} < \frac{c}{d}$ que pedir $\frac{\tilde{a}}{\tilde{b}} < \frac{\tilde{c}}{\tilde{d}}$.

Como $\frac{a}{b}$ es irreducible, al ser equivalente a $\frac{\tilde{a}}{\tilde{b}}$, existe un número entero r tal que:

$$\tilde{a} = a \cdot r \qquad \text{y} \qquad \tilde{b} = b \cdot r$$

Además, como b y $\tilde{b}$ son positivos, r es positivo también. De forma análoga, existe un entero positivo s tal que:

$$\tilde{c} = c \cdot s \qquad \text{y} \qquad \tilde{d} = d \cdot s$$

Por definición:

$$\begin{cases} \frac{a}{b} < \frac{c}{d} & \text{si vale que} \quad a \cdot d < b \cdot c \\ \frac{a \cdot r}{b \cdot r} < \frac{c \cdot s}{d \cdot s} & \text{si vale que} \quad a \cdot r \cdot d \cdot s < b \cdot r \cdot c \cdot \end{cases}$$

Como r y s son positivos, pedir que los números a, b, c, d satisfagan una desigualdad o la otra es lo mismo (multiplicar o dividir una desigualdad por un número positivo no la cambia).

De manera similar definimos las otras relaciones de orden (a saber >, ≤, ≥). Volviendo al problema de la pizza, queremos comparar las fracciones 19/8 y 14/6. Aunque la segunda fracción no es irreducible, al ser los denominadores positivos podemos aplicar la definición. Así, la primera persona comió más, dado que 19/8 > 14/6 porque 114 = 19 · 6 > 14 · 8 = 112.

Ejercicio 4.4. Probar las siguientes propiedades para números racionales:

- dadas fracciones $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2}$, con $\frac{a_1}{b_1} < \frac{c_1}{d_1}$ y $\frac{a_2}{b_2} < \frac{c_2}{d_2}$, vale que:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} < \frac{c_1}{d_1} + \frac{c_2}{d_2}$$

- dadas fracciones $\frac{a}{b}$, $\frac{c}{d}$, con $\frac{a}{b} < \frac{c}{d}$ y una fracción $\frac{e}{f}$ >0, vale que:

$$\frac{e}{f} \cdot \frac{a}{b} < \frac{e}{f} \cdot \frac{c}{d}$$

□ 3. Representación decimal de los números racionales

Representamos los números racionales como clases de equivalencia de fracciones. Hay otra manera de expresar un número racional, que a veces resulta muy útil y es la llamada **representación decimal**. Al estudiar los números enteros vimos que los podemos representar como una tira de números entre el 0 y el 9. Los números racionales tienen una representación parecida, pero la tira de números que los representa no tiene por qué ser finita, aunque sí tener un cierto período. Esto es que, a partir de un cierto lugar, comienza a repetirse indefinidamente.

Es importante observar que la expresión decimal de un número no es necesariamente única. Por ejemplo, los números 1 y $0,\overline{9}$ representan el mismo número racional, donde escribimos una barra arriba de una tira de números para indicar que en el desarrollo decimal del número esta expresión se repite una vez después de otra, infinitas veces. Veremos que ésta es la única ambigüedad que puede tener una expresión decimal.

¿Cómo representamos 1/2 en expresión decimal? La idea es copiar lo que hacemos con los números enteros. La escritura 1.986 es una notación para el número:

$$1.986 = 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0$$

O sea escribimos potencias de diez, y a cada potencia la multiplicamos por un número entre 0 y 9. Podemos tratar de hacer lo mismo para potencias negativas de diez, y marcar en la escritura (con una coma) el lugar a partir de donde comienzan las potencias negativas de 10.

Por ejemplo:

$$\begin{aligned} 1{,}21 &= 1 \cdot 10^0 + 2 \cdot 10^{-1} + 1 \cdot 10^{-2} \\ &= 1 + \frac{2}{10} + \frac{1}{100} \\ &= \frac{121}{100} \end{aligned}$$

Luego la expresión 1,21 representa el número racional $\frac{121}{100}$. De forma análoga, la expresión:

$$\begin{aligned} 0{,}5 &= 0 \cdot 10^0 + 5 \cdot 10^{-1} \\ &= \frac{0}{1} + \frac{5}{10} \\ &= \frac{5}{10} \sim \frac{1}{2} \end{aligned}$$

O sea la fracción $\frac{1}{2}$ se puede representar por la expresión 0,5.

Ejercicio 4.5. Representar por fracciones irreducibles los números racionales dados en expresión decimal 3,25; 4,3 y 3,14.

En estos ejemplo vimos cómo pasar de una escritura decimal a una fracción (en los casos más sencillos). ¿Qué escritura decimal le asociamos a una fracción?

Como vimos en la sección de números enteros, si tomamos dos números enteros a y b, con b no nulo y positivo, entonces existen un cociente q y un resto r, tales que:

$$a = q \cdot b + r \qquad \text{y} \qquad 0 \leq r < |b|$$

Esto nos permite escribir la fracción $\frac{a}{b}$ como:

$$\begin{aligned} \frac{a}{b} &= \frac{q \cdot b + r}{b} \\ &= \frac{q \cdot b}{b} + \frac{r}{b} \\ &= q + \frac{r}{b} \end{aligned}$$

y como $r < b$, la fracción $\frac{r}{b} < 1$. Así, todo número racional, se escribe como un número entero más un número racional entre 0 y 1. Por ejemplo:

$$\frac{3}{2} = 1 + \frac{1}{2}$$

Como $\frac{1}{2} < 1$, el número $\frac{3}{2}$ debe comenzar con un 1 su escritura decimal y sólo nos resta calcular qué viene después de la coma. A pesar de que ya vimos que $\frac{1}{2} = 0{,}5$, tratemos de deducir este resultado. Supongamos que $\frac{1}{2} = 0{,}x\ldots$, o sea que en la escritura decimal, el número $\frac{1}{2}$ comienza con el dígito x luego de la coma (que debe ser un número entre 0 y 9). Veamos cómo calculamos x.

Siguiendo con el ejemplo anterior, ¿qué pasa si multiplicamos el número 1,21 por 10? Si recordamos la definición del número 1,21, tenemos:

$$1{,}21 = 1 \cdot 10^0 + 2 \cdot 10^{-1} + 1 \cdot 10^{-2}$$

Luego:
$$\begin{aligned} 10 \cdot 1{,}21 &= 10 \cdot (1 \cdot 10^0 + 2 \cdot 10^{-1} + 1 \cdot 10^{-2}) \\ &= 1 \cdot 10^1 + 2 \cdot 10^0 + 1 \cdot 10^{-1} \\ &= 12{,}1 \end{aligned}$$

Ejercicio 4.6. Probar que multiplicar un número racional por 10 mueve la coma un lugar hacia la derecha en la expresión decimal del mismo.

Recordemos que queremos calcular el primer dígito de la expresión decimal de $\frac{1}{2}$ luego de la coma. Si $\frac{1}{2} = 0,x\ldots$, entonces:
$$\begin{aligned} 10 \cdot \frac{1}{2} &= 5 \\ &= x, \ldots . \end{aligned}$$

Luego $x = 5$ y hay un solo dígito no nulo en la expresión decimal de $\frac{1}{2}$, o sea:
$$\frac{1}{2} = 0{,}5 \qquad \text{y} \qquad \frac{3}{2} = 1{,}5$$

Sigamos el mismo razonamiento para calcular la expresión decimal de $\frac{1}{4}$. Como $0 < \frac{1}{4} < 1$, la expansión decimal de $\frac{1}{4}$ debe tener un cero a la izquierda de la coma, o sea:
$$\frac{1}{4} = 0, \ldots .$$

Llamemos x al primer dígito luego de la coma de su expresión decimal. Luego:
$$\begin{aligned} 10 \cdot \frac{1}{4} &= \frac{5}{2} \\ &= x, \ldots . \end{aligned} \tag{8}$$

Si calculamos el cociente y resto de dividir 5 por 2, tenemos que:
$$5 = 2 \cdot 2 + 1$$

con lo cual el número $\frac{5}{2} = 2 + \frac{1}{2}$. Ahora $0 < \frac{1}{2} < 1$. Luego $x = 2$, o sea $\frac{1}{4} = 0{,}2\ldots$.

¿Cómo calculamos el dígito que está a la derecha del 2? Hacemos exactamente lo mismo, si lo llamamos x, vale que:
$$\frac{1}{4} = 0{,}2x\ldots \qquad \text{con lo cual} \qquad \begin{aligned} 100 \cdot \frac{1}{4} &= 25 \\ &= 2x, \ldots . \end{aligned}$$

Luego $x = 5$ y $\frac{1}{4} = 0{,}25$.

Si miramos la ecuación (8), teníamos que:
$$10 \cdot \frac{1}{4} = 2 + \frac{1}{2}$$

como $\frac{1}{2} = 0{,}5$, de acá también se deduce que $10 \cdot \frac{1}{4} = 2{,}5$ con lo cual $\frac{1}{4} = 0{,}25$.

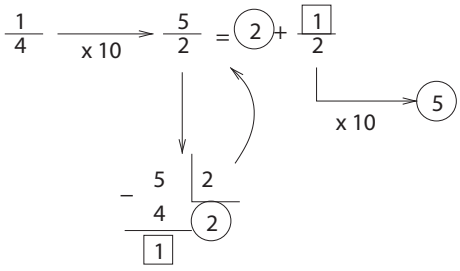


Figura 3. *Cálculo de la expresión decimal de 1/4.*

Podemos ver, gráficamente en la figura 3, lo que hicimos.

Para calcular la expresión decimal de una fracción $\frac{a}{b}$ basta considerar el caso en que a y b son positivos, dado que en caso contrario podemos considerar la fracción $|a|/|b|$ y agregar el signo correcto a la expresión decimal de esta fracción. El siguiente es un algoritmo para, dado un número racional expresado por una fracción $\frac{a}{b}$ (con a y b positivos), calcular su expresión decimal:

1. calcular el cociente y resto de la división de a por b. Llamemos q al cociente y r al resto;
2. si r es cero, terminar y mostrar q como respuesta. Caso contrario, poner q y una coma en lo que será la respuesta;
3. calcular el cociente y resto de dividir $10 \cdot r$ por b. Llamemos q al cociente y r al resto. Pegar q a la derecha de lo que será la respuesta;
4. si r es cero, terminar y mostrar la respuesta. Caso contrario, volver al paso 3.

Veamos cómo funciona el algoritmo calculando la expresión decimal de 31/25.

1. Calculamos cociente y resto de dividir 31 por 25:

$$31 = 1 \cdot 25 + 6$$

Así obtenemos que 31/25 = 1 + 6/25 = 1, ...

2. Multiplicamos 6 por 10 y calculamos el cociente y resto de dividir 60 por 25:

$$60 = 2 \cdot 25 + 10$$

Entonces el primer dígito decimal es 2, o sea 31/25 = 1,2 ....

3. Multiplicamos el resto 10 por 10 y calculamos el cociente y resto de dividirlo por 25. Así,

$$\begin{aligned} 10 \cdot 10 &= 100 \\ &= 4 \cdot 25 + 0 \end{aligned}$$

Como el resto es 0, terminamos, y la expresión decimal de 31/25 es 1,24.

Ejercicio 4.7. Calcular la expresión decimal del número racional 1/8.

Calculemos la expresión decimal del número racional 1/3. Usemos el algoritmo que dimos antes.

1. Calculamos el cociente y resto de dividir 1 por 3. El cociente es 0 y el resto es 1, con lo cual la expresión decimal comienza con 0.
2. Multiplicamos 1 por 10 y calculamos el cociente y resto de la división. Así:

$$10 = 3 \cdot 3 + 1$$

Luego el primer dígito luego de la coma es 3, 1/3 = 0,3....

3. Ahora debemos multiplicar el resto 1 por 10 y calcular el cociente y resto de dividir por 3. ¡Esto es repetir exactamente el último paso que hicimos! Es claro que continuar este proceso va a ser dividir infinitas veces 10 por 3 y agregar el cociente de esta división en la expresión decimal. O sea:

$$\begin{aligned}\frac{1}{3} &= 0{,}33333... \\ &= 0{,}\overline{3}\end{aligned}$$

En este ejemplo, la expresión decimal del número 1/3 no es finita. Lo que sucede es que se repite infinitamente el número 3 en dicha expresión.

¿Cómo entendemos que algunos números racionales tengan expresión finita y otros no? Lo que sucede es que los números con expresión finita son exactamente aquéllos donde el denominador de la fracción irreducible sólo posee potencias de 2 y de 5 en su factorización. Veamos esto con un ejemplo concreto. Si tenemos un número N con expresión decimal finita, después de la coma hay solamente finitos dígitos. Digamos:

$$N = 342{,}1572$$

Como multiplicar una expresión decimal por 10 mueve la coma un lugar a la derecha en dicha expresión, si movemos la coma 4 lugares tendremos el número entero 3.421.572. O sea multiplicando N por 10^4 obtenemos un número entero. Luego N se puede representar por la fracción:

$$\begin{aligned}N &= \frac{3.421.572}{10.000} \\ &= \frac{855.393}{2.500}\end{aligned}$$

La fracción 3.421.572/10.000 no es irreducible, pero satisface que la factorización de su denominador sólo tiene potencias de 2 y de 5. Luego, el denominador de la fracción irreducible (en este caso 2.500) es un divisor de 10^4 en cuyo caso en su factorización aparecen solamente potencias de 2 y 5 (aunque las potencias pueden ser menores que 4).

Esta idea que reflejamos en un ejemplo particular sirve para una expansión decimal cualquiera.

Ejercicio 4.8. Calcular las fracciones irreducibles que representen los números racionales 26,2914; 290,4377 y 946,17482.

Resta por ver la recíproca de la afirmación: si el denominador de la fracción irreducible de un número racional tiene solamente potencias de 2 y de 5 en su factorización, entonces la expresión decimal de dicho número es finita. Veamos nuevamente un ejemplo concreto para entender cómo probar esta afirmación. Miramos el número:

$$\begin{aligned}N &= \frac{1.979}{2^3 \cdot 5^4} \\ &= \frac{1.979}{5.000}\end{aligned}$$

Veamos la potencia de 2 y de 5 que aparecen en el denominador, y miremos la más grande. En nuestro ejemplo, la potencia más grande es 4, que aparece como exponente del número primo 5. Si multiplicamos a nuestro número N por 10^4, tenemos que el resultado es un número entero. Efectivamente, como $10^4 = 2^4 \cdot 5^4$, y tanto la potencia del primo 2 como la potencia del primo 5 en el denominador eran menores o iguales que 4, al multiplicar N por 10^4, vemos que el denominador se cancela. Así:

$$\begin{aligned} 10^4 \cdot \frac{1.979}{2^3 \cdot 5^4} &= 2^4 \cdot 5^4 \cdot \frac{1.979}{2^3 \cdot 5^4} \\ &= 2 \cdot 1\,979 \\ &= 3\,958 \end{aligned}$$

En conclusión, corriendo la coma 4 lugares hacia la derecha terminamos con un número entero con lo cual el número N no puede tener más que 4 dígitos después de la coma. El argumento para un número racional cualquiera es el mismo.

Ejercicio 4.9. Mirando la factorización del denominador de los siguientes números, decir cuántos dígitos tiene su expresión decimal, y calcularla explícitamente:

$$\frac{8.729}{2.000}, \frac{101}{2.500} \text{ y } \frac{19.283}{6.250}$$

Comenzamos diciendo que los números racionales tienen expresión decimal periódica, pero no es claro por qué debe pasar esto. Calculemos algunas expresiones decimales para entender la afirmación:

1. La expresión decimal de 1/11:

   - $1 = 11 \cdot 0 + 1$
   - $1 \cdot 10 = 10 = 11 \cdot 0 + 10$
   - $10 \cdot 10 = 100 = 11 \cdot 9 + 1$

   Como nos aparece nuevamente el 1 como resto, debe ser:

   $$\frac{1}{11} = 0,\overline{09}$$

   Observar que al calcular las divisiones, obtuvimos el conjunto de restos $\{1, 10\}$ que es un subconjunto de $\mathbb{Z}_{11}$ cerrado por multiplicación, ya que $10 \cdot 10 \equiv 1$ (mód 11). Además, el período de la expresión decimal tiene 2 cifras. Es claro que al obtener un resto por segunda vez, el desarrollo decimal comienza a repetirse.

2. La expresión decimal de 5/11:

   - $5 = 11 \cdot 0 + 5$
   - $5 \cdot 10 = 50 = 11 \cdot 4 + 6$
   - $6 \cdot 10 = 60 = 11 \cdot 5 + 5$

   Como nos aparece nuevamente el 5 como resto, debe ser:

   $$\frac{5}{11} = 0,\overline{45}$$

Notar que la expresión decimal es multiplicar por 5 la expresión decimal de 1/11.

3. La expresión de 1/7:

- $1 = 7 \cdot 0 + 1$
- $1 \cdot 10 = 10 = 7 \cdot 1 + 3$
- $3 \cdot 10 = 30 = 7 \cdot 4 + 2$
- $2 \cdot 10 = 20 = 7 \cdot 2 + 6$
- $6 \cdot 10 = 60 = 7 \cdot 8 + 4$
- $4 \cdot 10 = 40 = 7 \cdot 5 + 5$
- $5 \cdot 10 = 50 = 7 \cdot 7 + 1$

Como nos aparece nuevamente el 1 como resto, debe ser:

$$\frac{1}{7} = 0,\overline{142857}$$

Observar que al calcular las divisiones, obtuvimos el conjunto de restos {1, 3, 2, 6, 4, 5} que son todos los números no nulos de $\mathbb{Z}_7$ y el período de la expresión decimal tiene 6 cifras.

4. La expresión de 1/15:

- $1 = 15 \cdot 0 + 1$
- $1 \cdot 10 = 10 = 15 \cdot 0 + 10$
- $10 \cdot 10 = 100 = 15 \cdot 6 + 10$

Como nos aparece nuevamente el 10 como resto, debe ser:

$$\frac{1}{15} = 0,0\overline{6}$$

¿Por qué el período no comienza en el primer lugar como antes? El problema que tenemos es que aparece una potencia de 5 en el denominador. De la igualdad de números racionales:

$$\begin{aligned}\frac{1}{15} &= \frac{2}{30} \\ &= \frac{1}{10} \cdot \frac{2}{3}\end{aligned}$$

vemos que la expresión decimal de 1/15 es la expresión decimal de 2/3 = 0, $\overline{6}$ corriendo la coma un lugar a la izquierda.

Son justamente los números racionales cuyos denominadores en fracción irreducible son divisibles por 2 o por 5 aquellos donde el período no comienza necesariamente luego de la coma.

Veamos que todo número racional tiene una expresión decimal periódica y a la vez que toda expresión decimal periódica corresponde a la expresión de un número racional. Además, esta asociación es biyectiva, si identificamos las expresiones decimales de período $\overline{9}$ con la expresión obtenida sumándole una unidad al dígito anterior al período. Por ejemplo, 0,23$\overline{9}$ = 0,24.

Si $\frac{a}{b}$ es la fracción irreducible de un número racional con a y b positivos, el algoritmo para calcular la expresión decimal es dividir a por b y calcular el resto. Llamemos r_1 al primer resto y q_0 al primer cociente obtenidos en este proceso. El resto satisface $0 \le r_1 \le b-1$ (por definición de resto). Luego multiplicamos r_1 por 10 y volvemos a dividirlo por b. Llamemos r_2 a este segundo resto y q_1 al cociente. Continuando con el proceso, creamos una sucesión de restos $r_1, r_2, r_3, \ldots$ y una sucesión de cocientes $q_0, q_1, q_2, \ldots$, donde cada uno de los restos es un número entre 0 y $b-1$. Como el conjunto $\{0, 1, \ldots, b-1\}$ tiene b elementos, entre $r_1, r_2, \ldots r_{b+1}$ hay dos números iguales.

Para ilustrar la idea, supongamos que el resto r_2 es igual al resto r_5. Luego $10 \cdot r_2 = 10 \cdot r_5$. Al dividir por b, los restos de ambos números también son iguales. Así, $r_3 = r_6$. Análogamente, $r_4 = r_7$, etc. O sea la tira de restos r_2, r_3, r_4 se va a repetir siempre. A la vez los cocientes de dividir $10 \cdot r_2$ por b y $10 \cdot r_5$ por b también son los mismos, con lo cual $q_2 = q_5$, o sea el segundo y el quinto lugar de la expresión decimal coinciden. Repitiendo el argumento, vemos que en la expresión decimal se repite siempre la tira $q_2q_3q_4$, o sea:

$$\frac{a}{b} = q_0, q_1\overline{q_2q_3q_4}$$

Ejercicio 4.10. Mirar los ejemplos de los cálculos de expresión decimal anteriores, y comprobar que el período se da justamente entre los primeros restos que se repiten.

Ejercicio 4.11. Deducir del argumento dado anteriormente que la longitud del período de la fracción $\frac{a}{b}$ es a lo sumo b. Más aún, probar que en realidad el período es a lo sumo $b-1$.

El procedimiento para, dado un número en expresión decimal periódica, asociarle una fracción que lo represente, es más o menos conocido. Por ejemplo, al número:

$$0{,}23\overline{46981} \rightsquigarrow \frac{23}{100} + \frac{1}{100} \cdot \frac{46.981}{99.999}$$

o sea: primero escribimos 0,2346981 como 0,23+0,0046981, donde al último número (salvo correr la coma) el período le comienza en el primer dígito. Escribimos 0,23 como fracción de la manera descrita anteriormente, y a un número **periódico puro** (esto es que el período comienza justo después de la coma) le asociamos la fracción cuyo numerador es el período, y cuyo denominador es poner tantos nueves como dígitos tiene el período.

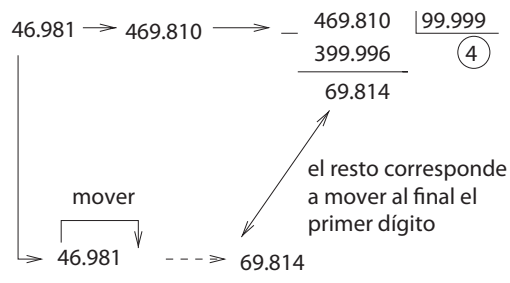


Figura 4. *Cálculo del cociente y resto de dividir 46.981 por 99.999.*

Es en este proceso donde queda claro que al número $0,\bar{9}$ le asociamos la fracción 9/9 = 1. De ahí la identificación de estas dos expresiones (hay un significado analítico de las expresiones decimales que también justifica esta identificación).

Veamos que las asociaciones que definimos son una la inversa de la otra (o sea que si a una expresión decimal le asociamos una fracción y a esta fracción le calculamos su expresión decimal, volvemos a la expresión con la que empezamos). ¿Qué pasa al multiplicar el número 46.981 por 10 y calcular el primer resto de dividir el resultado por 99.999? Como se ve en la figura 4, al dividir 469.810 por

99.999, el resto es 69.814, o sea se corrió el primer dígito de 46.981 (el número antes de ser multiplicado por 10) al último lugar, y el cociente es 4.

Si N es un número natural de n dígitos que no es el número que posee n nueves, o sea $N \neq 10^n - 1$ (por ejemplo $N \neq 999 = 10^3 - 1$), al dividir $10 \cdot N$ por el número que tiene n nueves, el cociente es el primer dígito de N y el resto se obtiene moviendo el primer dígito de N al último lugar. Veamos el argumento en un ejemplo, supongamos que $N = 69.814$. Al multiplicarlo por 10, tenemos el número:

$$\begin{aligned} 10 \cdot 69.814 &= 698.140 \\ &= 6 \cdot 100.000 + 98.140 \\ &= 6 \cdot (99.999 + 1) + 98.140 \\ &= 6 \cdot 99.999 + 98.140 + 6 \\ &= 6 \cdot 99.999 + 98.146 \end{aligned}$$

Como 98.146 es menor que 99.999, tenemos que el cociente es 6 y el resto es 98.146 (por unicidad del cociente y resto).

Es importante notar que usamos que $N \neq 10^n - 1$ en el argumento, ya que si lo fuera el cociente sería 10 y el resto 0. Este caso se corresponde con las expresiones decimales que tienen período $\overline{9}$.

Si continuamos multiplicando los restos por 10 y calculando el cociente y resto de la división por 99.999, es claro que obtendremos la expresión decimal $0,\overline{46981}$. Luego hemos mostrado que tenemos una biyección entre números racionales y expresiones decimales periódicas con período distinto de $\overline{9}$.

De los argumentos antes dados se deduce la siguiente observación: si la fracción irreducible $\frac{a}{b}$ tiene un desarrollo periódico puro de longitud r, entonces b divide a $10^r - 1$. Esto se debe a que la fracción que representa un período puro de r lugares se obtiene tomando el período como numerador y $10^r - 1$ como denominador. Al ser esta fracción igual a la fracción irreducible $\frac{a}{b}$, debe ser $10^r - 1$ un múltiplo de b.

En particular, podemos saber el período de una fracción irreducible $\frac{a}{b}$ mirando la mínima potencia de 10 que es congruente a 1 módulo b. Por ejemplo, para la fracción 1/7 tenemos:

$$\begin{aligned} 10^1 &\equiv 10 \cdot 1 \equiv 3 \pmod 7 \\ 10^2 &\equiv 10 \cdot 3 \equiv 2 \pmod 7 \\ 10^3 &\equiv 10 \cdot 2 \equiv 6 \pmod 7 \\ 10^4 &\equiv 10 \cdot 6 \equiv 4 \pmod 7 \\ 10^5 &\equiv 10 \cdot 4 \equiv 5 \pmod 7 \\ 10^6 &\equiv 10 \cdot 5 \equiv 1 \pmod 7 \end{aligned}$$

Luego $7 \mid 10^6 - 1$ y 6 es la menor potencia con esta propiedad, con lo cual el período de 1/7 es de longitud 6, como vimos en el tercer ejemplo. De igual forma:

$$10 \equiv 1 \pmod 3$$

con lo cual el período de 1/3 tiene longitud 1.

Ejercicio 4.12. Calcular la longitud del período de la expresión decimal de la fracción 1/9.091 sin calcular explícitamente el período.

Ejercicio 4.13. Hallar un número primo p tal que la fracción $1/p$ tenga período de longitud 2. Hacer lo mismo para períodos de longitud 3, 4, 5 y 6.

□ 4. Curiosidades

En esta sección daremos algunas curiosidades sobre los números racionales, aunque dichos resultados no serán utilizados en el próximo capítulo.

¿Cómo se ven los números racionales en la recta? Si pensamos que la recta real es una línea llena de puntos, y en ella dibujamos los números enteros, vemos en la figura 5 que éstos están bien separados unos de otros.

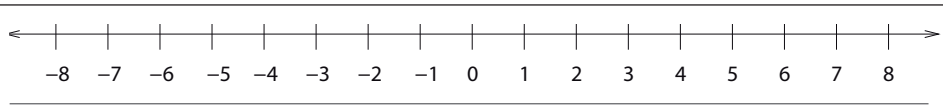


Figura 5. *Puntos enteros en la recta real.*

Si miramos los puntos racionales en la recta real no vemos agujeros entre ellos. Esto se debe a que entre dos números racionales cualesquiera siempre hay un número racional. Si $\frac{a}{b}$ y $\frac{c}{d}$ representan números racionales y $\frac{a}{b} < \frac{c}{d}$, el promedio de ambos satisface:

$$\frac{a}{b} < \frac{1}{2}\left(\frac{a}{b} + \frac{c}{d}\right) < \frac{c}{d}$$

como es fácil verificar. Así, por ejemplo, si tomamos los promedios comenzando por los números 0 y 1 y repetimos este proceso en todos los promedios nuevos que nos aparecen, tenemos los números:

$$\begin{gathered} 0 < 1, \\ 0 < \tfrac{1}{2} < 1, \\ 0 < \tfrac{1}{4} < \tfrac{1}{2} < \tfrac{3}{4} < 1, \\ 0 < \tfrac{1}{8} < \tfrac{1}{4} < \tfrac{3}{8} < \tfrac{1}{2} < \tfrac{5}{8} < \tfrac{3}{4} < \tfrac{7}{8} < 1 \\ \vdots \end{gathered}$$

Luego de n pasos, tenemos el conjunto de números racionales $\{\frac{0}{2^n}, \frac{1}{2^n}, \frac{2}{2^n}, \cdots, \frac{2^n}{2^n} = 1\}$ La distancia entre dos de ellos consecutivos es $\frac{1}{2^n}$. Si n es muy grande, estos números están muy amontonados entre sí. Es por esto que si tratamos de mirar los puntos racionales entre 0 y 1, para nosotros el dibujo está completamente lleno, a pesar de que faltan varios números (todos los irracionales, como por ejemplo $\frac{\sqrt{2}}{2}$).

Con esta noción geométrica de los números racionales, pareciera ser que los números racionales son muchos más que los números naturales, dado que "parecen llenar" la recta real, pero esto no es así. Dar una definición correcta del significado de que dos conjuntos tengan la misma cantidad de elementos está más allá del contenido de este libro por la extensión del tema, más que por la dificultad del contenido.

Es interesante, sin embargo, corregir la impresión errónea de que hay más números racionales que enteros. Para ello vamos a listar todos los números racionales en orden. Esto es: a cada número natural le podemos asociar un número racional de forma tal que cubrimos todos los números racionales. Es bastante intuitivo suponer que si un conjunto tiene *menos* elementos que otro, no vamos a poder asociarle a los elementos del segundo conjunto elementos distintos del primero. Por ejemplo, con los números {1, 2, 3} no podemos numerar el conjunto {♢, ♡, ♠, ♣}.

Una forma de numerar los números racionales se ve en la figura 6, donde los números en rojo no son tenidos en cuenta por no ser fracciones irreducibles.

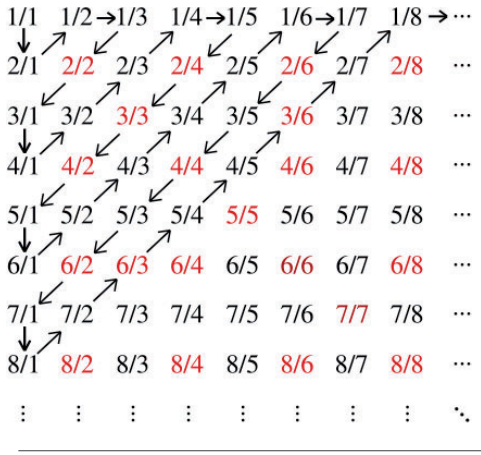


Figura 6. *Una forma de listar los números racionales.*

5. Números reales

Alejandro Petrovich

En este capítulo introduciremos el conjunto de los números reales. Nos proponemos dar una construcción de este sistema numérico utilizando un método particular para aproximar dichos números mediante fracciones o números racionales. Mostraremos mediante algunos ejemplos de carácter geométrico la forma de construir los números reales a partir de esta aproximación.

Algunos resultados de este capítulo serán enunciados sin demostración dado que la prueba matemática formal de los mismos requiere el manejo de ciertas técnicas que están fuera del alcance del presente libro.

Si c y d son dos números racionales con $c \leq d$, notaremos con $[c, d]$ al intervalo cerrado determinado por c y d, esto es:

$$[c, d] = \{x : c \leq x \leq d\}$$

Recordamos que para un número x, escribimos $|x|$ su valor absoluto:

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

En términos geométricos, el valor absoluto de un número racional expresa cuánto dista dicho número del 0. Si a es un número racional positivo, entonces $|x| = a$ si y sólo si $x = a$ o bien $x = -a$. Más aún, si x e y son dos números racionales, entonces el número $|x - y|$ expresa la distancia entre x e y. Por ejemplo, ¿cuál es la distancia entre 4 y -7? La respuesta es: $|4 - (-7)| = |11| = 11$.

Propiedad 5.1. *Una propiedad importante que verifican los números racionales referida al valor absoluto es la llamada* desigualdad triangular. *Esta desigualdad expresa lo siguiente:*

$$|x + y| \leq |x| + |y|$$

para todo par de números racionales x, y.

Demostración. Para demostrarla debemos separar en casos de la siguiente manera:

Primer caso: $x \geq 0$, $y \geq 0$. Luego $x + y \geq 0$ lo que implica $|x + y| = x + y$, $|x| = x$ y $|y| = y$. Por lo tanto $|x + y| = |x| + |y|$.

Segundo caso: $x < 0$, $y < 0$. Luego $x + y < 0$ lo que implica $|x + y| = -x - y$, $|x| = -x$ y $|y| = -y$. Por lo tanto $|x + y| = |x| + |y|$.

Tercer caso: $x \geq 0$, $y < 0$. Notar que en este caso no podemos determinar el signo de $x + y$. Lo que sí sabemos es que $|x| = x$ y $|y| = -y$. Si $x+y \geq 0$, entonces $|x + y| = x + y$.

Por lo tanto $|x + y| \leq |x| + |y|$ si y sólo si $x + y \leq x - y$, o equivalentemente, $y \leq -y$ y esta desigualdad se cumple ya que $y < 0$. Si $x+y < 0$, entonces $|x + y| = -x - y$. Por lo tanto $|x + y| \leq |x|+|y|$ si y sólo si $-x - y \leq x - y$, o equivalentemente, $-x \leq x$ y esta desigualdad se cumple pues $x \geq 0$.

Cuarto caso: $x < 0$, $y \geq 0$. La prueba es similar al caso anterior y la omitiremos.

Ejercicio 5.1. Mostrar que si a es un número racional positivo ó 0, entonces $|x| \leq a$ si y sólo si $-a \leq x \leq a$.

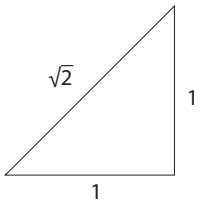


Figura 1. *Un triángulo con catetos que miden 1 e hipotenusa que mide* $\sqrt{2}$

Los números reales surgen como necesidad de resolver ciertas ecuaciones que no tienen solución en el conjunto de los números racionales. Entre dichas ecuaciones se encuentran las que nos permiten calcular ciertas raíces cuadradas. En efecto, una de las múltiples aplicaciones del número real es la de poder demostrar la existencia de raíces cuadradas de números positivos. En primer lugar, debemos precisar qué significa que un número admita una raíz cuadrada. Consideremos, para ilustrar este concepto, el siguiente ejemplo que aparece en geometría. Tomemos un triángulo rectángulo cuyos catetos miden 1 cm de longitud. ¿Qué longitud tiene la hipotenusa? Si llamamos h a la longitud de la hipotenusa, entonces según el Teorema de Pitágoras tenemos que $h^2 = 1^2 + 1^2 = 2$. Es decir h debe ser un número que elevado al cuadrado dé como resultado el número 2. Luego h debe ser solución de la ecuación $x^2 = 2$. Es claro que si esta ecuación admite una solución x, entonces $-x$ también es solución ya que $x^2 = (-x)^2 = 2$. Como la longitud de la hipotenusa debe ser positiva, la solución que estamos buscando debe ser única, en el sentido que dicha ecuación no puede admitir dos soluciones positivas. Diremos en este caso que *la raíz cuadrada* de 2 es la única solución positiva de la ecuación $x^2 = 2$ y dicha solución será denotada por $\sqrt{2}$. Sin embargo, para asegurarnos de que esta definición es correcta debemos garantizar que la ecuación $x^2 = 2$ admite solución. Comenzaremos probando que si dicha solución existe, entonces no puede ser un número racional.

Teorema 5.2. *Si x es un número racional, entonces $x^2 \neq 2$.*

Demostración. Supongamos por el absurdo que existe $x \in \mathbb{Q}$ tal que $x^2 = 2$. Por lo dicho anteriormente, podemos suponer, sin pérdida de generalidad, que x es positivo. Luego, existen dos números naturales p, q tales que $x = p/q$ donde además p/q es una fracción irreducible. Como $x^2 = 2$, entonces $p^2/q^2 = 2$. A partir de esta igualdad, se sigue que $p^2 = 2q^2$. Luego, p es un número natural que elevado al cuadrado nos da un número par. Por lo tanto p debe ser par, lo que implica que existe $k \in \mathbb{N}$ tal que $p = 2k$. Reemplazando p por $2k$ obtenemos $(2k)^2 = 4k^2 = 2q^2$. Luego, simplificando por 2 llegamos a que $2k^2 = q^2$, lo que implicaría que q^2 es par y por ende q es par. Por lo tanto p y q son números pares, lo que es imposible ya que p/q es una fracción irreducible.

Ejercicio 5.2. Mostrar que si n es un número natural, no existe un número racional x tal que $x^2 = 2^{2n+1}$.

Tanto el teorema 5.2 como el enunciado del ejercicio 5.2 muestran que es necesario ampliar el conjunto de los números racionales para poder resolver ciertas ecuaciones. En la sección 4 mostraremos, efectivamente, que la ecuación $x^2 = 2$ admite solución en el conjunto de los números reales. En la sección 2 mostraremos otro ejemplo de carácter geométrico que ilustra cómo aparecen los números reales en el cálculo de áreas de ciertas figuras geométricas.

□ 1. Sucesiones crecientes y acotadas

Diremos que una sucesión de números racionales $(a_n)_{n\geq 1}$ es **creciente** si $a_n \leq a_{n+1}$ para todo número natural n. Si $a_n < a_{n+1}$ $\forall n \in \mathbb{N}$, diremos que $(a_n)_{n\geq 1}$ es **estrictamente creciente**. Los conceptos de sucesión decreciente y estrictamente decreciente son análogos cambiando el orden de la desigualdad (es decir, $a_n \geq a_{n+1}$ y $a_n > a_{n+1}$).

En otras palabras, una sucesión es creciente cuando cada término es mayor o igual que el anterior, mientras que una sucesión es estrictamente creciente cuando cada término es estrictamente mayor que el anterior. Es fácil ver que una sucesión $(a_n)_{n\geq 1}$ es creciente (estrictamente creciente) si y sólo si $a_n \leq a_m$ ($a_n < a_m$) para todo par de números naturales n, m tal que $n < m$.

Es claro que la sucesión de los números naturales $a_n = n$ es una sucesión estrictamente creciente. Por otro lado, la sucesión $a_n = (-1)^n$ no es creciente ni decreciente.

Ejercicio 5.3.
1. Mostrar que las sucesiones $a_n = \frac{1}{n}$ y $b_n = \frac{1}{2^n}$ son estrictamente decrecientes.
2. Mostrar que la sucesión $c_n = \frac{n}{n+1}$ es estrictamente creciente.

Ejercicio 5.4. Dar un ejemplo de una sucesión creciente pero no estrictamente creciente.

Diremos que una sucesión de número racionales $(a_n)_{n\geq 1}$ es **acotada superiormente,** si existe un número racional d tal que $a_n \leq d$ para todo $n \in \mathbb{N}$. En este caso, diremos que d es una **cota superior** de la sucesión $(a_n)_{n\geq 1}$. Análogamente, diremos que $(a_n)_{n\geq 1}$ es **acotada inferiormente,** si existe un número racional c tal que $c \leq a_n$ para todo $n \in \mathbb{N}$, y c se denomina **una cota inferior** de la sucesión $(a_n)_{n\geq 1}$. Finalmente, diremos que $(a_n)_{n\geq 1}$ es **acotada** si es acotada superiormente e inferiormente.

Para ilustrar el concepto de sucesión acotada, consideremos la sucesión de los números naturales $a_n = n$ y la sucesión $b_n = 1/n$. La primera, está acotada inferiormente pero no superiormente. Cualquier número $c \leq 1$ es una cota inferior. Sin embargo, ningún número d tiene la propiedad de ser mayor que todos los números naturales. Es decir, si d es un número racional, existe algún natural $m > d$, por lo que $a_m > d$, y luego d no puede ser una cota superior de $(a_n)_{n\geq 1}$. Por otra parte, la sucesión b_n está acotada tanto superior como inferiormente. De hecho, cualquier número ≤ 0 es una cota inferior, y cualquier número ≥ 1 es una cota superior.

Es importante destacar que una sucesión $(a_n)_{n\geq 1}$ es acotada si todos sus términos están dentro de un intervalo $[c, d]$ donde c y d son cotas inferiores y superiores de $(a_n)_{n\geq 1}$, respectivamente. Esto significa que $c \leq a_n \leq d$ para todo $n \geq 1$.

Ejercicio 5.5.
1. Probar que toda sucesión creciente de números racionales es acotada inferiormente.
2. Probar que toda sucesión decreciente de números racionales es acotada superiormente.

Ejercicio 5.6. Mostrar cotas superiores e inferiores para las sucesiones $a_n = \frac{n}{n+1}$, $b_n = \frac{1}{2^n}$ y $c_n = (-1)^n$

□ 2. Un ejemplo geométrico

Consideremos el gráfico de la función $y = f(x) = 1/x$ en el intervalo $[1, 2]$. ¿Cuál es el área de la región $\mathfrak{R}$ comprendida por dicho gráfico, el eje x y las dos rectas verticales $x = 1$ y $x = 2$? En la figura 2 ilustramos a la región $\mathfrak{R}$ marcada con color verde.

Llamemos S al valor del área de la región $\mathfrak{R}$. Dado que no tenemos una herramienta para calcular el valor de S, desarrollaremos un nuevo mecanismo para poder aproximar dicho valor, utilizando algunos conocimientos elementales de geometría. Entre todas las figuras geométricas de las cuales sabemos calcular el área se encuentra el *rectángulo*. Recordemos que el área de un rectángulo de base b y altura h es el producto $b{\cdot}h$. Veamos cómo podemos utilizar esta fórmula para aproximar el valor de S. Observemos que, si consideramos el rectángulo R que tiene como base el intervalo cerrado $[1, 2]$ y altura $f(2) = 1/2$, dicho rectángulo se encuentra por debajo del gráfico de la función y el área del mismo es $1/2$. Es claro que este valor no va a coincidir con el valor de S que queremos calcular, ya que hay puntos de $\mathfrak{R}$ que no pertenecen a R. Estos puntos se corresponden con la región en blanco de la figura 3. Si bien no hemos calculado el valor de S, hemos aproximado dicho valor por el número $1/2$ y además $1/2 < S$. Una pregunta natural es la siguiente: ¿cuál es el error cometido al usar esta primera aproximación? Entendemos por error a la diferencia entre el valor exacto S y el valor $1/2$, es decir $S - 1/2$. Como no conocemos el valor de S, no podemos determinar el valor exacto del error cometido. Sin embargo, es importante destacar que el valor $S - 1/2$ coincide con el área de la región en blanco de la figura 3.

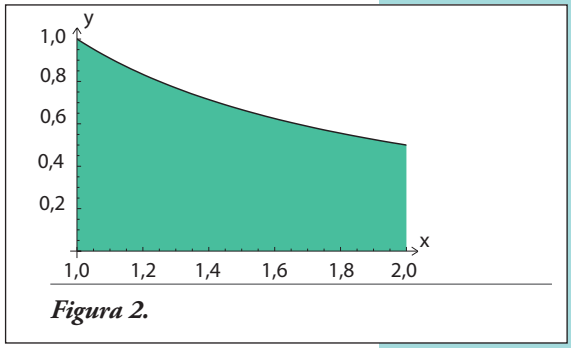


Figura 2.

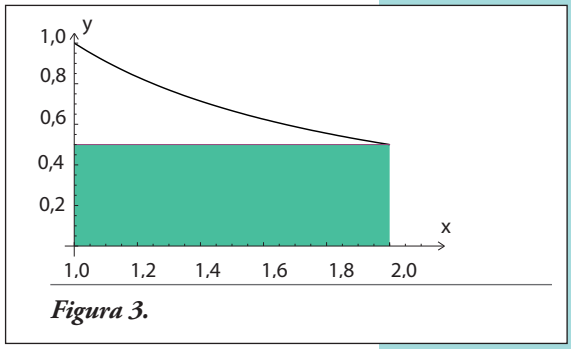


Figura 3.

Supongamos ahora que dividimos al intervalo $[1, 2]$ en dos *subintervalos* I_1, I_2 de la misma longitud. Como el intervalo $[1, 2]$ tiene longitud 1, resulta que $I_1 = [1, 3/2]$ e $I_2 = [3/2, 2]$.

Luego, cada uno de estos intervalos tiene longitud 1/2. A continuación, construimos dos rectángulos R_1,R_2 que tienen como base los intervalos I_1, I_2 y cuyas alturas son respectivamente $f(3/2) = 2/3$ y $f(2) = 1/2$, es decir el valor de f en los extremos derechos de ambos intervalos. Si hacemos el dibujo de dichos rectángulos (Figura 4) se observa también que están por debajo de la gráfica de la función $y = 1/x$. Como el área de R_1 es $1/3$ y el área de R_2 es $1/4$ resulta que el área de la figura resultante de la unión de los dos rectángulos es $1/3 + 1/4 = 7/12$. Al igual que en el caso anterior, se observa que este valor no va a coincidir con el valor de S que queremos calcular ya que hay puntos de $\mathfrak{R}$ que no pertenecen a ninguno de dichos rectángulos. En términos conjuntistas, esto quiere decir que existen puntos de $\mathfrak{R}$ que no pertenecen a la unión $R_1 \cup R_2$. Dichos puntos son los que se corresponden con la región en blanco de la figura 4. En este segundo caso hemos aproximado el valor de S por el número racional 7/12. Como $1/2 < 7/12 < S$ se deduce que el error cometido en este caso es menor que en el caso anterior, ya que $S - 7/12 < S - 1/2$. Por lo tanto, esta segunda aproximación es mejor que la anterior. Esta propiedad se pone de manifiesto comparando las figuras 3 y 4, ya que el área de la región en blanco de la figura 4 es menor que la correspondiente en la figura 3.

A partir de estas dos primeras aproximaciones podemos obtener como generalización natural la siguiente construcción. Para cada número natural n dividimos al intervalo $[1, 2]$ en n subintervalos $I_1, I_2, \ldots, I_n$ de la misma longitud, $1/n$. Los intervalos construidos de esta manera serán:

$$I_1 = [1, 1 + \frac{1}{n}],\ \ I_2 = [1 + \frac{1}{n}, 1 + \frac{2}{n}], \ldots,\ \ I_n = [1 + \frac{n-1}{n}, 2]$$

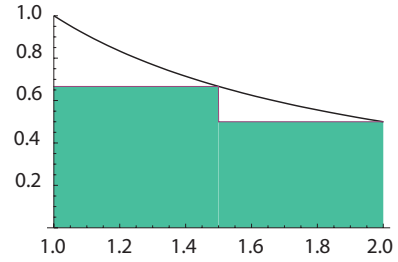


Figura 4.

A partir de estos intervalos definimos n rectángulos R_1,R_2, ... ,R_n que tienen como base los intervalos I_1, I_2, ... , I_n respectivamente, cuyas alturas son $h_1 = f(1+1/n) = n/n+1$, $h_2 = f(1+2/n) = n/n+2$, ... , $h_n = f(2) = 1/2$, es decir el valor de f en los extremos derechos de cada uno de estos intervalos. Vemos que si $1 \leq i \leq n$, el valor de la altura del i-ésimo rectángulo R_i es $h_i = n/n+i$,y por lo tanto el área de R_i es $1/n \cdot n/n+i = 1/n+i$. Llamemos $R(n)$ a la unión de estos n rectángulos. Por lo tanto, el área total resultante de la unión de estos n rectángulos es:

$$A(R(n)) = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}$$

Observemos que para cada $n \in \mathbb{N}$, $A(R(n))$ es un número racional. Al igual que en los casos $n = 1$ y $n = 2$, la figura resultante de unir estos n rectángulos está por debajo de la gráfica de la función $y = 1/x$ y no coincide con la región total $\mathfrak{R}$ (Figura 5). Sin embargo, a medida que le damos valores a n cada vez más grandes, *los diferentes valores de* $A(R(n))$ *se van acercando cada vez más al valor* S. Esto se interpreta gráficamente viendo que el área de la parte marcada en blanco va a ser cada vez más pequeña a medida que n toma valores cada vez más grandes. Para cada n se tiene, además, que dicha área coincide con el error cometido, cuyo valor está dado por la fórmula:

$$S - \left(\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}\right)$$

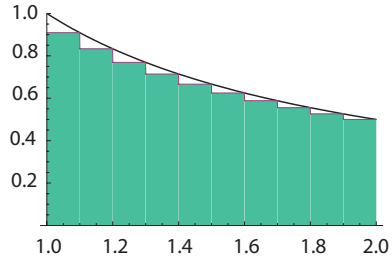


Figura 5.

A partir de estas consideraciones, podemos enunciar los siguientes resultados:

1. para cada $n \in \mathbb{N}$, $A(R(n)) < S$;
2. si $n < m$, entonces $A(R(n)) < A(R(m))$. Es decir, los números $A(R(n))$ van creciendo a medida que n toma valores cada vez más grandes;
3. para cada $n \in \mathbb{N}$, $A(R(n))$ es un número racional;
4. el error cometido $S - \left(\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}\right)$ se acerca a 0 a medida que n toma valores cada vez más grandes.

Es muy importante destacar que cada una de estas condiciones requiere una justificación matemática rigurosa, ya que el análisis que hemos hecho para afirmar tales condiciones fue hecho en base a una idea intuitiva que proviene de una interpretación geométrica dada por el gráfico de la función. Por ejemplo, en la condición (1) se afirma que $A(R(n)) < S$. Es obvio que para justificar esto deberíamos conocer el valor de S, que no sabemos por el momento. Otro problema es determinar qué clase de número representa S. ¿S es un número racional? La respuesta es negativa: *S no es un número racional*[10]. El número S es un nuevo ejemplo de un *número real* que no es racional, es decir un número *irracional*, definición que daremos más adelante.

Lo que sí podemos justificar es lo afirmado en los ítems 2 y 3. La condición 2 nos dice que la sucesión $A(R(n))_{n\geq 1}$ es estrictamente creciente. La prueba es la siguiente:

De acuerdo a la fórmula de arriba, sabemos que para cada n se tiene:
$A(R(n)) = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}$. Luego, si cambiamos n por n+1 tenemos que:
$A(R(n+1)) = \frac{1}{n+2} + \frac{1}{n+3} + \ldots + \frac{1}{2n+2}$. Si a esta expresión sumamos y restamos la fracción $\frac{1}{n+1}$ obtenemos $A(R(n+1)) = \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + \ldots + \frac{1}{2n} + \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1}$
Usando el hecho que la suma de los primeros n términos de esta suma es $A(R(n))$ deducimos que:

$$A(R(n+1)) = A(R(n)) + \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1}$$

o bien, como $\frac{1}{2n+2} - \frac{1}{n+1} = -\frac{1}{2n+2}$

$$A(R(n+1)) = A(R(n)) + \frac{1}{2n+1} - \frac{1}{2n+2}$$

Como $\frac{1}{2n+1} - \frac{1}{2n+2} = \frac{1}{(2n+1)(2n+2)}$ deducimos la fórmula:

[10] La prueba matemática de este hecho es difícil ya que se requieren técnicas que están fuera de los alcances y objetivos del presente libro, motivo por el cual la omitiremos.

$$A(R(n+1)) = A(R(n)) + \frac{1}{(2n+1)(2n+2)}$$

Como $\frac{1}{(2n+1)(2n+2)}$ es un número positivo, concluimos que $A(R(n)) < A(R(n+1))$ para todo $n \geq 1$, mostrando de esta manera que la sucesión $(A(R(n)))_{n\geq 1}$ determinada por las áreas de las regiones $R(n)$ es estrictamente creciente. Luego, si $n < m$ entonces $A(R(n)) < A(R(m))$.

La condición 3 es claramente verdadera ya que para cada número natural n los números $\frac{1}{n+i}$, con $1 \leq i \leq n$ son racionales y, por lo tanto, su suma será también un número racional.

Más aún, la sucesión $(A(R(n)))_{n\geq 1}$ es acotada superiormente. En efecto, sabemos que $A(R(n)) = \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}$. Como cada sumando es menor o igual que la fracción $\frac{1}{n}$, se tiene que $A(R(n)) \leq \frac{1}{n} + \frac{1}{n} + \ldots \frac{1}{n}$. Como la cantidad de términos de esta sumatoria es n, deducimos que $A(R(n)) \leq n \cdot \frac{1}{n} = 1$, lo que prueba que 1 es una cota superior de la sucesión $(A(R(n)))_{n\geq 1}$.

Tal como se ha mencionado anteriormente, tampoco podemos justificar por el momento lo afirmado en el punto 4 ya que, al no conocer con precisión el valor de S no podremos conocer el error cometido al calcular el área de la región $\mathfrak{R}$. Sin embargo, es conveniente hacer un análisis más detallado del error. Si bien no podemos conocer para cada número natural n el valor exacto de dicho error, podemos hacer una e*stimación* del mismo en el siguiente sentido:

Si fijamos un número ε arbitrariamente pequeño, entonces podemos encontrar un número natural n_0 tal que el error cometido al aproximar el valor de S por el área $A(R(n_0))$ es menor que ε. Por ejemplo, ¿cuántos rectángulos se necesitan construir para que el error cometido sea menor que 10^{-3}? En la sección 4 daremos una respuesta a este problema.

□ 3. Límite de sucesiones

Para poder definir el concepto de número real necesitaremos introducir el de límite de una sucesión. En la sección anterior dimos una idea de cómo se puede aproximar el área S de la región $\mathfrak{R}$ calculando las áreas de las regiones $R(n)$ cuyos valores están dados por la sucesión $(A(R(n)))_{n\geq 1}$. Decimos, en ese caso, que el valor S representa un número real que se obtiene como *límite* de la sucesión $(A(R(n)))_{n\geq 1}$. Es importante destacar que a medida que n toma valores cada vez más grandes, las áreas $A(R(n))$ de las regiones $R(n)$ se van aproximando cada vez más al valor de S, pero nunca podremos calcular el valor exacto de S mediante esta aproximación. Consideremos la sucesión $a_n = \frac{1}{n}$. Los términos de esta sucesión son las sucesivas divisiones 1, 1/2 , 1/3 , 1/4 , 1/5 , ... A medida que los denominadores se agrandan, los términos son cada vez más pequeños.

Imaginemos que queremos repartir un kilogramo de helado entre n personas de modo tal que todas las porciones tengan el mismo peso. Es claro que cuanto mayor sea el número

de personas, la porción de helado que recibirá cada una será menor. Veamos el siguiente ejemplo: ¿entre cuántas personas hay que repartir el kilogramo de helado para que el peso de cada porción sea menor a 10^{-1} kilogramos (100 gramos)? Para responder esta pregunta debemos ver para qué valor de n se cumple la desigualdad $1/n < 10^{-1}$. Pero $1/n < 10^{-1}$ si y sólo si $10^1 < n$. Luego, n debe ser un número natural mayor que 10. Por lo tanto, si repartimos el kilogramo de helado entre 11 personas o más, el peso de la porción que recibirá cada una de ellas será menor que 10^{-1} kilogramos. Notar que el valor de n no es único, ya que hay infinitos números naturales mayores que 10. Por ejemplo: si repartimos el kilogramo de helado entre 20 personas, el peso de cada porción será también menor que 10^{-1} kilogramos.

Podríamos plantear este otro problema: ¿entre cuántas personas hay que repartir el kilogramo de helado para que el peso de cada porción sea igual a 2/5? Esto lleva a resolver la ecuación $1/n = 2/5$. Pero esta ecuación no tiene solución, porque n debería ser 5/2. Luego, cuando decimos que los términos de la sucesión $(1/n)_{n\geq 1}$ van siendo cada vez más chicos a medida que n toma valores cada vez más grandes significa que, si tomamos un número ε positivo arbitrariamente pequeño, es posible encontrar un número natural n_0 tal que $1/n_0 < \varepsilon$ y no necesariamente $1/n_0 = \varepsilon$. Por otra parte, en este ejemplo se ve que si $1/n_0 < \varepsilon$ entonces cualquier n mayor o igual que n_0 también verifica la desigualdad $1/n < \varepsilon$.

Sea $(a_n)_{n\geq 1}$ una sucesión de números racionales. Diremos que $(a_n)_{n\geq 1}$ tiene límite 0 o que **converge a 0** cuando n tiende a ∞, si para todo $\varepsilon \in \mathbb{Q}_{>0}$ existe $n_0 \in \mathbb{N}$ tal que $|a_n| < \varepsilon$ para todo $n \geq n_0$. Más generalmente, si l es un número racional, diremos que $(a_n)_{n\geq 1}$ **tiene límite l cuando n tiende** a ∞, si la sucesión $(a_n - l)_{n\geq 1}$ converge a 0.

Escribiremos $\lim_{n\to\infty} a_n = l$ para indicar que la sucesión $(a_n)_{n\geq 1}$ tiene límite l cuando n tiende a ∞.

Para una sucesión creciente (o decreciente), decir $\lim_{n\to\infty} a_n = l$ equivale a decir que: a medida que n se hace cada vez más grande, los valores de a_n se acercan a l tanto como uno quiera[11].

Si n es un número natural, entonces la diferencia $|a_n - l|$ expresa el error cometido al aproximar el valor de l por el término a_n. Por lo tanto, si ε es un número arbitrariamente pequeño, la definición anterior nos dice que, a partir de un cierto momento, el error cometido al aproximar l por a_n es menor que ε. Ese momento es el menor valor posible de n_0.

Como vimos, la sucesión $a_n = 1/n$ tiene límite 0. Si achicamos el valor de ε, el momento a partir del cual la sucesión distará del 0 en menos de ε será mayor. Por ejemplo, ¿entre cuántas personas hay que repartir el kilogramo de helado para que el peso de cada porción sea menor a 10^{-2} kilogramos? En este caso la respuesta será: *por lo menos* 101.

Dos sucesiones diferentes pueden tener el mismo límite. Por ejemplo, tomemos las sucesiones definidas por $a_n = 1/n$ y $b_n = 1/2n$ para todo n. Ambas sucesiones convergen a 0 pero son diferentes, ya que $a_1 = 1$ y $b_1 = 1/2$. Por otra parte, no todas las sucesiones

[11] El concepto de límite de una sucesión es delicado. Un abordaje más profundo requiere conceptos de análisis matemático que no desarrollamos en este libro. Aquí solamente estudiaremos sucesiones crecientes o decrecientes.

tienen límite. Por ejemplo, la sucesión $a_n = (-1)^n$ no tiene límite. En efecto si n toma valores cada vez más grandes y n es par, entonces a_n vale siempre 1, lo que indicaría que el límite debería ser 1; pero si n toma valores cada vez más grandes y n es impar, entonces a_n vale siempre -1 y luego el límite debería ser -1 lo que es imposible.

Algunas propiedades importantes de los límites de sucesiones son:

Propiedades 5.3. *Si $(a_n)_{n\geq 1}$ y $(b_n)_{n\geq 1}$ son dos sucesiones que convergen a los números racionales ℓ_1 y ℓ_2 respectivamente, entonces:*

- *la suma $(a_n + b_n)_{n\geq 1}$ es una sucesión que converge a $\ell_1 + \ell_2$,*
- *si q es un número racional, la sucesión $(q \cdot a_n)_{n\geq 1}$ converge a $q \cdot \ell_1$,*
- *el producto $(a_n \cdot b_n)_{n\geq 1}$ es una sucesión que converge a $\ell_1 \cdot \ell_2$.*

Supongamos que una sucesión $(a_n)_{n\geq 1}$ de números racionales tenga límite l. Entonces, los términos de la sucesión $(a_n)_{n\geq 1}$ se van acercando entre sí en el sentido de que las distancias $|a_m - a_k|$ son cada vez más pequeñas a medida que k y m toman valores cada vez más grandes. Esta propiedad se deduce de la siguiente desigualdad:

$$|a_m - a_k| = |(a_m - l) + (l - a_k)| \leq |a_m - l| + |l - a_k|$$

En efecto, cuando m y k toman valores cada vez más grandes, tanto $|a_m - l|$ como $|l - a_k|$ pueden hacerse tan chicos como uno quiera, y por lo tanto su suma $|a_m - l| + |l - a_k|$ también. Más aún, si $(a_n)_{n\geq 1}$ es cualquier sucesión creciente y acotada, entonces sus términos también se van acercando entre sí a medida que n y m toman valores cada vez más grandes ¡aunque no sepamos si la sucesión $(a_n)_{n\geq 1}$ tiene límite racional!

Podemos ilustrar este hecho con el siguiente ejemplo ficticio. Ivana Pavlova fue la única sobreviviente de un accidente aéreo ocurrido en el desierto de Sahara el 10 de septiembre de 1945. Ivana tenía la ventaja de que su organismo le permitía sobrevivir en el desierto con absorber cada día una pequeña dosis de agua, sin importar la cantidad. Pero para ello no podía dejar de tomar agua ni un solo día. Entre los restos del avión que se estrelló, Ivana encontró un bidón de agua de 10 litros. Supongamos que $C(n)$ es la cantidad medida en litros que Ivana toma el día n, siendo el primer día el 10 de septiembre de 1945. Definimos $S(n)$ a la cantidad total de agua que ha tomado Ivana desde el 10 de septiembre hasta el día n. Es decir $S(n) = C(1) + C(2) + \ldots + C(n)$. Como Ivana debe tomar agua todos los días y, siempre debe dejar algo de agua en el bidón, inferimos que $C(n) > 0$ y que $S(n) < 10$ para todo n. Luego, la sucesión $(S(n))_{n\geq 1}$ es estrictamente creciente y acotada superiormente por 10.[12] Notemos que si k es un número natural, la diferencia $S(n + k) - S(n) = C(n + 1) + C(n + 2) + \ldots C(n + k)$ expresa la cantidad de agua que Ivana bebe durante k días consecutivos a partir del día n. Es obvio que Ivana no puede tomar 5 litros de agua en dos días diferentes porque se quedaría sin agua. Sin embargo, se puede afirmar algo más: *a partir de cierto día, la cantidad total de agua que*

[12] Una manera que tiene Ivana para garantizar su supervivencia es tomar cada día la mitad del agua que le queda. Esto es, el primer día toma 5 litros, es decir 10/2 litros. El segundo día toma 10/4, el tercero 10/8, y en general el enésimo día toma $10/2^n$.

Ivana va a consumir, entre ese día y cualquier otro día posterior, será menor que 5 litros. En efecto, la propiedad que acabamos de enunciar se escribe simbólicamente como sigue: debe existir un $n_0 \in \mathbb{N}$ tal que $S(n) - S(n_0) < 5$ para todo $n \geq n_0$. Veamos cómo podemos probar esto. Supongamos por el absurdo que esta propiedad no se cumple, en particular no se cumple si $n_0 = 1$, es decir el primer día. Por lo tanto, existe un número natural $n_1 > 1$ tal que $S(n_1) - S(1) \geq 5$. Como la propiedad tampoco se cumple para n_1, debe existir otro número natural $n_2 > n_1$ tal que $S(n_2) - S(n_1) \geq 5$. Luego, $S(n_2) = S(n_2) - S(n_1) + S(n_1) - S(1) + S(1) \geq 10 + S(1) > 10$, lo cual es absurdo.

Por lo tanto, debe existir un día n_0 en el que la cantidad total de agua que consume Ivana desde el día n_0 hasta cualquier otro día es menor a 5 litros. Por ejemplo: si n_0 es el 31 de octubre de 1945, significa que para que Ivana pueda sobrevivir, está obligada a consumir menos de 5 litros durante todo el mes de noviembre. Pero también debe consumir menos de 5 litros durante los meses de noviembre, diciembre y enero de 1946.

Es importante destacar que si cambiamos el valor 5 litros por 1 litro o medio litro de agua, la misma propiedad se sigue cumpliendo, es decir se verifica lo siguiente: si ε es un número racional positivo, debe existir $n_0 \in \mathbb{N}$ tal que $S(n) - S(n_0) < \varepsilon$ *p*ara todo $n \geq n_0$. De lo contrario, como en la argumentación anterior, para todo k natural podríamos encontrar una colección de números $1 < n_1 < n_2 < \ldots < n_k$ tales que $S(n_1) - S(1) \geq \varepsilon$, $S(n_2) - S(n_1) \geq \varepsilon$, ... , $S(n_k) - S(n_{k-1}) \geq \varepsilon$, y por lo tanto:

$$\begin{aligned} S(n_k) > S(n_k) - S(1) &= S(n_k) - S(n_{k-1}) + S(n_{k-1}) - S(n_{k-2}) + \cdots + S(n_2) - S(n_1) + S(n_1) - S(1) \\ &\geq k \cdot \varepsilon \end{aligned}$$

Esto es un absurdo, porque sabemos, por otro lado, que $S(n) < 10$ para todo n, lo que implica que $10 > S(n_k) > k \cdot \varepsilon$ para todo k, pero tomando $k \geq 10/\varepsilon$ esta desigualdad no se cumple.

Esta propiedad dice que los términos de la sucesión $(S(n))_{n\geq 1}$ se van acercando entre sí a medida que n toma valores cada vez más grandes. Observemos que no hemos usado (ni tampoco lo sabemos) que la sucesión tenga límite. Los datos que hemos usado acerca de la sucesión $(S(n))_{n\geq 1}$ es que es acotada y estrictamente creciente. Observando la demostración se ve que la misma propiedad se cumple si la sucesión es acotada y creciente.

Basados en estas observaciones podemos enunciar el siguiente teorema:

Teorema 5.4. *Si $(a_n)_{n\geq 1}$ es una sucesión de números racionales creciente y acotada superiormente y ε es un racional positivo, entonces existe $n_0 \in \mathbb{N}$ tal que $a_n - a_{n_0} < \varepsilon \ \forall n \geq n_0$.*

□ 4. El número real, definición informal

En esta sección introduciremos la noción de número real utilizando el concepto de límite de sucesiones.

4.1. La definición

Por lo visto en el capítulo anterior podemos representar a un número racional x como un número decimal periódico de la forma:

$$\begin{aligned} x &= a, x_1 x_2 \dots x_n y_1 y_2 \dots y_k y_1 y_2 \dots y_k y_1 \dots \\ &= a, x_1 x_2 \dots x_n \overline{y_1 y_2 \dots y_k} \end{aligned}$$

en el que la parte periódica corresponde a la sucesión finita $y_1, y_2, \dots y_k$, y la parte decimal no periódica corresponde a la sucesión finita $x_1, x_2, \dots x_n$, siendo a la parte entera del número x. Cuando $y_1 = y_2 = \dots = y_k = 0$ diremos que el número x representa un *número decimal exacto*.

A partir de esta representación surge la idea natural de generalizar el concepto de número racional definiendo una clase más grande de números que admiten una *representación decimal arbitraria e infinita* de la forma $a,z_1z_2 \dots z_n\dots$, con a un número entero, y al igual que en el caso de las fracciones, los números $z_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Consideremos por ejemplo el número x representado por: $x = 0{,}101101110 \dots$ Es decir, x se define como el número decimal cuya parte entera es cero y la sucesión $(z_n)_{n\geq 1}$ de dígitos después de la coma se obtiene concatenando los números naturales 10, 110, 1.110, ... A partir de esta construcción, se puede ver que el dígito 0 aparece en los lugares 2, 5, 9, 14, ... Los lugares en donde figura el 0 después de la coma determinan una sucesión que denotamos con $(cero_n)_{n\geq 1}$. Por lo tanto, $cero_1 = 2$, $cero_2 = 5$, $cero_3 = 9$, ... Observar que las diferencias 5 - 2 = 3; 9 - 5 = 4; 14 - 9 = 5; ... , dicen que la cantidad de unos que figuran entre la aparición de un 0 y la siguiente se va incrementando de uno en uno. Deducimos de esta propiedad que si $n \in \mathbb{N}$, entonces $cero_{n+1} = cero_n + n + 2$ y $cero_1 = 2$. Luego, las diferencias $cero_{n+1} - cero_n = n+2$ son cada vez más grandes a medida que n va creciendo.

A partir de esta recurrencia se deduce que este número no puede representar un número racional. En efecto, si x fuese un número racional, entonces tendríamos una parte periódica que corresponde a cierta sucesión finita $y_1, y_2 \dots y_k$. Como el 0 aparece infinitas veces en la representación decimal de x, entonces existiría algún índice i entre 1 y k tal que $y_i = 0$. Por lo tanto, existe un n_0 tal que en los lugares n_0, $n_0 + k$, $n_0 + 2k$, ... aparecerá un 0. Por otro lado, como la sucesión $cero_n$ recorre todos los lugares donde aparece el dígito 0, deducimos que, a partir de cierto momento, la diferencia entre dos términos consecutivos de la sucesión $cero_n$ debería ser menor o igual que k, lo que es imposible ya que $cero_{n+1} - cero_n = n + 2$ para todo $n \geq 1$. Esto prueba que x no puede ser un número racional.

A partir del número x podemos construir la siguiente sucesión de números racionales:

$$\begin{aligned} x_1 &= 0,1 \\ x_2 &= 0,10 \\ x_3 &= 0,101 \\ &\dots \\ x_n &= 0, z_1 z_2 z_3 \dots z_n \end{aligned}$$

Es decir el enésimo término de esta sucesión es el número racional cuya parte entera es 0 y los n dígitos después de la coma coinciden con los primeros n dígitos de x. Esta sucesión posee dos propiedades importantes:

- la primera es que es una sucesión de números racionales positivos, creciente y acotada superiormente por 1;
- la segunda es que los términos de esta sucesión representan números decimales exactos y, como dijimos, para todo $n \in \mathbb{N}$ los n dígitos de x_n coinciden con los primeros n dígitos del número x.

A medida que n toma valores cada vez más grandes, los términos de esta sucesión se aproximan cada vez más al número x en un sentido que precisaremos más adelante. Esto nos dice que la sucesión $(x_n)_{n\geq 1}$ es una sucesión creciente y acotada de números racionales positivos que *define* al número x.

Tal como ha sido mencionado en la sección anterior, dos sucesiones distintas pueden tener el mismo límite. Tomemos por ejemplo la siguiente sucesión:

$$y_1 = 0,10;\ y_2 = 0,10110;\ y_3 = 0,101101110;\ y_4 = 0,10110111011110,\ldots$$

El enésimo término de esta sucesión es el número racional cuya parte entera es 0 y después de la coma es el número natural que se obtiene concatenando los números 10,110,1110,11110, ... , 10^n+10^{n-1} +...+10. La sucesión $(y_n)_{n\geq 1}$ es diferente de $(x_n)_{n\geq 1}$, ya que por ejemplo x_3 = 0, 101 mientras que y_3 = 0, 101101110, pero ambas sucesiones definen al número x.

Otro ejemplo, que ya hemos visto, en el que un número se define a partir de una sucesión de números racionales creciente y acotada es el área S de la figura 2. Según lo que hemos observado en la sección 4, las áreas $A(R(n))$ se acercan a S a medida que n se hace cada vez más grande. En otras palabras, la sucesión $A(R(n))$ debería tener como límite al número S. Pero ya hemos mencionado que S no es un número racional. Si queremos poder hablar del área S, debemos agregarle a los racionales ese número, que lo podemos definir precisamente a partir de la sucesión $A(R(n))$.

Ambos ejemplos vuelven a ilustrar que la recta racional está *incompleta* y nos conducen a pensar que deberíamos agregar números nuevos. Basados en los ejemplos, nos proponemos introducir el concepto de número real a partir de sucesiones crecientes y acotadas de números racionales. Haremos esta definición de manera formal en la sección siguiente. Por ahora, informalmente, llamaremos *número real* al "límite" de una sucesión creciente y acotada de números racionales.

Notaremos con $Sucec(\mathbb{Q})$ al conjunto de todas las sucesiones crecientes y acotadas de números racionales y con $Sucec(\mathbb{Q}_{>0})$ al conjunto de todas las sucesiones crecientes y acotadas de números racionales positivos. Sabemos que si $(a_n)_{n\geq 1}$ es una sucesión acotada y creciente de números racionales positivos, entonces pueden ocurrir dos cosas:

1. la sucesión $(a_n)_{n\geq 1}$ tiene como límite un número racional ℓ,
2. la sucesión $(a_n)_{n\geq 1}$ no tiene límite (racional).

En el primer caso, la sucesión $(a_n)_{n\geq 1}$ define al número racional ℓ. En el segundo caso, la sucesión define un nuevo número, que no es racional. A estos números se los llama

números irracionales. Simbólicamente, escribimos $\lim_{n\to\infty} a_n = x$ para indicar que la sucesión $(a_n)_{n\geq 1}$ define el número x. Notaremos con $\mathcal{I}$ al conjunto de los números irracionales. Llamaremos *conjunto de los números reales* al conjunto $\mathbb{R} = \mathbb{Q} \cup \mathcal{I}$. Observar que si q es un número racional, entonces q es también el límite de una sucesión creciente y acotada de números racionales: basta considerar la sucesión $(a_n)_{n\geq 1}$ que toma el valor constante igual a q, es decir $a_n = q$ para todo $n \geq 1$.

Si bien la definición que dimos no es muy precisa, nos alcanza para desarrollar las ideas principales de los números reales. Uno de los problemas con que nos enfrentamos es que no tenemos una "noción de distancia", o de "cercanía", para los números reales. Específicamente, dado que definimos los números reales como límites de sucesiones, ¿cómo deberíamos definir la distancia entre dos números reales? La noción de distancia en $\mathbb{R}$ es consecuencia del orden entre los reales.

4.2. El orden

Una forma de comparar dos números reales positivos cuando ambos están expresados por medio de su desarrollo decimal es la que sigue. Supongamos, por ejemplo que:

$$x = 0{,}123456101101110\ldots$$
$$y = 0{,}1237666101101110\ldots$$

En este caso los primeros tres dígitos de x e y después de la coma coinciden, mientras que el cuarto dígito de x es 4 que es menor que el cuarto dígito de y que es 7. Luego, en este caso podemos afirmar que $x < y$. Más generalmente, si $x = a{,}x_1x_2x_3\ \ldots\ x_n\ldots$, $y = b{,}y_1y_2y_3\ \ldots\ y_n\ldots$ y $x \neq y$, entonces $x < y$ si y sólo si $a < b$ o $a = b$ y $x_1 < y_1$ o $a = b$, $x_1 = y_1$ y $x_2 < y_2$ o ..., es decir $x < y$ si $a < b$ o bien $a = b$ y existe $n \in \mathbb{N}$ tal que $x_n < y_n$ y $x_j = y_j$ para todo j entre 1 y n - 1.

La relación de orden definida de esta manera se denomina *orden lexicográfico*. Este nombre tiene su razón de ser en la forma de determinar cuándo una palabra aparece antes que otra en el diccionario. Supongamos que tenemos las palabras *encender y encendido*. Las primeras seis letras de ambas coinciden, mientras que la séptima letra de *encender* es una e y la séptima letra de *encendido* es una i. Como en el alfabeto de la lengua española la letra e aparece antes que la letra i, deducimos que primero aparece la palabra *encender* y luego *encendido*. El orden de aparición de las letras es análogo a la forma que están ordenados los dígitos 0,1,2,3,4,5,6,7,8,9.

Hay que tener cuidado y no utilizar este orden para comparar dos expresiones decimales diferentes pero que representan el mismo número. Consideremos por ejemplo $x = 0{,}\overline{9} = 0{,}999999999\ldots$ e $y = 1 = 1{,}0000000000\ldots$ Vimos en el Capítulo 4 que $x = y$. Sin embargo, si aplicáramos el orden lexicográfico a estas dos expresiones decimales llegaríamos a que $x < y$, ya que el primer dígito de x antes de la coma es 0 y el primer dígito (el único) de y es 1.

En la sección 5 precisaremos cómo extender la relación de orden ≤ definida entre dos números racionales x, y al conjunto de los números reales.

4.3. Las operaciones

A continuación, definiremos la suma y el producto de números reales.

Supongamos que $(a_n)_{n\geq 1}$ y $(b_n)_{n\geq 1}$ son dos sucesiones de números racionales. Sabemos que para cada número natural n, a_n y b_n son números racionales. Por lo tanto, la suma $a_n + b_n$ y el producto $a_n \cdot b_n$ dan como resultado un número racional. De esto se desprende que, si definimos la suma y el producto de dos sucesiones $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ *término a término*, el resultado obtenido será una nueva sucesión cuyos términos son también números racionales. Más precisamente, definimos la sucesión suma $(a_n + b_n)_{n\geq 1}$ como la sucesión que en cada $n \in \mathbb{N}$ toma el valor $a_n + b_n$ y análogamente, definimos la sucesión producto $(a_n \cdot b_n)_{n\geq 1}$ como la sucesión que en cada $n \in \mathbb{N}$ toma el valor $a_n \cdot b_n$. Por ejemplo: supongamos que $(a_n)_{n\geq 1}$ es la sucesión $a_n = \frac{n}{n+1}$ y $(b_n)_{n\geq 1}$ es la sucesión dada por $b_n = \frac{1}{n}$ para todo $n \geq 1$. Entonces, la sucesión suma $(a_n + b_n)_{n\geq 1}$ es la sucesión que en cada n toma el valor $\frac{n^2+(n+1)}{n(n+1)}$. Los sucesivos valores de esta sucesión serán, entonces, 3/2 , 7/6 , 13/12, ...

Ejercicio 5.7. Probar que:

1. la suma de dos sucesiones crecientes y acotadas de números racionales es también una sucesión creciente y acotada de números racionales;
2. el producto de dos sucesiones crecientes y acotadas de números racionales positivos es también una sucesión creciente y acotada de números racionales positivos.

Sean $x, y \in \mathbb{R}$ y sean $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ dos sucesiones en $Sucec(\mathbb{Q})$ tales que $\lim_{n\to\infty} a_n = x$ y $\lim_{n\to\infty} b_n = y$. Definimos

$$x + y = \lim_{n\to\infty} (a_n + b_n)$$

Del ejercicio 5.7 se sigue que la suma $x+y$ de dos números reales x, y da como resultado otro número real. Más aún, el resultado no depende de qué sucesiones converjan a x y a y respectivamente, esto es, si $(c_n)_{n\geq 1}$, $(d_n)_{n\geq 1}$ son otras dos sucesiones que convergen a x y a y respectivamente, entonces $\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} (c_n + d_n)$. La prueba de esta propiedad se verá en la última sección.

Es importante destacar que cuando x e y son números racionales, la suma definida de esta manera coincide con la suma habitual de fracciones. Para ver esto basta usar las sucesiones constantes $a_n = x$ y $b_n = y$ (que convergen a x y a y respectivamente), cuya suma es la sucesión constante $a_n + b_n = x + y$.

Para ilustrar cómo se hace para sumar dos números irracionales, consideremos el número irracional $x = 0{,}101101110\ldots$ definido al comienzo de esta sección.

Veamos cómo se calcula la suma $x + x = 2x$. Recordemos que una sucesión que converge a x es, por ejemplo, la sucesión $y_1 = 0,10$; $y_2 = 0,10110$; $y_3 = 0,101101110$; $y_4 = 0,10110111011110$; ... Luego, $2x = \lim_{n\to\infty} 2y_n$, donde $(2y_n)_{n\geq 1}$ es la sucesión $2y_1 = 0,20$; $2y_2 = 0,20220$; $2y_3 = 0,202202220$; $2y_4 = 0,20220222022220$; ... En este caso se ve que $2x = 0,202202220$ ... es el número real que se obtiene concatenando después de la coma los números 20,220,2220, ...

¿Cómo se define la resta entre dos números reales? Para responder a esta pregunta necesitaremos un resultado que es consecuencia del Teorema 5.4, a saber:

Teorema 5.5. *Si $(a_n)_{n\geq 1}$ es una sucesión creciente y acotada de números racionales, entonces existe una sucesión $(c_n)_{n\geq 1}$ decreciente de números racionales que satisface que $\lim_{n\to\infty}(c_n - a_n) = 0$.*

Es inmediato probar este teorema en el caso que la sucesión $(a_n)_{n\geq 1}$ tenga como valor límite un número racional ℓ. En efecto, en este caso basta tomar como sucesión $(c_n)_{n\geq 1}$ la sucesión constante igual a ℓ. Sin embargo, la prueba es difícil cuando el valor límite no es racional y requiere ciertas herramientas que están fuera del alcance del presente libro. Lo que expresa esencialmente el resultado del teorema es que si una sucesión creciente y acotada $(a_n)_{n\geq 1}$ converge a cierto número real x (que puede ser racional o irracional), es posible construir otra sucesión $(c_n)_{n\geq 1}$ que tiene el mismo valor "límite", pero que es decreciente.

El Teorema 5.5 es útil para probar que todo número real admite un inverso aditivo, eso es, si $x \in \mathbb{R}$, existe un único $y \in \mathbb{R}$ tal que $x + y = 0$. Para ver esto, tomemos una sucesión $(a_n)_{n\geq 1}$ creciente y acotada de números racionales que tenga límite x. Por el mencionado teorema, existe una sucesión $(c_n)_{n\geq 1}$ decreciente de números racionales tal que, para todo k, c_k es cota superior de la sucesión $(a_n)_{n\geq 1}$ y tal que $\lim_{n\to\infty}(c_n - a_n) = 0$. La sucesión $(-c_n)_{n\geq 1}$ es creciente y acotada, porque por ejemplo $-a_1$ es una cota superior. Luego, el número $y = \lim_{n\to\infty}(-c_n)$ es un número real y vale que $x + y = 0$ pues, por definición de suma, se tiene que $x + y = \lim_{n\to\infty}(a_n + (-c_n)) = \lim_{n\to\infty}(a_n - c_n) = 0$. Por otro lado, la ecuación $x+y = 0$ tiene solución única, como veremos en la sección 5. Notaremos con $-x$ al único valor de y que es solución de la ecuación $x+y = 0$. A partir de esto podemos definir la resta entre dos números reales a, b como:

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

Tomemos el ejemplo del número x definido al comienzo de esta sección, y sea $(x_n)_{n\geq 1}$ la sucesión definida por:

$$x_1 = 0,1;\ x_2 = 0,10;\ x_3 = 0,101; \ldots;\ x_n = 0,z_1z_2z_3\ldots z_n; \ldots$$

Ya hemos mencionado que los términos de esta sucesión se van acercando cada vez más al número x a medida que n toma valores cada vez más grandes. A partir de la resta de números reales definida anteriormente, podemos justificar esta idea de aproximación del siguiente modo. Si calculamos las diferencias entre x y los diferentes valores de x_n, entonces estas diferencias son cada vez más pequeñas, es decir: si ε es un número racional positivo, entonces existe $n_0 \in \mathbb{N}$ tal que $x - x_{n_0} < \varepsilon$.

Para probar esto, necesitamos saber cómo calcular la diferencia entre x y un término cualquiera de la sucesión $(x_n)_{n\geq 1}$. Supongamos que $x_k = 0, z_1 z_2 z_3 \ldots z_k$ es uno de estos términos. Entonces, la resta $x - x_k$ va a coincidir con el valor límite de la sucesión $(x_n - x_k)_{n\geq 1}$. A partir de $n = k + 1$ en adelante estas diferencias van a dar como resultado los números $0,\overbrace{000\ldots0}^{k} z_{k+1},\ 0,\overbrace{000\ldots0}^{k} z_{k+1}z_{k+2},\ \ldots$ Por lo tanto, la diferencia $x - x_k$ da como resultado el número real $x - x_k = 0,\overbrace{000\ldots0}^{k} z_{k+1}z_{k+2}\ldots$ Entonces, deducimos que $x - x_k < \frac{1}{10^k}$ pues el desarrollo decimal de la fracción $\frac{1}{10^k}$ es $0,\overbrace{000\ldots0}^{k-1}1$
Por lo tanto, cuando n toma valores cada vez más grandes, las diferencias $x - x_n$ convergen a 0.

Para definir el producto $x \cdot y$, entre dos números reales, lo haremos primero en el caso en que x e y sean números reales positivos. Un número real x es *positivo* si está definido por una sucesión $(a_n)_{n\geq 1}$ (creciente y acotada de números racionales) tal que existe n_0 para el que $a_{n_0} > 0$. Observemos que si $(a_n)_{n\geq 1}$ es una sucesión tal que $a_{n_0} > 0$, la sucesión $(b_n)_{n\geq 1}$ definida por:

$$b_n = \begin{cases} a_{n_0} & \text{si } n \leq n_0 \\ a_n & \text{si } n > n_0 \end{cases}$$

define el mismo número que la sucesión $(a_n)_{n\geq 1}$ y tiene todos sus términos positivos. En otras palabras, si x es un número real positivo, existe una sucesión creciente y acotada de números racionales positivos que lo define.

Sean $x, y \in \mathbb{R}$ y sean $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ dos sucesiones en $Sucec(\mathbb{Q}_{\geq 0})$ tales que $\lim_{n\to\infty} a_n = x$ y $\lim_{n\to\infty} b_n = y$.
Definimos

$$(*) \quad x \cdot y = \lim_{n\to\infty} (a_n \cdot b_n)$$

Al igual que en el caso de la suma, deducimos del Ejercicio 5.7 que el producto de dos números reales positivos da como resultado un número real positivo. Cuando x e y son números racionales positivos, el producto definido de esta manera coincide con el producto habitual: basta tomar (al igual que en el caso de la suma) las sucesiones constantes que toman el valor x e y respectivamente, es decir $a_n = x$ y $b_n = y$ para todo n. Por lo tanto, la sucesión producto será la sucesión constante $x \cdot y$. En la última sección se probará que esta definición de producto no depende de qué sucesiones converjan a x y a y respectivamente. Esto es, si $(c_n)_{n\geq 1}$, $(d_n)_{n\geq 1}$ son otras dos sucesiones que convergen a x y a y, entonces $\lim_{n\to\infty} (a_n \cdot b_n) = \lim_{n\to\infty} (c_n \cdot d_n)$.

¿Cómo definir $x \cdot y$ cuando alguno de los números x o y es negativo ó 0?

Definimos que si $x = 0$ o $y = 0$ el producto $x \cdot y = 0$. Si $x < 0$ e $y < 0$, entonces definimos $x \cdot y = (-x) \cdot (-y)$. Como $-x > 0$ y $-y > 0$ la expresión $(-x) \cdot (-y)$ se calcula por medio de la fórmula $(*)$. Si $x < 0$ e $y > 0$, definimos $x \cdot y = -((-x) \cdot y)$. Finalmente, si $x > 0$ e $y < 0$, definimos $x \cdot y = -(x \cdot (-y))$. De esta forma tenemos definido el producto para cualquier par de números reales.

Para poder definir la división x/y, con $y \neq 0$, entre dos números reales x e y apelamos de nuevo al Teorema 5.5. En efecto, probemos primero que si y es un número real positivo, entonces existe un número real positivo z tal que $y \cdot z = 1$. Para ello tomemos una sucesión $(a_n)_{n\geq 1}$ cuyo valor límite es y. Por el Teorema 5.5 sabemos que existe una sucesión $(c_n)_{n\geq 1}$ decreciente tal que $\lim_{n\to\infty}(c_n - a_n) = 0$ y tal que $a_n \leq c_m$ para todo par de números naturales n, m. Entonces, la sucesión $(d_n)_{n\geq 1}$ definida por $d_n = \frac{1}{c_n}$ es creciente y acotada superiormente por $\frac{1}{a_1}$. Luego el valor límite de esta sucesión es un número real positivo z. Vemos que $y \cdot z = 1$. En efecto, $y \cdot z = \lim_{n\to\infty} a_n \cdot \frac{1}{c_n}$. Por otro lado, $1 - a_n \cdot \frac{1}{c_n} = \frac{c_n - a_n}{c_n}$.
Como $a_n \leq c_n$ y $c_n \geq a_1$, deducimos que $0 \leq \frac{c_n - a_n}{c_n} \leq \frac{c_n - a_n}{a_1}$. Como la sucesión $(c_n - a_n)_{n\geq 1}$ tiende a 0, entonces la sucesión $(\frac{c_n - a_n}{a_1})_{n\geq 1}$ también converge a 0, lo que prueba que la sucesión $(1 - a_n \cdot \frac{1}{c_n})_{n\geq 1}$ tiene límite 0. Esto prueba que $\lim_{n\to\infty} a_n \cdot \frac{1}{c_n} = 1$ y por ende $y \cdot z = 1$.
No pueden existir dos valores diferentes de z tales que $y \cdot z = 1$. Por lo tanto, notaremos con y^{-1} a la única solución de la ecuación $y \cdot z = 1$, que es el inverso multiplicativo de y. Esto nos muestra que la división $1/y$ está bien definida si y es un número real positivo. Si $y < 0$, definimos $\frac{1}{y} = -\frac{1}{-y}$. Más generalmente, si x e y son dos números reales, donde y es diferente de cero, definimos $\frac{x}{y} = x \cdot \frac{1}{y}$.

4.4. Raíces

Veamos cómo la estructura algebraica del conjunto de los números reales nos permite demostrar que ciertas ecuaciones, que no se pueden resolver en el conjunto de los números racionales, admiten solución en $\mathbb{R}$. Nuestro próximo paso será demostrar efectivamente que la ecuación $x^2 = 2$ admite solución en $\mathbb{R}$. Más precisamente, vamos a construir una sucesión creciente de números racionales positivos, cuyo cuadrado converge a 2.
Definimos la siguiente sucesión de números racionales:

$$x_1 = 1, \qquad x_{n+1} = \frac{6x_n - x_n^3}{4}$$

Es claro que es una sucesión de números racionales porque x_1 lo es y porque si x_n es racional, entonces $\frac{6x_n - x_n^3}{4}$ también es racional. Queremos probar que esta sucesión es creciente y acotada. Primero probaremos que es acotada. Más precisamente, afirmamos que para todo n natural se tiene $x_n^2 < 2$. Es decir que, por ejemplo, $|x_n| < 2$, pues si $|x_n| \geq 2$ entonces, $x_n^2 = |x_n|^2 \geq 2^2 = 4$, lo que contradice nuestra afirmación. Probemos entonces la afirmación por inducción. Vale cuando $n = 1$, pues $x_1^2 = 1$. Y si vale para n, tenemos:

$$\begin{aligned} x_{n+1}^2 &= \frac{(6x_n - x_n^3)^2}{4^2} \\ &= \frac{36x_n^2 - 12x_n^4 + x_n^6}{16} \end{aligned}$$

Entonces, $x_{n+1}^2 < 2$ si y sólo sí $\frac{36x_n^2 - 12x_n^4 + x_n^6}{16} < 2$, que a su vez vale si y sólo si $36x_n^2 - 12x_n^4 + x_n^6 < 32$, si y sólo sí $36x_n^2 - 12x_n^4 + x_n^6 - 32 < 0$. Esta expresión tiene un aspecto complicado, pero si ahora llamamos $y = x_n^2 - 2$, tenemos:

$$y^2 = x_n^4 - 4x_n^2 + 4$$
$$y^3 = x_n^6 - 6x_n^4 + 12x_n^2 - 8$$

por lo que $y^3 - 6y^2 = x_n^6 - 6x_n^4 + 12x_n^2 - 8 - 6(x_n^4 - 4x_n^2 + 4) = x_n^6 - 12x_n^4 + 36x_n^2 - 32$. Es decir, debemos probar que $y^3 - 6y^2 < 0$, o, en otros términos, que $y^2(y-6) < 0$. Pero observemos que la hipótesis inductiva es, precisamente, que $y < 0$, por lo que $y^2 > 0$ e $y - 6 < 0$, y así $y^2(y - 6) < 0$.

Veamos ahora que la sucesión $(x_n)_{n\geq 1}$ es estrictamente creciente. Para esto, debemos probar que $\frac{6x_n - x_n^3}{4} > x_n$. Pero esta afirmación es equivalente a $6x_n - x_n^3 > 4x_n$, que a su vez es equivalente a $2x_n - x_n^3 > 0$, y ésta a $x_n(2 - x_n^2) > 0$. Pero la hipótesis inductiva dice ahora que la sucesión es estrictamente creciente desde $x_1 = 1$ hasta x_n, por lo que $x_n > 1$ y en particular $x_n > 0$. Y por otra parte, sabemos que $2 - x_n^2 > 0$, con lo que se tiene $x_n(2 - x_n^2) > 0$.

Por último, queremos ver que la sucesión x_n^2 converge a 2. Esto es lo mismo que probar que $x_n^2 - 2$ converge a 0. Llamemos $e_n = x_n^2 - 2$. Pero:

$$e_{n+1} = \frac{(6x_n - x_n^3)^2}{4^2} - 2 = \frac{36x_n^2 - 12x_n^4 + x_n^6 - 32}{16}$$
$$= \frac{e_n^2(e_n - 6)}{16}$$

(observando que e_n es lo que antes llamamos y). Sin embargo, ya probamos que para todo n vale $1 \leq x_n^2 < 2$, por lo que $-1 \leq x_n^2 - 2 < 0$, es decir $-7 \leq e_n - 6 < -6$. En valor absoluto, tenemos $|e_n - 6| \leq 7$, y esto dice que: $|e_{n+1}| = e_n^2 \frac{|e_n - 6|}{16} \leq e_n^2 \frac{7}{16} < \frac{e_n^2}{2}$.
Como $|e_n| \leq 1$, tenemos $e_n^2 \leq |e_n|$, por lo que:
$|e_{n+1}| \leq \frac{|e_n|}{2} \leq \frac{|e_{n-1}|}{4} \leq \frac{|e_{n-2}|}{8} \leq \cdots \leq \frac{|e_1|}{2^n} = \frac{1}{2^n}$

Esto demuestra que e_n converge a 0.

Calculando los primeros términos de la sucesión x_n, podemos ver que esta sucesión aproxima muy rápidamente a $\sqrt{2}$, es decir, es posible obtener los primeros dígitos de la expresión decimal de $\sqrt{2}$ calculando unos pocos términos de la sucesión. Por otra parte, tiene la desventaja de que los numeradores y denominadores de sus términos también crecen muy rápidamente.

$x_1 = \frac{1}{1}$

$x_2 = \frac{5}{4}$

$x_3 = \frac{355}{256}$

$x_4 = \frac{94.852.805}{67.108.864}$

$x_5 = \frac{1.709.678.476.417.571.835.487.555}{1.208.925.819.614.629.174.706.176}$

$$x_6 = \frac{9.994.796.326.591.347.130.392.203.807.311.551.183.419.838.794.447.313.956.622.219.314.498.503.205}{7.067.388.259.113.537.318.333.190.002.971.674.063.309.935.587.502.475.832.486.424.805.170.479.104}$$

Si usamos los primeros 60 decimales, tenemos:

$x_1 = 1{,}0$
$x_2 = 1{,}250$
$x_3 = 1{,}386718750$
$x_4 = 1{,}413416936993598937988281250$
$x_5 = 1{,}414212889391814151023461353186456301465542817474840830982429$
$x_6 = 1{,}414213562372614671850871862475475730106604515369430303090371$
$x_7 = 1{,}414213562373095048801688479449619739849546778721185275386329$
$x_8 = 1{,}414213562373095048801688724209698078569671875376884531681736$
$x_9 = 1{,}414213562373095048801688724209698078569671875376948073176679$

Ejercicio 5.8. Probar que si k es un número natural, entonces la sucesión dada por $x_1 = 1$, $x_{n+1} = \frac{3kx_n - x_n^3}{2k}$ define un número real positivo $\sqrt{k}$ tal que $(\sqrt{k})^2 = k$.

Ejercicio 5.9. Probar que todo número racional positivo admite una raíz cuadrada.

Más aún, se tiene el siguiente teorema, cuya demostración es más delicada.

Teorema 5.6. *Si $x \in \mathbb{R}_{>0}$, entonces existe un único $y \in \mathbb{R}_{>0}$ tal que $y^2 = x$. Es decir, todo número real positivo admite raíz cuadrada.*

4.5. Estimación del error

Cerraremos esta sección con el análisis de la manera de estimar el error cometido al aproximar un número real dado por una sucesión de números racionales.

Supongamos que $(a_n)_{n\geq 1}$ sea una sucesión creciente de números racionales que converge a un límite ℓ, donde ℓ es un número real. Si ε es un número positivo arbitrariamente pequeño, el problema es determinar a partir de qué momento el error cometido al aproximar ℓ por los términos de la sucesión es menor o igual que ε. Como la sucesión $(a_n)_{n\geq 1}$ es creciente, el error cometido para cada término a_n está dado por la diferencia $\ell - a_n$. Luego, debemos encontrar un número natural n_0 que verifique $\ell - a_{n_0} \leq \varepsilon$. Como $(a_n)_{n\geq 1}$ es creciente, entonces $\ell - a_n \leq \varepsilon$ para todo $n \geq n_0$ ya que a ℓ le estamos restando un número mayor o igual que a_{n_0}. Por lo tanto, todos los errores siguientes serán menores o iguales a ε.

Un problema que ya hemos mencionado es que si no conocemos el valor de ℓ, no podemos determinar el valor de los diferentes errores dados por las diferencias $(\ell - a_n)_{n\geq 1}$ tal como ocurre en el problema geométrico que hemos introducido en la sección 2. Sin embargo, podemos utilizar la siguiente propiedad: si n_0 es tal que $a_n - a_{n_0} \leq \varepsilon$ para todo $n \geq n_0$, entonces $\ell - a_{n_0} \leq \varepsilon$. Por lo tanto, para encontrar un término de la sucesión que permita aproximar ℓ con un error menor

o igual que ε basta encontrar un n_0 tal que $a_n - a_{n_0} \leq \varepsilon$ para todo $n \geq n_0$.

Para ilustrar esta propiedad consideremos el área S de la región $\mathfrak{R}$ en la figura 2 que hemos visto en la sección 2. La sucesión $(A(R(n)))_{n\geq 1}$ tiene como valor límite el número S. Además 1 es una cota superior de la sucesión $(A(R(n)))_{n\geq 1}$. Por lo tanto, todos los términos de esta sucesión son menores o iguales que 1, lo que implica que $S \leq 1$. Como S no puede ser 1, entonces $0 < S < 1$.

Para demostrar que la sucesión $A(R(n))_{n\geq 1}$ es estrictamente creciente, se usó la recurrencia:

$$(\heartsuit) \quad A(R(n+1)) = A(R(n)) + \frac{1}{(2n+1)(2n+2)}$$

Veamos cómo podemos generalizar esta recurrencia escribiendo $A(R(n + k))$ en términos de $A(R(n))$. Para lograr esto usaremos la recurrencia ($\heartsuit$) del siguiente modo. Como en esta recurrencia el n es arbitrario, podemos cambiar n por $n + 1$ y obtenemos la fórmula:

$$\begin{aligned} A(R(n+2)) &= A(R(n+1)) + \frac{1}{(2n+3)(2n+4)} \\ &= A(R(n)) + \frac{1}{(2n+1)(2n+2)} + \frac{1}{(2n+3)(2n+4)} \end{aligned}$$

A su vez, si en esta última fórmula cambiamos n por $n + 1$ obtenemos la fórmula:

$$\begin{aligned} A(R(n+3)) &= A(R(n+1)) + \frac{1}{(2n+3)(2n+4)} + \frac{1}{(2n+5)(2n+6)} \\ &= A(R(n)) + \frac{1}{(2n+1)(2n+2)} + \frac{1}{(2n+3)(2n+4)} + \frac{1}{(2n+5)(2n+6)} \end{aligned}$$

Siguiendo de la misma manera, obtenemos que:

$$A(R(n+k)) = A(R(n)) + \frac{1}{(2n+1)(2n+2)} + \frac{1}{(2n+3)(2n+4)} + \cdots + \frac{1}{(2n+2k-1)(2n+2k)}$$

Observar que en cada uno de los denominadores de estas fracciones aparece el producto de dos enteros consecutivos, siendo el menor un número impar y, por ende, el que le sigue un número par. Notar también que la cantidad de sumandos que aparece en esta recurrencia, sin contar el término $A(R(n))$, es igual a k.

Para estimar el error, vamos a acotar la suma de las fracciones que figuran en la fórmula de arriba. Como $\frac{1}{2n+2j-1} \leq \frac{1}{2n+2j-2}$ para todo j entre 1 y k, se tiene que:

$$\begin{aligned} A(R(n+k)) - A(R(n)) &= \frac{1}{(2n+1)(2n+2)} + \frac{1}{(2n+3)(2n+4)} + \ldots + \frac{1}{(2n+2k-1)(2n+2} \\ &\leq \frac{1}{(2n)(2n+2)} + \frac{1}{(2n+2)(2n+4)} + \ldots + \frac{1}{(2n+2k-2)(2n+2k)} \quad k) \\ &= \frac{1}{4}\Big(\frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} + \ldots + \frac{1}{(n+k-1)(n+k)}\Big) \end{aligned}$$

Por otro lado, como $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$, $\frac{1}{(n+1)(n+2)} = \frac{1}{n+1} - \frac{1}{n+2}$, etcétera, obtenemos:

$$\frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} + \ldots + \frac{1}{(n+k-1)(n+k)} =$$

$$= \frac{1}{n} - \frac{1}{n+1} + \frac{1}{n+1} - \frac{1}{n+2} + \ldots + \frac{1}{n+k-1} - \frac{1}{n+k}$$

Como los términos de esta suma se cancelan todos salvo el primero y el último, deducimos que:

$$A(R(n+k)) - A(R(n)) \leq \frac{1}{4}\left(\frac{1}{n} - \frac{1}{n+k}\right) = \frac{1}{4} \cdot \frac{k}{n(n+k)}$$

Como $\frac{k}{n+k} \leq 1$, deducimos que:

$$A(R(n+k)) - A(R(n)) \leq \frac{1}{4n}$$

para todo *n* y para todo *k*. Notar que esta desigualdad también es válida si *k* = 0.

Luego, si fijamos un $n_0 \in \mathbb{N}$ se deduce que $A(R(n_0+k)) - A(R(n_0)) \leq \frac{1}{4n_0}$ para todo entero *k* no negativo. Luego, si $n \geq n_0$ y $k = n - n_0$ obtenemos la desigualdad:

$$A(R(n)) - A(R(n_0)) \leq \frac{1}{4n_0}$$

Luego, si ε es un número racional positivo, resulta que $\frac{1}{4n_0} \leq \varepsilon$ si y sólo si $n_0 \geq \frac{1}{4\varepsilon}$. Por lo tanto, deducimos que para este n_0 encontrado se tiene que:

$$S - A(R(n_0)) \leq \varepsilon$$

Como aplicación vamos a determinar cuántos rectángulos son necesarios para que el error cometido al calcular el área *S* sea menor o igual que 10^{-3}. En este caso $\varepsilon = 10^{-3}$. Luego, si tomamos $n_0 \geq \frac{1}{4 \cdot 10^{-3}}$ la cantidad de rectángulos será el valor de n_0. Pero $\frac{1}{4 \cdot 10^{-3}} = 250$con lo cual basta dividir al intervalo [1, 2] en por lo menos 250 subintervalos de la misma longitud. Por lo tanto, si tomamos 250 rectángulos o más, el error cometido en el cálculo del área será menor o igual que 1/1.000 .

□ 5. La construcción formal

En esta última parte, nos proponemos dar una construcción formal de los números reales. En la sección anterior, presentamos los números reales como aquellos que se obtienen como límite de una sucesión creciente y acotada de números racionales. Para poder justificar esta construcción, observemos primero que un mismo número *x* se puede aproximar por diferentes sucesiones. De hecho, existen infinitas sucesiones que convergen al mismo número *x*. Esto nos permite asociar a cada número irracional *x* un conjunto de sucesiones que comparten la propiedad de que todas tienen como límite al número *x*. Por otro lado, si dos sucesiones tienen el mismo límite, su diferencia tiende a 0. Esto nos lleva a la siguiente definición:

Sean $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ dos sucesiones en Sucec($\mathbb{Q}$). Diremos que $(a_n)_{n\geq 1}$ y $(b_n)_{n\geq 1}$ **son equivalentes** (y escribiremos $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$) si:

$$\lim_{n\to\infty}(a_n - b_n) = 0$$

Ejercicio 5.10. Probar que ~ es una relación de equivalencia definida en el conjunto *Sucec*($\mathbb{Q}$).

Llamaremos **número real** a la clase de equivalencia de una sucesión en Sucec($\mathbb{Q}$). Si en la clase de equivalencia hay una sucesión de términos positivos, diremos que el número es **positivo.**

Si $(a_n)_{n\geq 1} \in$ Sucec($\mathbb{Q}$), notaremos con $C[(a_n)_{n\geq 1}]$ a la clase de equivalencia de $(a_n)_{n\geq 1}$. Simbólicamente, un número real es un elemento x de la forma $x = C[(a_n)_{n\geq 1}]$, donde $(a_n)_{n\geq 1} \in$ Sucec($\mathbb{Q}$).

Consideremos por ejemplo las sucesiones $(x_n)_{n\geq 1}$, $(y_n)_{n\geq 1}$ de números racionales definidas en la sección anterior dadas por:

$x_1 = 0{,}1$; $x_2 = 0{,}10$; $x_3 = 0{,}101$; $x_4 = 0{,}1011$; $x_5 = 0{,}10110$; $x_6 = 0{,}101101$; ...
$y_1 = 0{,}10$; $y_2 = 0{,}10110$; $y_3 = 0{,}101101110$; $y_4 = 0{,}10110111011110$;
$y_5 = 0{,}1011011011110111110$; $y_6 = 0{,}10110111011110111111011111110$; ...

Las sucesivas diferencias dan:

$y_1 - x_1 = 0$
$y_2 - x_2 = 0{,}00110$
$y_3 - x_3 = 0{,}000101110$
$y_4 - x_4 = 0{,}00000111011110$
$y_5 - x_5 = 0{,}000011011110111110$
$y_6 - x_6 = 0{,}00000011011110111111011111110$; ...

Se observa que estas diferencias se acercan cada vez más a 0, por lo que estas sucesiones son equivalentes. Su clase de equivalencia es el *número real positivo* $x = 0{,}\,101101110$ ...

Es importante destacar que si q es un número racional, entonces q se identifica como el número real dado por la clase de equivalencia de la sucesión $(a_n)_{n\geq 1}$ constante igual a q, es decir $a_n = q$ para todo $n \geq 1$.

5.1. Desarrollos decimales

Al comienzo del capítulo mencionamos que al conjunto de números racionales queríamos agregarle números cuya expresión decimal después de la coma fuera infinita y no periódica. Vimos cómo estos números están definidos por sucesiones crecientes y acotadas. Por ejemplo, si a es un número tal, podemos considerar la sucesión $(a_n)_{n\geq 1}$ dada por el número racional que tiene como expresión decimal los primeros n dígitos del número a. En esta

sección pretendemos mostrar que las clases de equivalencia de sucesiones crecientes y acotadas de números racionales tienen expresiones decimales (eventualmente infinitas).

Esto nos permite pensar a los números reales de dos maneras distintas, ya sea como expresiones decimales o como clases de equivalencia de sucesiones crecientes y acotadas de números racionales.

A pesar de que el concepto de número real como un número cuya expresión decimal no es necesariamente periódica ni finita es más intuitivo, el trabajar con sucesiones crecientes y acotadas de números racionales permite operar con los números reales de manera más simple. También permite probar algunas propiedades importantes de dichos números.

No hay un algoritmo que permita calcular explícitamente la expresión decimal de una sucesión creciente y acotada de números racionales. El problema radica en que dos números pueden estar muy cerca uno del otro, pero tener varios dígitos distintos en su expresión decimal. Por ejemplo, el número 1,0001 dista del número 0,9999 en 0,0002. A pesar de que la distancia entre ambos es muy pequeña, todos los dígitos de sus representaciones son distintos.

Consideremos una sucesión creciente y acotada de número racionales $(a_n)_{n\geq 1}$. Supongamos que todos los a_n son positivos. Llamemos por ℓ el número real que representa la clase de equivalencia de esta sucesión. Para calcular la escritura antes de la coma del número ℓ, miramos el conjunto:

$$\mathcal{T}_0 = \{m \in \mathbb{Z} \,:\, m < a_n \text{ para algún } n\}$$

Como la sucesión $(a_n)_{n\geq 1}$ es acotada, el conjunto T_0 es acotado superiormente. Luego tiene un mayor elemento, o sea existe un número entero b tal que $m \leq b$ para todo $m \in \mathsf{T}_0$. Tomamos como expresión decimal del número ℓ antes de la coma al número b. Por la forma en que construimos el número b, es claro que $a_n - b \leq 1$ para todo n, pues si existe un n tal que $a_n - b > 1$, entonces $b + 1 < a_n$, en cuyo caso $b + 1$ sería un elemento de T_0, lo que no pasa por ser b el elemento más grande de dicho conjunto.

Para calcular el primer dígito luego de la coma consideramos la sucesión de números racionales $10 \cdot (a_n - b)$. Como $a_n - b \leq 1$ para todo n, $10 \cdot (a_n - b) \leq 10$ para todo n. Además, como existe algún n_0 tal que $b < a_{n_0}$, la sucesión $a_n - b$ es positiva a partir de n_0. Si miramos, como antes, el mayor elemento del conjunto:

$$\mathcal{T}_1 = \{m \in \mathbb{Z} \,:\, m < 10 \cdot (a_n - b) \text{ para algún } n\}$$

tenemos que ese número está entre 0 y 9. Llamamos x_1 a dicho elemento y lo tomamos como el primer dígito de la expresión decimal del número ℓ luego de la coma. El procedimiento es el mismo para calcular los dígitos subsiguientes. Supongamos que ya calculamos los primeros k dígitos después de la coma y obtuvimos la expresión $b, x_1x_2 \ldots x_k$. Para calcular el dígito siguiente, x_{k+1} consideramos el conjunto:

$$\mathcal{T}_{k+1} = \{m \in \mathbb{Z} \,:\, m < 10^{k+1} \cdot (a_n - b, x_1x_2 \ldots x_k) \text{ para algún } n\}$$

El máximo de este conjunto está entre 0 y 9 y ése es el dígito x_{k+1}.

Veamos en un ejemplo concreto cómo funciona este método.

Ejemplo. Consideremos la sucesión creciente y acotada $a_n = 1 - \frac{1}{10^n}$. Los primeros términos de la sucesión son $a_1 = 1 - \frac{1}{10} = 0{,}9$, $a_2 = 1 - \frac{1}{100} = 0{,}99$, $a_3 = 0{,}999$, etc. Llamemos ℓ al número real que define esta sucesión. Intuitivamente, el número ℓ debería tener por expresión decimal $0{,}\overline{9}$; es decir que ℓ sería el número racional de período 9, que es igual al número entero 1. Veamos que éste es el caso.

Para determinar el número antes de la coma, debemos mirar el mayor número entero menor que a_n para algún n. Claramente, todos los términos de la sucesión son mayores que 0 y menores que 1. Luego, el número b es 0. Es decir que la expresión decimal de ℓ tiene un 0 antes de la coma. Para calcular el primer dígito luego de la coma, debemos multiplicar por 10 la sucesión $a_n - b = a_n$. Así obtenemos la sucesión $10 \cdot a_1 = 9$, $10 \cdot a_2 = 9{,}9$, $10 \cdot a_3 = 9{,}99$, etc. El mayor número entero que sea más chico que algún término de esta sucesión es el número 9. Luego, el primer dígito del número ℓ luego de la coma es el 9.

Para calcular el siguiente dígito, debemos considerar la sucesión $100 \cdot (a_n - 0{,}9)$, cuyos términos son 0;9; 9,9; 9,99, etc. El mayor número entero más chico que algún término de esta sucesión es el 9, y por lo tanto el desarrollo decimal de ℓ hasta este punto es 0,99. Así siguiendo, vemos que todos los dígitos de ℓ luego de la coma serán nueves, o sea $\ell = 0{,}\overline{9}$.

Ejemplo. Consideremos las sucesión constante $a_n = 1$. ¿Cuál es la expresión decimal asociada al número ℓ que define esta sucesión? Intuitivamente uno espera que la expresión decimal de ℓ sea 1. Aplicando el procedimiento anterior a esta nueva sucesión, vemos que para encontrar el dígito antes de la coma, debemos mirar el mayor entero menor que 1. Claramente, el mayor entero menor que 1 es el número 0. Luego $\ell = 0$, ...

Para calcular el primer dígito después de la coma, debemos mirar la sucesión $(10a_n)_{n\geq 1}$. Esta sucesión toma los valores $10 \cdot a_1 = 10 \cdot 1 = 10$; $10 \cdot a_2 = 10 \cdot 1 = 10$, etcétera; o sea que es la sucesión cuyos términos son todos iguales a 10.

El mayor número entero menor que 10 es el 9, luego el primer dígito después de la coma de ℓ es 9. En todos los pasos siguientes del procedimiento obtenemos la sucesión constantemente 10, y por lo tanto todos los dígitos de la expresión decimal de ℓ son nueves. Así podemos deducir que $\ell = 0{,}\overline{9}$. Recordemos que el número racional $0{,}\overline{9}$ coincide con el número natural 1, simplemente obtuvimos una representación decimal distinta del resultado esperado.

El procedimiento que describimos anteriormente tiene la particularidad de que la expresión de los números decimales exactos termina con infinitos nueves. Por otra parte, sin importar la sucesión que se elija para representar a un número, el procedimiento va a devolver la misma expresión decimal.

Para encontrar el desarrollo decimal de ℓ supusimos que todos los términos de la sucesión a_n eran positivos. Si algunos son menores o iguales que 0 y otros son positivos,

se pueden cambiar los negativos por 0 y obtendremos una sucesión equivalente. En cambio, si la sucesión no tiene términos positivos, hay dos casos posibles. En un caso, la sucesión converge al número 0, y se decreta que la expresión decimal de ℓ en este caso es simplemente 0. En el otro caso, la sucesión no converge al número 0, y se debe aplicar el Teorema 5.5. En efecto, podemos encontrar una sucesión c_n decreciente y de términos negativos tal que $\lim_{n\to\infty}(c_n - a_n) = 0$. El procedimiento se debe aplicar entonces a la sucesión creciente $(-c_n)_{n\geq 1}$ y poner un signo menos a la expresión decimal así obtenida.

Es importante destacar que este procedimiento es teórico. Es decir, nos muestra que todo número real tiene una expresión decimal, pero dada una sucesión creciente acotada de números racionales en general es imposible obtener los dígitos de manera concreta, a menos que se disponga de información adicional.

5.2. La recta real

Otra interpretación de los números reales está dada por el conjunto de puntos de la recta. Vimos en las secciones anteriores que los números racionales no llenan la recta, porque hay puntos cuya distancia al origen no podemos medir con ellos (por ejemplo la hipotenusa de un triángulo rectángulo de lado 1, como vimos en la figura 1). En la sección anterior probamos que podemos ver a los números reales como tiras infinitas de números cuyos dígitos están entre 0 y 9 más un signo. Esto nos permite marcar los números reales dentro de la recta, de la misma manera en que lo hacemos con los números decimales exactos. El lugar exacto en que se debe marcar un número es en general imposible de determinar dado que nuestra precisión es acotada, pero se puede ubicar con un error tan chico como se quiera.

Recíprocamente, a cualquier punto p de la recta se le puede asociar un número real. Llamamos x_1 a un entero que esté a la izquierda de p, e y_1 a un entero que esté a la derecha. Consideramos el intervalo $I_1 = [x_1, y_1]$. Partimos este intervalo al medio y obtenemos dos intervalos, el intervalo $[x_1, \frac{x_1+y_1}{2}]$ y el intervalo $[\frac{x_1+y_1}{2}, y_1]$. Nos fijamos en cuál de estos intervalos está el punto p, y llamamos I_2 al intervalo que lo contiene. Digamos que $I_2 = [x_2, y_2]$. Continuamos partiendo sucesivamente los intervalos $I_n = [x_n, y_n]$ por la mitad y en cada paso llamamos I_{n+1} al nuevo intervalo que contiene al punto p. Consideramos ahora la sucesión $(x_n)_{n\geq 1}$. Como los puntos x_n, y_n se obtienen como suma y cociente de números racionales, son todos números racionales. Además, es claro que la sucesión $(x_n)_{n\geq 1}$ es creciente y acotada. Es bastante intuitivo ver que p es el punto límite de la sucesión x_n, dado que estos puntos están tan cerca como uno quiera del punto p, como se puede ver en la figura 6. Luego, p se puede identificar con la clase de equivalencia de la sucesión $(x_n)_{n\geq 1}$, mostrando así que el conjunto de números reales describe todos los puntos de la recta.

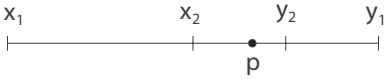


Figura 6. *Primeros intervalos que contienen a p.*

5.3. Orden

Nuestro próximo paso será definir y estudiar el orden de los números reales.

Si $x = C\,[(a_n)_{n\geq 1}]$ e $y = C[(b_n)_{n\geq 1}]$ son dos números reales diferentes, decimos que $x < y$ si existe $n_0 \in \mathbb{N}$ tal que $a_n < b_{n_0}$ para todo $n \in \mathbb{N}$; es decir, si todos los términos de la sucesión $(a_n)_{n\geq 1}$ son menores que algún término de la sucesión $(b_n)_{n\geq 1}$.

Notar que si x e y son números racionales y las sucesiones $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ son las sucesiones constantes x e y respectivamente, el orden definido de esta manera coincide con el orden usual.

La definición de $<$ es correcta en el sentido de que no depende de qué sucesiones se elijan para representar a los números reales x e y. Es decir, si $(a_n)_{n\geq 1}$ y $(\tilde{a}_n)_{n\geq 1}$ son dos sucesiones que representan al número x, y si $(b_n)_{n\geq 1}$ y $(\tilde{b}_n)_{n\geq 1}$ son dos sucesiones que representan al número y, entonces todos los términos de la sucesión $(a_n)_{n\geq 1}$ son menores que algún término de la sucesión $(b_n)_{n\geq 1}$ si y sólo si todos los términos de la sucesión $(\tilde{a}_n)_{n\geq 1}$ son menores que algún término de la sucesión $(\tilde{b}_n)_{n\geq 1}$ en cada clase de equivalencia.

Por otro lado, es inmediato ver que la relación $\leq$ definida en $\mathbb{R}$ por la relación $x \leq y$ si y sólo si $x = y$ o bien $x < y$ es una relación de orden. Más aún, la relación $\leq$ es una relación de orden *total*, es decir, si x e y son dos números reales cualesquiera, entonces o bien $x \leq y$ o bien $y \leq x$. La demostración de estos hechos excede el nivel de este libro y la omitimos.

En resumen:

Proposición 5.7. *La relación $\leq$ está bien definida y es una relación de orden total en $\mathbb{R}$.*

Como ya vimos, todo número real se puede dar por su desarrollo decimal. El orden lexicográfico descripto en la sección 4.2 para las expresiones decimales de dos números reales coincide con el orden que describimos aquí, y se puede usar como definición alternativa.

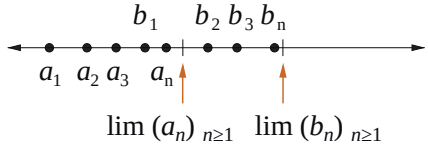


Figura 7. *Gráfico del orden de números reales.*

5.4. Operaciones

En esta sección definimos la suma y el producto de dos números reales. Aquí se puede apreciar la ventaja de presentar a estos números por medio de sucesiones, y no por su desarrollo decimal. En efecto, no es claro cómo, a partir de dos representaciones decimales infinitas, se puede calcular la representación de la suma o el producto. El principal obstáculo en este punto es el acarreo en la suma de expresiones infinitas.

Sean $x = C[(a_n)_{n\geq 1}], y = C[(b_n)_{n\geq 1}] \in \mathbb{R}$. Definimos la suma $x + y$ como sigue:

$$x + y = C[(a_n + b_n)_{n\geq 1}]$$

En el caso en que $x > 0$ e $y > 0$, elegimos $a_n > 0$ y $b_n > 0$ para todo n y definimos:

$$x \cdot y = C[(a_n \cdot b_n)_{n\geq 1}]$$

Se desprende del ejercicio 5.7 que el resultado de sumar dos números reales es un número real, y que el resultado de multiplicar dos números reales positivos es un número real positivo. Para definir el producto $x \cdot y$ para todo par de números reales utilizamos la misma técnica de la sección 4.3.

Para ver que estas operaciones están bien definidas, debemos ver que, sin importar qué sucesiones elijamos en cada clase de equivalencia, al sumar o multiplicar obtenemos sucesiones equivalentes. En efecto, sabemos que dos sucesiones distintas en *Sucec*($\mathbb{Q}$) pueden representar el mismo número real.

Proposición 5.8. *Sean* $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$, $(c_n)_{n\geq 1}$, $(d_n)_{n\geq 1}$ *sucesiones en Sucec*($\mathbb{Q}$) *tales que* $(a_n)_{n\geq 1} \sim (c_n)_{n\geq 1}$ *y* $(b_n)_{n\geq 1} \sim (d_n)_{n\geq 1}$. *Entonces*

- $(a_n + b_n)_{n\geq 1} \sim (c_n + d_n)_{n\geq 1}$
- $(a_n \cdot b_n)_{n\geq 1} \sim (c_n \cdot d_n)_{n\geq 1}$

En particular la suma y el producto definidos en 5.4 no dependen del sistema de representantes, y por lo tanto son operaciones bien definidas.

Demostración. Como $(a_n)_{n\geq 1} \sim (c_n)_{n\geq 1}$ y $(b_n)_{n\geq 1} \sim (d_n)_{n\geq 1}$ se sigue que $\lim_{n\to\infty} a_n - c_n = 0$ y $\lim_{n\to\infty} b_n - d_n = 0$. Luego $\lim_{n\to\infty} (a_n - c_n) + (b_n - d_n) = 0$, y por lo tanto $\lim_{n\to\infty} (a_n + b_n) - (c_n + d_n) = 0$, probando de esta manera que $(a_n + b_n)_{n\geq 1} \sim (c_n + d_n)_{n\geq 1}$.

Para probar la segunda parte de la proposición, probemos que $\lim_{n\to\infty} (a_n \cdot b_n) - (c_n \cdot d_n) = 0$. Para ver esto, escribimos esta diferencia del siguiente modo:

$$(a_n \cdot b_n) - (c_n \cdot d_n) = (a_n \cdot b_n) - (b_n \cdot c_n) + (b_n \cdot c_n) - (c_n \cdot d_n)$$

Sacando factor común, obtenemos la igualdad:

$$(a_n \cdot b_n) - (c_n \cdot d_n) = b_n \cdot (a_n - c_n) + c_n \cdot (b_n - d_n)$$

Como $\lim_{n\to\infty} a_n - c_n = 0$, $\lim_{n\to\infty} b_n - d_n = 0$ y tanto $(b_n)_{n\geq 1}$ como $(c_n)_{n\geq 1}$ son sucesiones acotadas, inferimos que $\lim_{n\to\infty} (a_n \cdot b_n) - (c_n \cdot d_n) = 0$. En efecto, si una sucesión es acotada y otra tiene límite 0, entonces el producto de ambas tiene también límite 0.

A partir de la suma y el producto definidos de esta manera, se puede demostrar el siguiente teorema.

Teorema 5.9.
1. Si $a \in \mathbb{R}$ entonces existe un único número real x que satisface la ecuación $a + x = 0$.
2. Si $a \in \mathbb{R}$ y $a \neq 0$, entonces existe un único número real y que satisface la ecuación $a \cdot y = 1$.

Demostración. Si a es la clase de la sucesión $(a_n)_{n\geq 1}$, la existencia de una sucesión $(x_n)_{n\geq 1}$ en $Sucec(\mathbb{Q})$ tal que $C[(a_n + x_n)_{n\geq 1}] = 0$ ya se vio en la sección 4.3. También se vio la existencia de una sucesión $(y_n)_{n\geq 1}$ en $Sucec(\mathbb{Q})$ tal que $C[(a_n \cdot y_n)_{n\geq 1}] = 1$. Falta ver que cualquier otra sucesión que cumpla la misma propiedad es equivalente a éstas.

Sea $(x'_n)_{n\geq 1}$ otra sucesión tal que $C[(a_n + x'_n)_{n\geq 1}] = 0$. Entonces, tenemos que $\lim_{n\to\infty}(a_n + x_n) = 0$ y $\lim_{n\to\infty}(a_n + x'_n) = 0$. Por lo tanto, restando, tenemos
$\lim_{n\to\infty}(x_n - x'_n) = \lim_{n\to\infty}((a_n + x_n) - (a_n + x'_n)) = 0$. Es decir, $C[(x_n)_{n\geq 1}] = C[(x'_n)_{n\geq 1}]$

La prueba para el producto es más técnica y la omitimos.

Los números reales x e y del teorema son respectivamente el inverso aditivo y el inverso multiplicativo de a. A partir del teorema, se demuestra que las ecuaciones del tipo $a + x = b$ y $a \cdot y = b$ (en el caso en que $a \neq 0$) tienen solución única en el conjunto de los números reales. Es decir, podemos *restar* dos números y dividir por un número distinto de 0. Al valor de x lo notamos con $x = b - a$; al valor de y *l*o notamos con $y = b/a$.

A partir de las operaciones definidas en el conjunto $\mathbb{R}$, se puede probar que la suma es asociativa, conmutativa, con elemento neutro y, como dijimos, todo elemento tiene un inverso aditivo. Además, el producto es asociativo, conmutativo, con elemento neutro, y todo número real distinto de 0 tiene un inverso multiplicativo. Por último, se puede ver que el producto es distributivo sobre la suma. En resumen, se tiene el siguiente resultado:

Teorema 5.10. *El conjunto $\mathbb{R}$ es un cuerpo, denominado el* cuerpo de números reales.

5.5. Raíces

Los números reales permiten resolver muchas ecuaciones que no tienen solución en el conjunto de los números racionales. Ya vimos que una de estas ecuaciones es la ecuación $x^2 = 2$. Otro tipo de ecuaciones que se pueden resolver en el conjunto $\mathbb{R}$ son las ecuaciones del tipo $x^n = a$, donde a es un número real positivo y n es un número natural. En este sentido, el Teorema 5.6 se puede generalizar mostrando que *la ecuación $x^n = a$ admite una única solución positiva*.

Dicha solución se denomina *la raíz enésima de a*. Simbólicamente la raíz enésima de a se escribe con $\sqrt[n]{a}$.

A partir de este resultado se puede definir la *exponenciación fraccionaria*. En efecto, si a es un número real positivo y m/n es un número racional, se define:

$$a^{\frac{m}{n}} = \sqrt[n]{a^m}$$

Para comprender el porqué de esta definición debemos tener en cuenta la siguiente propiedad básica de la exponenciación: si k, l son números naturales, entonces $(a^k)^l = a^{k \cdot l}$. Ahora bien, si $k = \frac{m}{n}$ y $l = n$, para que esta propiedad siga valiendo, debemos tener $(a^{\frac{m}{n}})^n = a^{\frac{m}{n} n} = a^m$. Por lo tanto, se debe definir, como hemos hecho, $a^{\frac{m}{n}} = \sqrt[n]{a^m}$

Ejercicio 5.11. Probar que si $a \in \mathbb{R}_{>0}$ entonces $(a^k)^l = a^{k \cdot l}$ para todo par de números racionales k, l.

Como conclusión, los números reales nos permiten generalizar algunas operaciones algebraicas, como la exponenciación, cuando el exponente es un número racional en lugar de un número entero. Usando límites, también se puede definir la exponenciación cuando el exponente es un número real. Esta definición es más técnica y la omitiremos en el presente libro.

5.6. Completitud de los números reales

En las secciones anteriores introdujimos el orden y la suma (y resta) de números reales. Con estas herramientas, se puede dar una definición de límite para sucesiones de números reales, de manera análoga a como se hizo en la sección 3. Esta noción de límite coincide con la anterior cuando se la utiliza para sucesiones de números racionales con límite racional.

Consideremos ahora una sucesión $(a_n)_{n \geq 1} \in Sucec(\mathbb{Q})$. Esta sucesión representa a un número real que llamaremos ℓ. Por otra parte, cada término a_k de la sucesión se puede ver como un número real, considerando la clase de equivalencia de la sucesión constante a_k. Una propiedad interesante del límite de sucesiones de números reales es que el límite de la sucesión de los números a_k(vistos como números reales) es precisamente ℓ.

La propiedad más importante del conjunto de los números reales es que es *completo*. Esto quiere decir lo siguiente: cualquier sucesión **de números reales** $(x_n)_{n \geq 1}$ creciente y acotada tiene límite en el conjunto de los números reales.

En resumen, en este capítulo comenzamos viendo que los números racionales no son completos, en el sentido de que hay sucesiones crecientes y acotadas de números racionales que no tienen límite en el conjunto de los racionales. Entonces, agregamos al conjunto de los números racionales los límites de estas sucesiones, formando así el conjunto de los números reales. La noción de límite de los números racionales se extiende al conjunto de números reales, y, finalmente, con esta noción de límite, resulta que las sucesiones crecientes y acotadas de números reales *tienen límite* en el conjunto de los números reales. Es decir, hemos creado un conjunto de números completo.

5.7. Números importantes

Un número real importante en el análisis matemático es el *número e* *[13]. Este número aparece en diferentes áreas de la matemática como probabilidad, combinatoria, ecuaciones diferenciales, matemática financiera, entre otras.

El número *e* se puede definir mediante la siguiente sucesión creciente y acotada de números racionales:

$$a_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!}$$

Los primeros términos de esta sucesión, calculados con 60 decimales, son:

a_1 = 2,0
a_2 = 2,5
a_3 = 2,666666666666666666666666666666666666666666666666666666666666
a_4 = 2,708333333333333333333333333333333333333333333333333333333333
a_5 = 2,716666666666666666666666666666666666666666666666666666666666
a_6 = 2,718055555555555555555555555555555555555555555555555555555555
a_7 = 2,718253968253968253968253968253968253968253968253968253968253
a_8 = 2,718278769841269841269841269841269841269841269841269841269841
a_9 = 2,718281525573192239858906525573192239858906525573192239858906
a_{10} = 2,718281801146384479717813051146384479717813051146384479717813
a_{11} = 2,718281826198492865159531826198492865159531826198492865159531
a_{12} = 2,718281828286168563946341724119501897279675057452835230613008

Puede compararse este resultado con los primeros 120 dígitos del desarrollo decimal de *e*:

e = 2,71828 18284 59045 23536 02874 71352 66249 77572 47093 69995 95749 66967 62772 40766
30353 54759 45713 82178 52516 64274 27466 39193 20030 59921

Es claro que $(a_n)_{n\geq 1}$ es una sucesión creciente de números racionales. No es tan claro que es acotada. Esto puede probarse utilizando las siguientes propiedades que se prueban fácilmente por inducción:

- $n! \geq 2^n$ para todo $n \in \mathbb{N}$,
- $\frac{1}{2} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$ para todo $n \in \mathrm{N}$.

En efecto,
$$a_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \leq 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = 3 - \frac{1}{2^n} < 3$$

para todo $n \in \mathbb{N}$. Hemos probado que la sucesión $(a_n)_{n\geq 1}$ está acotada superiormente por 3, con lo cual define un número real. Podemos refinar la cuenta anterior de la siguiente manera:

*[13] La primera referencia al número *e* fue publicada en una tabla en un apéndice de un trabajo del matemático escocés John Napier. A pesar de que Napier no usó la constante misma, calculó el valor de algunos logaritmos con ella. El *descubrimiento* real de la constante se debe a Jacob Bernoulli, al tratar de calcular el límite de la sucesión $b_n = (1 + 1/n)^n$. Leonhard Euler fue el primero en usar la letra e para dicha constante en 1727 y la primera publicación de *e* fue su trabajo *Mechanica* de 1736.

$$\begin{aligned} a_n &\leq 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots + \frac{1}{2^n} \\ &= 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots + \frac{1}{2^n} - \frac{1}{4} + \frac{1}{6} \\ &= 3 - \frac{1}{2^n} - \frac{1}{4} + \frac{1}{6} < 3 - \frac{1}{12} \end{aligned}$$

por lo que $2 < e < 3$ y entonces e no es entero.

Teorema 5.11. *El número e es irracional.*

La prueba de este hecho es un poco más técnica que otras pruebas del libro. La incluimos, de todos modos, para el lector interesado.

Demostración. Supongamos que e es un número racional m/d. Como e no es entero, $d > 1$. Llamemos N al número

$$\begin{aligned} N &= d! \cdot \left(e - \left(1 + \frac{1}{1!} + \cdots + \frac{1}{d!} \right) \right) \\ &= d! \left(\frac{m}{d} - \left(1 + \frac{1}{1!} + \cdots + \frac{1}{d!} \right) \right) \\ &= m \cdot (d-1)! - \left(d! + \frac{d!}{1} + \frac{d!}{2!} + \cdots + \frac{d!}{d!} \right) \end{aligned}$$

Claramente N es un número entero ya que $\frac{d!}{k!} = (k+1) \cdot (k+2) \cdots d$ es entero si $k \leq d$. Veamos que, sin embargo, $0 < N < 1$, lo que es imposible para un número entero.

Por la definición del número e, deducimos que el número real $e - \left(1 + \frac{1}{1!} + \cdots + \frac{1}{d!}\right)$ está definido por la sucesión:

$$c_n = \begin{cases} 0 & \text{si } n \leq d \\ \frac{1}{(d+1)!} + \frac{1}{(d+2)!} + \cdots + \frac{1}{n!} & \text{si } n > d \end{cases}$$

Luego, el número N está definido por la sucesión $(d! \cdot c_n)_{n \geq 1}$, cuyos términos son todos positivos para $n > d$, con lo cual $N > 0$. Para ver que $N < 1$, notamos que si $k > d$,

$$\frac{d!}{k!} = \frac{1}{(d+1) \cdot (d+2) \cdots k} \leq \frac{1}{(d+1)^{k-d}}$$

Además, la desigualdad es estricta si $k > d + 1$. Esto implica que si $n > d + 1$,

$$d! \cdot c_n = \frac{d!}{(d+1)!} + \frac{d!}{(d+2)!} + \cdots + \frac{d!}{n!} < \frac{1}{d+1} + \frac{1}{(d+1)^2} + \cdots + \frac{1}{(d+1)^{n-d}}$$

Puede probarse por inducción que, para todo k natural,

$$\frac{1}{d+1} + \frac{1}{(d+1)^2} + \cdots + \frac{1}{(d+1)^k} = \frac{1}{d} - \frac{1}{d} \cdot \frac{1}{(d+1)^k} < \frac{1}{d}$$

Luego, concluimos que $N \leq 1/d < 1$ (porque $d > 1$).

Una forma alternativa con la que habitualmente se presenta al número e es con la sucesión:

$$b_n = \left(1 + \frac{1}{n}\right)^n$$

Otro número de vital importancia en la ciencia es el número π. En geometría, π se puede definir como el cociente entre la longitud de una circunferencia y su diámetro[14]. De hecho, el número π tiene su origen en el deseo de medir la longitud de una circunferencia y el área de un círculo. Las primeras aproximaciones conocidas de π, debidas a los babilonios y los egipcios, se remontan al 1900 a.C. y eran 25/8 y 256/81 respectivamente. Esta última apareció en el *papiro Rhind*, bajo la afirmación de que el área de un círculo es similar a la de un cuadrado cuyo lado es igual al diámetro del círculo disminuido en 1/9, es decir, igual a 8/9 del diámetro. El primero en construir una sucesión que permitía aproximar π tanto como se quisiera fue Arquímedes (287-212 a.C.) en su trabajo *Medida de un círculo*.

Desde entonces, se han construido distintas sucesiones que definen al número π. Entre ellas, podemos mencionar la siguiente sucesión creciente y acotada de números racionales:

$$a_n = 2 + 2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{3} \cdot \frac{2}{5} + \cdots + 2 \cdot \frac{1}{3} \cdot \frac{2}{5} \cdots \frac{n}{2 \cdot n + 1}$$

Es claro que la sucesión $(a_n)_{n \geq 1}$ es una sucesión creciente de números racionales.

Para ver que es acotada, basta observar que, para cada $k \in \mathbb{N}$, se tiene que $\frac{k}{k+1} < \frac{1}{2}$, y entonces:

$$\begin{aligned}
a_n &= 2 + 2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{3} \cdot \frac{2}{5} + \cdots + 2 \cdot \frac{1}{3} \cdot \frac{2}{5} \cdots \frac{h}{2 \cdot n + 1} \\
a_n &< 2 + 2 \cdot \frac{1}{2} + 2 \cdot \frac{1}{2} \cdot \frac{1}{2} + \cdots + 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} \qquad (1) \\
2 + 2 \cdot \frac{1}{2} + 2 \cdot \frac{1}{2} \cdot \frac{1}{2} + \cdots + 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} &= 2\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n}\right) = 2\left(2 - \frac{1}{2^n}\right) \\
&= 4 - \frac{1}{2^{n-1}} \qquad (2) \\
\text{De (1) y (2), entonces: } a_n &< 4 - \frac{1}{2^{n-1}}
\end{aligned}$$

lo que nos dice que $a_n < 4$ para todo $n \in \mathbb{N}$. Los primeros términos de esta sucesión, calculados con 20 cifras decimales son:

a_1 = 2,66666666666666666666
a_2 = 2,93333333333333333333
a_3 = 3,04761904761904761904
a_4 = 3,09841269841269841269
a_5 = 3,12150072150072150072
a_6 = 3,13215673215673215673

[14] El primer uso de la letra griega π para esta constante se encuentra en el libro *A New Introduction to Mathematics* de William Jones, del año 1706. Esta notación se popularizó luego de que la adoptara Leonhard Euler en 1737.

a_7 = 3,13712953712953712953
a_8 = 3,13946968064615123438
a_9 = 3,14057816968033686299
a_{10} = 3,14110602160137763852
a_{11} = 3,14135847252013627030
a_{12} = 3,14147964896114041355
a_{13} = 3,14153799317347574178
a_{14} = 3,14156615934494796921
a_{15} = 3,14157978813759582119
a_{16} = 3,14158639603706144639
a_{17} = 3,14158960558823046434
a_{18} = 3,14159116699150187848
a_{19} = 3,14159192767514692640
a_{20} = 3,14159229874033963270

El número π tampoco es racional, aunque la demostración es algo más complicada que en el caso de *e*. Los primeros 120 dígitos del desarrollo decimal de π son:

π = 3,14159 26535 89793 23846 26433 83279 50288 41971 69399 37510 58209 74944 59230 78164
06286 20899 86280 34825 34211 70679 82148 08651 32823 06647

En la actualidad se conocen más de 10^{12} cifras del desarrollo decimal de π. La mejor aproximación posible de π por un número racional con numerador y denominador de hasta cuatro dígitos es 355/113 (3,1415929 ...).

6. Números complejos

□ 1. Introducción

Ya vimos en el capítulo de números reales que todo número real positivo tiene una raíz cuadrada. Los números negativos, en cambio, no tienen una raíz **real**. Uno de los grandes avances de la matemática se produjo al *inventar* raíces cuadradas de los números negativos. Esto lo hicieron fundamentalmente Girolamo Cardano y Lodovico Ferrari alrededor de 1540. No obstante, esto significaba un salto de abstracción que no todos los matemáticos de la época estaban en condiciones de dar. La definición moderna de los números complejos es muy posterior, y se debe a William Rowan Hamilton, en el año 1833. Para definir los complejos, Hamilton introdujo un nuevo símbolo, la letra i, que corresponde a un número cuyo cuadrado es -1. Claro, si queremos operar con este nuevo número, tenemos que ser capaces de sumarle otros números reales, y también de multiplicarlo por ellos. Por ejemplo, tenemos que permitir números como $2{,}34 \cdot \pi \cdot i - 4{,}5 \cdot (2 + 3 \cdot i)$. ¿Cuáles son, exactamente, todos los números que estamos agregando al introducir i? Si b es un número real, agregamos $b \cdot i$. Y si a es un número real, agregamos $a + b \cdot i$. Y podemos ver que con esto basta.

Si tenemos dos números de esta forma, $a + b \cdot i$ y $a' + b' \cdot i$, entonces los podemos sumar y obtenemos un número de esta forma: $(a + b \cdot i) + (a' + b' \cdot i) = a + a' + b \cdot i + b' \cdot i = (a + a') + (b + b') \cdot i$. Y también los podemos multiplicar. Usando la propiedad distributiva, la conmutativa y que $i^2 = -1$, obtenemos que:

$$\begin{aligned}(a + b \cdot i) \cdot (a' + b' \cdot i) &= a \cdot a' + a \cdot b' \cdot i + b \cdot i \cdot a' + b \cdot i \cdot b' \cdot i \\ &= a \cdot a' + (a \cdot b' + b \cdot a') \cdot i + b \cdot b' \cdot i^2 \\ &= a \cdot a' + (a \cdot b' + b \cdot a') \cdot i + b \cdot b' \cdot (-1) \\ &= a \cdot a' + (a \cdot b' + b \cdot a') \cdot i - b \cdot b' \\ &= (a \cdot a' - b \cdot b') + (a \cdot b' + b \cdot a') \cdot i\end{aligned}$$

Es decir, el producto de dos números de la forma $a + b \cdot i$ es de la forma $\bar{a} + \bar{b} \cdot i$. Quiere decir que podemos definir nuestro nuevo conjunto de números, el de los números complejos, como aquellos que se escriben en la forma $a + b \cdot i$, donde a y b son números reales. Usualmente, omitimos el punto y escribimos $a + bi$. El conjunto de los números complejos se escribe $\mathbb{C}$.

Ejemplo. Los siguientes son números complejos: $2 + 3i$; $2 + 3{,}14i$; $-17 + 3/7i$; $-2 + i$ (que es igual a $-2 + 1i$); $2i$ (que es igual a $0 + 2i$); 1 (que es igual a $1 + 0i$). Si $z = 2 + 3i$ y $w = 1 + 4i$, entonces:

$$\begin{aligned}z + w &= (2 + 3i) + (1 + 4i) \\ &= 3 + 7i\end{aligned}$$

$$\begin{aligned} zw &= (2 + 3i) \cdot (1 + 4i) \\ &= 2 + 2 \cdot 4i + 3i \cdot 1 + 3i \cdot 4i \\ &= 2 - 12 + (8 + 3)i \\ &= -10 + 11i \end{aligned}$$

$$\begin{aligned} z - w &= (2 + 3i) - (1 + 4i) \\ &= 2 + 3i - 1 - 4i \\ &= 1 - i \end{aligned}$$

Ejercicio 6.1. Si $z = -2+6i$ y $w = \frac{1}{2} + 2i$, calcular $z - w$, $w - z$, $2z$, $4w - 3z$, $z \cdot w$, z^2.

Así como los números reales, salvo el 0, tienen inverso, los números complejos, salvo el 0, también tienen inverso. Pero para encontrar el inverso de un número complejo hay que aprender un poco más de la estructura de los números complejos.

Se dice que un número complejo tiene una *parte real* y una *parte imaginaria*. La parte real es la que no acompaña a i, mientras que la parte imaginaria es el número real que acompaña a i. Si $z = 2 + 7i$, la parte real de z es 2 y la parte imaginaria de z es 7. Escribimos $\mathrm{Re}(z)$ la parte real de z, e $\mathrm{Im}(z)$ la parte imaginaria de z. Es decir, $\mathrm{Re}(2 + 7i) = 2$ e $\mathrm{Im}(2 + 7i) = 7$. Otros ejemplos: $\mathrm{Re}(\pi - i) = \pi$, $\mathrm{Im}(\pi - i) = -1$, $\mathrm{Re}(i) = \mathrm{Re}(0 + 1 \cdot i) = 0$, $\mathrm{Im}(1) = \mathrm{Im}(1 + 0 \cdot i) = 0$.

Observación. Los números reales son también números complejos; por ejemplo $4 = 4 + 0i$, y 4 es un número natural, por lo tanto también entero, racional y real, y por lo tanto también complejo. En términos de conjuntos:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Vistos como números complejos, los reales son aquéllos que tienen parte imaginaria igual a 0.

Si $z = a + bi$ es un complejo, llamamos *conjugado* de z al complejo $a - bi$, y lo escribimos $\bar{z}$. Es decir:

$$\overline{a + bi} = a - bi, \quad \text{y entonces } \mathrm{Re}(\bar{z}) = \mathrm{Re}(z), \quad \mathrm{Im}(\bar{z}) = -\mathrm{Im}(z)$$

Ejercicio 6.2. El conjugado de $7 + 2i$ es $7 - 2i$. ¿Cuál es el conjugado de $7 - 2i$? Calcular además $\bar{4}$, $\bar{i}$, $-\bar{i}$.

La principal utilidad de conjugar números complejos es que $z \cdot \bar{z}$ es un número real, como podemos ver en esta cuenta, en la que $z = a + bi$:

$$z\bar{z} = (a + bi)(a - bi) = a^2 - abi + bia - b^2 i^2 = a^2 + b^2$$

Y no sólo es un número real: es un real positivo, distinto de 0 a menos que z sea 0. Esto es porque como a y b son números reales, $a^2 \geq 0$ y $b^2 \geq 0$. Y la única manera en que $a^2 + b^2$ puede ser 0 es que tanto a como b sean 0, es decir que z sea 0.

□ 2. Dibujos

Para trabajar con números complejos resulta útil graficarlos en el plano. Para eso, dibujamos un complejo $z = a + bi$ con coordenadas a y b. Es decir, sus coordenadas están dadas por su parte real y su parte imaginaria. En la figura 1 dibujamos 3; $1 + i$; $2 - i$; $-3 + 2i$; $-3 - 2i$; i y $-i$. Si queremos medir la distancia en el plano de un número complejo al 0, debemos usar el teorema de Pitágoras. En la figura 2 se calcula la distancia de $3 + 2i$ al 0, que es $\sqrt{2^2 + 3^2} = \sqrt{13}$. Dado un complejo $z = a + bi$, su módulo $|z|$ es la distancia al 0. Es decir:

$$|a + bi| = \sqrt{a^2 + b^2}$$

Antes vimos que si $z = a + bi$, entonces $z\,\bar{z} = a^2 + b^2$. Lo que vemos, entonces es que:

$$z\bar{z} = |z|^2. \text{ En particular, } z\bar{z} \in \mathbb{R}_{\geq 0}, \text{ y}$$
$$z\bar{z} = 0 \text{ si y sólo si } z = 0$$

Y esto dice cómo encontrar los inversos de los números complejos, ya que si $z \neq 0$, entonces $z\,\frac{\bar{z}}{|z|^2} = 1$, por lo que:

$$z^{-1} = \frac{\bar{z}}{|z|^2}$$

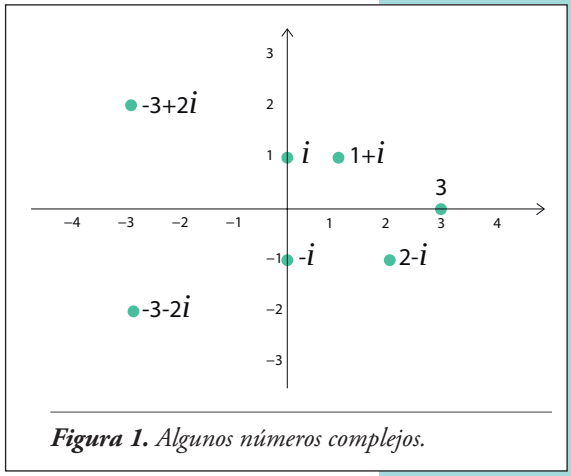


Figura 1. *Algunos números complejos.*

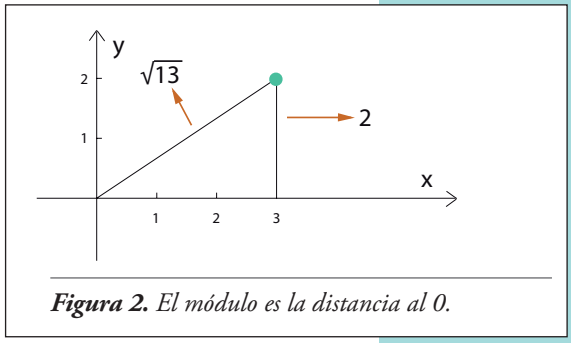


Figura 2. *El módulo es la distancia al 0.*

Ejemplos.

$$(3+4i)^{-1} = \frac{3-4i}{9+16}$$
$$= \frac{3-4i}{25}$$
$$= \frac{3}{25} - \frac{4}{25}i$$

$$(2+3i)/(3+4i) = (2+3i)\cdot(3+4i)^{-1}$$
$$= (2+3i)\cdot\left(\frac{3}{25} - \frac{4}{25}i\right)$$
$$= \frac{2\cdot 3 + 3\cdot 4}{25} + \frac{-2\cdot 4 + 3\cdot 3}{25}i$$
$$= \frac{18}{25} + \frac{1}{25}i$$

Ejercicio 6.3. Verificar que $(3 + 4i) \cdot (3/25 - 4/25\,i) = 1$ y que $(2 + 3i) = (18/25 + 1/25\,i) \cdot (3 + 4i)$.

□ 3. Distancia y desigualdad triangular

Dado que los complejos se dibujan en el plano y el módulo da una noción de distancia, podemos con los números complejos recuperar parte de la geometría en dos dimensiones.

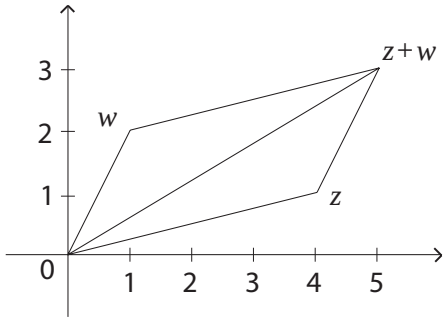


Figura 3. *Suma de $z = 4 + i$ más $w = 1 + 2i$.*

Lo primero que debemos hacer es entender la suma de dos complejos de manera geométrica. Lo que resulta, es algo que muchos denominan *regla del paralelogramo*; podemos verlo en la figura 3. Allí se suman $z = 4 + i$ con $w = 1 + 2i$. Para hacerlo analíticamente, simplemente sumamos la parte real y la imaginaria: $(4 + i) + (1 + 2i) = 5 + 3i$. Para hacerlo geométricamente, se puede pensar que en el punto $4 + i$ se para un vector[15] paralelo a w. Este vector termina en $1+2i$ pero corrido en $4+i$; esto es, termina en $5 + 3i$. Pero la suma es conmutativa; también puede pensarse que en el punto $1 + 2i$ paramos un vector paralelo a z, que terminará también en $5 + 3i$. Las dos formas de hacer la cuenta dan los lados de un paralelogramo que tiene vértices 0, z, w y $z + w$.

Pensemos ahora en el triángulo con vértices en 0, z y $z + w$. Como en todo triángulo, la longitud de uno de sus lados es menor a la suma de las longitudes de los otros dos. De hecho, es claro que ir de 0 a $z + w$ directamente es más corto que ir de 0 a z y luego de z a $z + w$. En términos de módulos, la distancia de 0 a $z + w$ es $|z + w|$, la distancia de 0 a z es $|z|$ y la distancia de z a $z + w$ es $|w|$. Resulta entonces que:

$$|z + w| \leq |z| + |w|$$

Esto vale para cualquier z y w en $\mathbb{C}$. Si ahora reemplazamos z por $x - w$ en la desigualdad anterior, resulta $|x - w + w| \leq |x - w| + |w|$. Es decir:

$$|x - w| \geq |x| - |w|$$

Esto vale para cualquier x y w en $\mathbb{C}$.

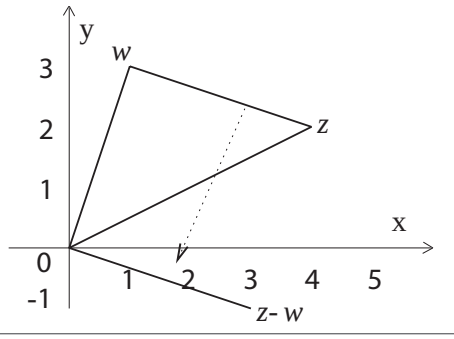


Figura 4. *Diferencia y distancia.*

En el párrafo anterior utilizamos un concepto clave, que permite obtener la distancia entre dos complejos cualesquiera. Ya vimos que el módulo $|z|$ da la distancia de z a 0. ¿Cómo se puede obtener la distancia entre dos complejos z y w ? La solución es cambiarle el nombre a z y w. Lo que vimos es que la distancia de x a $x + y$ es $|y|$. Si ahora x es z y $x + y = w$, entonces $y = w - x = w - z$, con lo que obtenemos que la distancia de z a w es $|y| = |w - z|$. Esta deducción que hicimos algebraicamente también se puede hacer de manera geométrica, como en la figura 4. En la figura calculamos geométricamente $z - w$ que, visto como vector, es paralelo al vector que nace en w y termina en z. Luego, la distancia de w a z, que es el módulo de ese vector, coincide con $|z - w|$.

[15] Un *vector* es un segmento con un sentido. Esto es, *comienza* en un punto y *termina* en otro. En un *segmento*, en cambio, no se distingue un extremo de otro.

□ 4. Los complejos forman un cuerpo

Así como los racionales o los reales, el conjunto de los números complejos forma un *cuerpo*. Es decir, la suma es conmutativa, asociativa y con elemento neutro (el 0), y todo elemento tiene un opuesto. Además, el producto es conmutativo y asociativo, con elemento neutro y todo elemento distinto del 0 tiene inverso. Y el producto distribuye sobre la suma. De todas estas propiedades, nos queda por verificar la asociativa y la conmutativa del producto, y la propiedad distributiva. Veamos que el producto es conmutativo. Para probarlo, usamos que el producto *de números reales* es conmutativo.

$$(a + bi)(c + di) = ac - bd + (ad + bc)i = ca - db + (da + cb)i = (c + di)(a + bi)$$

De la misma manera, usando que el producto de números reales es distributivo sobre la suma, tenemos:

$$\begin{aligned}(a + bi)\,((c + di) + (e + fi)) &= (a + bi)\,((c + e) + (d + f)i)\\ &= a(c + e) - b(d + f) + (a(d + f) + b(c + e))i\\ &= ac + ae - bd - bf + (ad + af + bc + be)i\end{aligned}$$

$$\begin{aligned}(a + bi)(c + di) + (a + bi)(e + fi) &= (ac - bd + (ad + bc)i) + (ae - bf + (af + be)i)\\ &= ac - bd + ae - bf + (ad + bc + af + be)i\end{aligned}$$

y vemos que ambas expresiones coinciden.

Por último, usando que el producto de números reales es asociativo, podemos probar que el de los complejos lo es:

$$\begin{aligned}(a + bi)\,((c + di)(e + fi)) &= (a + bi)(ce - df + (cf + de)i)\\ &= ace - adf - b(cf + de) + (a(cf + de) + b(ce - df))i\\ &= ace - adf - bcf - bde + (acf + ade + bce - bdf)i\end{aligned}$$

$$\begin{aligned}((a + bi)(c + di))\,(e + fi) &= (ac - bd + (ad + bc)i)(e + fi)\\ &= ace - bde - (ad + bc)f + (acf - bdf + ade + bce)i\\ &= ace - bde - adf - bcf + (acf - bdf + ade + bce)i\end{aligned}$$

y vemos que ambas expresiones coinciden.

□ 5. Un cuerpo no ordenado

Los racionales y los reales están ordenados: hay una relación $x < y$ que dice cuándo un número es menor que otro. Ese orden se comporta bien con la suma y el producto. A diferencia de $\mathbb{Q}$ y $\mathbb{R}$, en $\mathbb{C}$ no se puede establecer un orden que se lleve igual de bien con las operaciones. Veamos esto. Primero vamos a definir qué entendemos por "llevarse bien con la suma y el producto".

Una relación de orden $<$ en un cuerpo es **compatible con las operaciones** si se satisfacen las siguientes propiedades:

1. es una relación de orden **total**, esto es, si para todo par de elementos x, y una (y sólo una) de las siguientes afirmaciones es cierta: $x < y$, o $x = y$, o $x > y$;
2. si $x < y$ y z es un elemento cualquiera, entonces $x + z < y + z$;
3. si $x > 0$ e $y > 0$ entonces $x\,y > 0$.

Primero, veamos que si un cuerpo tiene un orden compatible con las operaciones entonces sucede que:

- si $a < a'$ y $b < b'$ entonces $a + b < a' + b'$;
- si $x > 0$ entonces $-x < 0$, y si $x < 0$ entonces $-x > 0$;
- para todo $x \neq 0$, es $x^2 > 0$.

Para probar la primera de estas afirmaciones, se utiliza dos veces la propiedad 1: por un lado, $a + b < a' + b$ y por el otro $a' + b < a' + b'$, así que $a + b < a' + b < a' + b'$.

La segunda afirmación se prueba por reducción al absurdo. Supongamos que $x > 0$ y que no es cierto que $-x < 0$. Entonces $-x \geq 0$, es decir, o bien $-x = 0$, o bien $-x > 0$. Pero si fuese $-x = 0$, entonces sería $x = 0$, que contradice $x > 0$. Y si fuese $-x > 0$, entonces como también $x > 0$ resulta $-x + x > 0+0$, es decir $0 > 0$, que es absurdo.

Por último, la tercera afirmación tiene dos posibilidades. O bien $x > 0$, en cuyo caso $x^2 = x \cdot x > 0$ por la propiedad 3, o bien $x < 0$, en cuyo caso $-x > 0$ y $x^2 = (-x) \cdot (-x) > 0$ de nuevo por la propiedad 3.

Ahora, supongamos que en los complejos hubiese un orden compatible con las operaciones. Entonces, podemos preguntarnos por i. Por la tercera de las afirmaciones anteriores, como $i \neq 0$, debe ser $i^2 > 0$, es decir $-1 > 0$. Pero entonces: $1 = -(-1) < 0$. Y por otra parte, $1 = (-1)^2 > 0$, nuevamente por la tercera afirmación. Tenemos entonces la contradicción de $1 < 0$ por un lado y $1 > 0$ por el otro.
Conclusión: no hay orden posible que sea compatible con las operaciones.

□ 6. Forma polar

Ya hemos dibujado números complejos en el plano, y definimos el módulo de un complejo como la distancia al 0. Ahora vamos a definir el *argumento,* que es un ángulo. Más precisamente, si z es un número complejo distinto de 0, su argumento es el ángulo entre la semirrecta que sale de 0 y pasa por 1 y la semirrecta que sale de 0 y pasa por z, yendo de la primera a la segunda en sentido antihorario, como se muestra en la figura 5. Al argumento del complejo z lo escribimos $\arg(z)$, y, midiendo los ángulos en radianes, se puede tomar

como un número entre 0 y 2π. El argumento es 0 si z es un real positivo, y es π si es un real negativo.

Recordemos cómo se mide un ángulo en radianes. Según la explicación técnica, se toma la intersección del ángulo sobre la circunferencia de radio 1 con centro en el vértice del ángulo, como en la figura 6, y se mide la *longitud* del arco que resulta.

La explicación sencilla es que 360° son 2π radianes y otros ángulos se obtienen proporcionalmente: 180° son π radianes, 90° son $\pi/2$ radianes, 60° son $\pi/3$ radianes, 120° son $2\pi/3$ radianes, etc.

Ejercicio 6.4. Calcular los argumentos de 4; $1 + i$; $2 + 2i$; $8i$; $-8i$; -7; $2-2i$.

Teniendo el argumento y el módulo de un complejo, se puede saber cuál es el complejo. Efectivamente, mirando la figura 7, se observa que el coseno y el seno del argumento de z se pueden calcular en términos de a y b.

Si $z = a + bi$ y $z \neq 0$, entonces $\cos(\arg(z)) = \frac{a}{|z|}$, y $\operatorname{sen}(\arg(z)) = \frac{b}{|z|}$.

Obtenemos que:

$$a = |z| \cos(\arg(z)),\ b = |z| \operatorname{sen}(\arg(z))$$

Entonces, un complejo se puede expresar por medio de su módulo y su argumento. Usaremos en este libro la notación $z = (|z| ; \arg(z))$. Es decir, $(r ; \alpha)$ es el complejo que tiene módulo r y argumento α. Esta forma de expresar un complejo se llama *forma polar*, para distinguirla de la *forma binómica* $z = a + bi$.

Como dijimos antes, de la forma polar a la binómica se pasa con senos y cosenos: $(r ; \alpha) = r \cos \alpha + ir \operatorname{sen} \alpha$. De la binómica a la polar se hace con las inversas: arcoseno y arcocoseno. Si $z = a + bi \neq 0$, entonces $r = \sqrt{a^2 + b^2}$ y α es el ángulo tal que $\cos \alpha = a/r$ y $\operatorname{sen} \alpha = b/r$. Se puede tomar arc cos a/r, que dará un ángulo entre 0 y π, es decir con parte imaginaria ≥ 0. Si $b \geq 0$, ése es el argumento, α = arc cos a/r. En cambio, si $b < 0$ se debe tomar $\alpha = 2\pi$ - arc cos a/r.

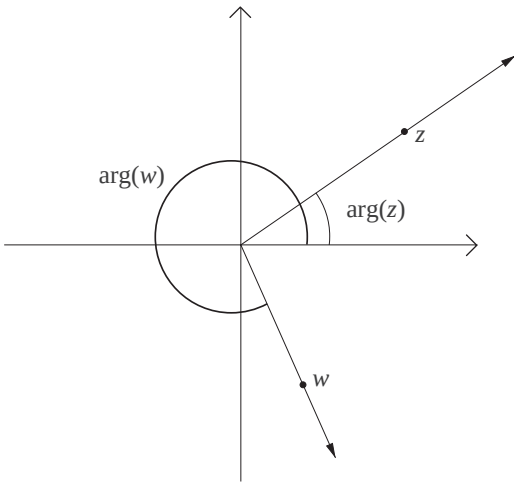


Figura 5. *El argumento es el ángulo.*

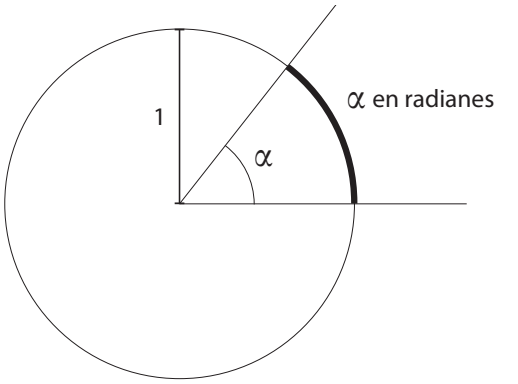


Figura 6. *Un ángulo medido en radianes.*

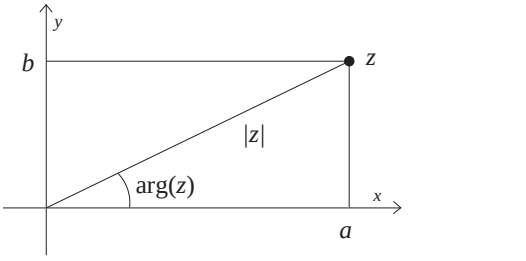


Figura 7. *Forma polar y binómica.*

Ejemplo. Si $z = 1 + i$, entonces $\arg(z) = \pi/4$ y $|z| = \sqrt{1^2 + 1^2} = \sqrt{2}$, por lo que la forma polar de z es $(\sqrt{2}\,;\,\pi/4)$.

Ejemplo. Si la forma polar de un complejo es $(3\,;\,\pi/3)$, entonces para conocer su forma binómica calculamos $a = 3\cos(\pi/3) = 3/2$, y $b = 3\,\mathrm{sen}(\pi/3) = 3\frac{\sqrt{3}}{2}i$, por lo que el complejo es $\frac{3}{2} + 3\frac{\sqrt{3}}{2}i$.

Observación. Cuando hablamos de ángulos, entendemos que el ángulo 2π es igual al ángulo 0. Más generalmente, no cambia un ángulo si le sumamos 2π, ni si lo restamos. Por la misma razón, tampoco cambia si sumamos o restamos 4π, ó 6π, 8π, etc. En otras palabras, un complejo, con módulo r y argumento α, es decir con forma polar $(r\,;\,\alpha)$, se puede escribir también con forma polar $(r\,;\,\alpha + 2k\pi)$, con $k \in \mathbb{Z}$.

Ejercicio 6.5. Pasar a forma polar $1 + i$; $1 - i$; $-1 + i$; $-1 - i$; $2 + 2i$; $-3 - 3i$; $4 - 4i$; 4 y -5.

□ 7. Leyes de de Moivre

Una de las ventajas de la forma polar es la simplicidad con la que permite calcular productos y cocientes. Recordemos que $\cos(\alpha + \beta) = \cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta$ *y* que $\mathrm{sen}(\alpha + \beta) = \cos\alpha\,\mathrm{sen}\,\beta + \mathrm{sen}\,\alpha\cos\beta$. Ahora, si:

$$z = (r\,;\,\alpha) \text{ y } w = (s\,;\,\beta)$$

entonces:

$$\begin{aligned} z \cdot w &= r(\cos\alpha + i\,\mathrm{sen}\,\alpha)\,.s\,(\cos\beta + i\,\mathrm{sen}\,\beta) \\ &= rs\,((\cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta) + i(\cos\alpha\,\mathrm{sen}\,\beta + \mathrm{sen}\,\alpha\cos\beta)) \\ &= rs\,(\cos(\alpha + \beta) + i\,\mathrm{sen}(\alpha + \beta)) \end{aligned}$$

Es decir, la forma polar de $z \cdot w$ es $(rs\,;\,\alpha + \beta)$. Geométricamente, multiplicar por un complejo z con forma polar $(r\,;\,\alpha)$, modifica módulos y argumentos de la siguiente manera: los módulos se multiplican por r (si $r > 1$ las cosas se agrandan, si $r = 1$ quedan igual y si $r < 1$ se achican), y los ángulos se giran α. Podemos ver el efecto en la figura 8. El efecto de multiplicar por i, cuya forma polar es $(1;\frac{\pi}{2})$, es rotar un ángulo de $\frac{\pi}{2}$ hacia la izquierda, sin agrandar ni achicar. El efecto de multiplicar por $(1/2;\frac{\pi}{3})$ es rotar $\frac{\pi}{3}$ hacia la izquierda, y multiplicar los tamaños por 1/2, es decir reducirlos a la mitad. En la figura original, la cintura es horizontal y apunta al eje de coordenadas (el 0). Cuando se lo multiplica por $(1/2;\frac{\pi}{3})$ sigue apuntando hacia el 0 pero con un ángulo de $\frac{\pi}{3}$ con respecto al eje horizontal. Por otra parte, el efecto de multiplicar por $(2\,;\,-\frac{\pi}{6})$ es rotar hacia la izquierda $-\frac{\pi}{6}$, es decir $\frac{\pi}{6}$ hacia la derecha, y multiplicar los tamaños por 2.

Ya vimos cómo multiplicar en forma polar; veamos ahora cómo dividir. Supongamos que $w \neq 0$ (es decir, que $s \neq 0$) y calculemos la forma polar de z/w. Para eso, debemos encontrar la forma polar de w^{-1}. Pero w^{-1} es el complejo que multiplicado por w da 1, y la forma polar de 1 es $(1\,;\,0)$. Entonces, si la forma polar de w^{-1} es $(t\,;\,\gamma)$, debe ser $(s\,;\,\beta)\cdot(t\,;\,\gamma) = (1\,;\,0)$, es decir, $(st\,;\,\beta + \gamma) = (1\,;\,0)$, por lo que: $t = s^{-1}$ y $\gamma = -\beta$. Como

se trata de ángulos, es lo mismo decir $\gamma = -\beta$ que $\gamma = 2\pi - \beta$. Entonces, la forma polar de z/w es la de $z \cdot w^{-1}$, y es $(r\,;\,\alpha) \cdot (1/s;\,-\beta) = (\,r/s;\,\alpha - \beta)$.

Ejemplo. Multiplicamos y dividimos algunos complejos en forma polar:

$$(2\,;\,\frac{\pi}{2})(3\,;\,\frac{\pi}{3}) = (6\,;\,\frac{5\pi}{6})$$

$$(2{,}23\,;\,\pi)(1{,}24\,;\,\frac{3\pi}{2}) = (2{,}7652\,;\,\frac{5\pi}{2})$$

$$= (2{,}7652\,;\,\frac{\pi}{2})$$

$$(2\,;\,\frac{\pi}{2})/(3\,;\,\frac{\pi}{3}) = (\frac{2}{3}\,;\,\frac{\pi}{6})$$

$$(2\,;\,\frac{\pi}{2})^{-1} = (\frac{1}{2}\,;\,-\frac{\pi}{2})$$

$$= (\frac{1}{2}\,;\,\frac{3\pi}{2})$$

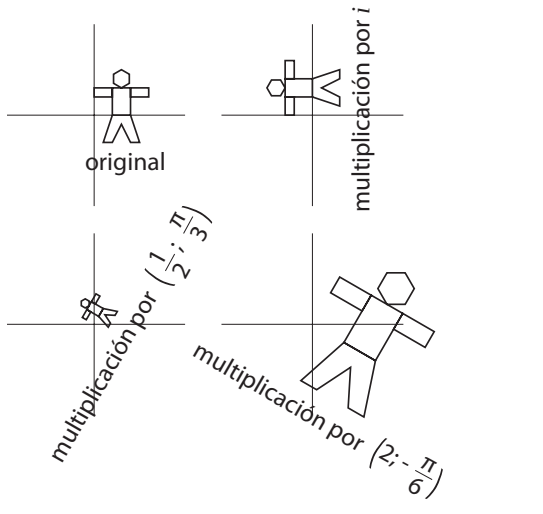


Figura 8. *Multiplicación por distintos complejos.*

□ 8. Raíces de la unidad

Si n es un número natural, el conjunto de los números complejos z tales que $z^n = 1$ tiene propiedades importantes. Vamos a usar la notación G_n para ese conjunto:

$$G_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

Los elementos de G_n se suelen llamar *raíces n-ésimas de la unidad*, o *raíces n-ésimas de* 1. Veamos qué forma polar tienen. Si $z = (r\,;\,\alpha)$ está en G_n, entonces $z^n = 1$. Como z^n tiene forma polar $(r^n;\,n\alpha)$, entonces:

$$(r^n;\,n\alpha) = (1\,;\,0)$$

Mirando los módulos, esto quiere decir $r^n = 1$. Como r es un número real ≥ 0, esta condición tiene como solución únicamente $r = 1$. Por otra parte, el ángulo $n\alpha$ debe ser igual al ángulo 0, es decir que pueden ser iguales como números, o diferir en 2π, 4π, etc. Esto es, puede ser $n\alpha = 0$, ó $n\alpha = 2\pi$, ó $n\alpha = 4\pi$, etc. En otras palabras, $n\alpha = 2k\pi$, donde k es un número entero. Dividiendo por n, obtenemos $\alpha = 2k\pi/n$ para un entero k. Luego, los elementos de G_n son los complejos con forma polar $(1\,;\,2k\pi/n)$, con $k \in \mathbb{Z}$. A primera vista, podría parecer que son infinitos, porque hay uno por cada k entero. Sin embargo, el complejo que corresponde a $k = n$ da como ángulo 2π, que es el mismo ángulo que 0, y por lo tanto tomando $k = 0$ y $k = n$ tenemos la misma solución. Más aún, ¿cuándo dos ángulos $2k\pi/n$ y $2j\pi/n$ son iguales?

La respuesta es que son iguales cuando existe un entero t tal que $2k\pi/n - 2j\pi/n = 2t\pi$.

Esto es, cuando $\frac{2(k-j)\pi}{n} = 2t\pi$, es decir cuando $k - j = tn$. La conclusión es que $(1\,;\frac{2k\pi}{n})$ y $(1\,;\frac{2j\pi}{n})$ son el mismo complejo cuando $k \equiv j$ (mód n). Por lo tanto, hay n soluciones distintas de la ecuación $z^n = 1$, que son los números complejos:

$$(1\,;\ \frac{2k\pi}{n}) = \cos(\frac{2k\pi}{n}) + i\,\mathrm{sen}(\frac{2k\pi}{n}), \qquad \text{con } k = 0, 1, \cdots, n-1$$

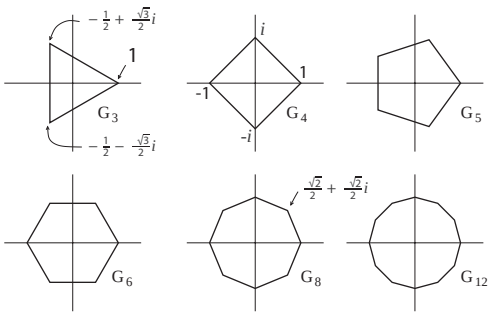


Figura 9. *El grupo G_n para distintos n.*

Todos estos números están a distancia 1 del 0, y entre uno y el siguiente hay siempre el mismo ángulo. Lo que resulta, entonces, es que son los vértices de un n-ágono regular centrado en 0, como puede verse en la figura 9. En la figura mostramos el n-ágono completo, aunque los elementos de G_n son sólo los vértices. Hay algunos valores de n para los que podemos calcular más explícitamente los elementos de G_n (es decir, sin senos ni cosenos sino sólo con raíces). Por ejemplo, como $\cos(\frac{2\pi}{3}) = -\frac{1}{2}$ y $\mathrm{sen}(\frac{2\pi}{3}) = \frac{\sqrt{3}}{2}$, entonces:

$$G_3 = \{1,\ -\frac{1}{2} + \frac{\sqrt{3}}{2}i,\ -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$$

De manera similar se obtiene que:

$$G_4 = \{1,\ i,\ -1,\ -i\},$$
$$G_6 = \{1,\ \frac{1}{2} + \frac{\sqrt{3}}{2}i,\ -\frac{1}{2} + \frac{\sqrt{3}}{2}i,\ -1,\ -\frac{1}{2} - \frac{\sqrt{3}}{2}i,\ \frac{1}{2} - \frac{\sqrt{3}}{2}i\},$$
$$G_8 = \{1,\ \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,\ i,\ -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,\ -1,\ -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i,\ -i,\ \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\}$$

Para cada n natural, el conjunto G_n tiene las siguientes propiedades:

- $1 \in G_n$, ya que $1^n = 1$.
- Si $z \in G_n$ entonces $z^{-1} \in G_n$, ya que $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$.
- Si $z \in G_n$ y $w \in G_n$ entonces $z \cdot w \in G_n$, ya que $(zw)^n = z^n w^n = 1 \cdot 1 = 1$.

De hecho, podemos calcular explícitamente el producto y los inversos de las raíces n-ésimas. Si $z = (1\,;\, 2k\pi/n)$ y $w = (1\,;\, 2j\pi/n)$, entonces:

$$z^{-1} = (1\,;\ -\frac{2k\pi}{n}) \qquad\qquad zw = (1\,;\ \frac{2(k+j)\pi}{n})$$
$$= (1\,;\ 2\pi - \frac{2k\pi}{n})$$
$$= (1\,;\ \frac{2(n-k)\pi}{n})$$

Una de las aplicaciones de las raíces n-ésimas es la de calcular explícitamente los vértices de algunos n-ágonos regulares (no sólo centrados en 0 y con un vértice en 1). Por ejemplo, ¿cómo podemos encontrar los vértices de un hexágono regular centrado en 0, tal que uno de sus vértices es $1 + 3i$? La solución viene de recordar que multiplicar por un complejo rota y

"estira" el plano complejo. Entonces, si a cada uno de los elementos de G_6 los multiplicamos por $1 + 3i$, rotaremos el hexágono que forma G_6 y lo estiraremos de manera que $1 + 3i$ será uno de sus vértices. Hagamos la prueba, llamando $z_0, \ldots, z_5$ a los elementos de G_6:

k	z_k	$z_k \cdot (1+3i)$
0	1	$1+3i$
1	$\frac{1}{2}+i\frac{\sqrt{3}}{2}$	$\frac{1-3\sqrt{3}}{2}+\frac{3+\sqrt{3}}{2}i$
2	$-\frac{1}{2}+i\frac{\sqrt{3}}{2}$	$\frac{-1-3\sqrt{3}}{2}+\frac{-3+\sqrt{3}}{2}i$
3	-1	$-1-3i$
4	$-\frac{1}{2}-i\frac{\sqrt{3}}{2}$	$\frac{-1+3\sqrt{3}}{2}+\frac{-3-\sqrt{3}}{2}i$
5	$\frac{1}{2}-i\frac{\sqrt{3}}{2}$	$\frac{1+3\sqrt{3}}{2}+\frac{3-\sqrt{3}}{2}i$

¿Cómo podemos encontrar el hexágono regular que tiene centro en $4 + 3i$ y que tiene un vértice en $6 + 2i$? Lo que debemos pensar ahora es que, así como multiplicar por un complejo rota y estira el plano, sumar un complejo lo traslada. Si al hexágono buscado le restamos el centro, obtendremos un hexágono regular centrado en 0 al que podemos calcularle los vértices. Y luego, a los vértices de ese hexágono centrado en 0 les sumamos nuevamente el centro, para obtener el hexágono buscado.

Cuando al vértice $6 + 2i$ le restamos el centro $4 + 3i$, nos queda $2 - i$. Entonces, primero buscamos los vértices del hexágono centrado en 0 y que tiene un vértice en $2 - i$. Eso se hace, como ya vimos, multiplicando los elementos de G_6 por $2 - i$. Y finalmente les volvemos a sumar $4 + 3i$. Obtenemos así los vértices:

k	z_k	$z_k \cdot (2-i)$	$z_k \cdot (2-i) + (4+3i)$
0	1	$2-i$	$6+2i$
1	$\frac{1}{2}+i\frac{\sqrt{3}}{2}$	$\frac{2+\sqrt{3}}{2}+i\frac{-1+2\sqrt{3}}{2}$	$\frac{10+\sqrt{3}}{2}+i\frac{5+2\sqrt{3}}{2}$
2	$-\frac{1}{2}+i\frac{\sqrt{3}}{2}$	$\frac{-2+\sqrt{3}}{2}+i\frac{1+2\sqrt{3}}{2}$	$\frac{6+\sqrt{3}}{2}+i\frac{7+2\sqrt{3}}{2}$
3	-1	$-2+i$	$2+4i$
4	$-\frac{1}{2}-i\frac{\sqrt{3}}{2}$	$\frac{-2-\sqrt{3}}{2}+i\frac{1-2\sqrt{3}}{2}$	$\frac{6-\sqrt{3}}{2}+i\frac{7-2\sqrt{3}}{2}$
5	$\frac{1}{2}-i\frac{\sqrt{3}}{2}$	$\frac{2-\sqrt{3}}{2}+i\frac{-1-2\sqrt{3}}{2}$	$\frac{10-\sqrt{3}}{2}+i\frac{5-2\sqrt{3}}{2}$

Los hexágonos resultantes se pueden observar en la figura 10.

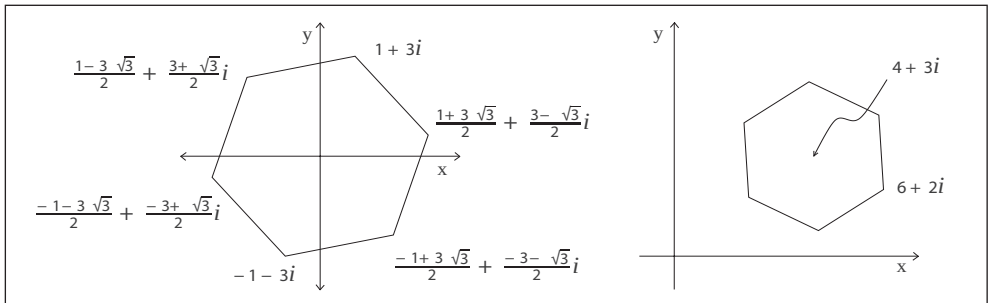


Figura 10. *Un hexágono centrado en 0 y uno centrado en 4 + 3i.*

Ejercicio 6.6. Encontrar los vértices de un triángulo equilátero con centro en $-2 + i$ y un vértice en $2i$. Más difícil: encontrar el tercer vértice de un triángulo equilátero que tiene dos de sus vértices en $1 + i$ y $-3 + 2i$.

□ 9. Raíces de un número complejo

Una vez que conocemos las raíces n-ésimas de la unidad, podemos conocer las raíces n-ésimas de otros números complejos si conocemos una de ellas. Supongamos que queremos conocer las raíces n-ésimas de x, es decir los números complejos w tales que $w^n = x$. Si w_1 y w_2 son dos de ellas, entonces $(\frac{w_2}{w_1})^n = \frac{w_2^n}{w_1^n} = \frac{x}{x} = 1$. Esto dice que w_2/w_1 es una raíz n-ésima de la unidad. Por lo tanto, si $z = w_2/w_1$, tenemos que $w_2 = z \cdot w_1$. Y no solo eso, si z' es una raíz n-ésima de la unidad cualquiera, entonces $z' \cdot w_1$ es una raíz n-ésima de x, porque $(z' \cdot w_1)^n = z'^n \cdot w_1^n = 1 \cdot x = x$.

Conclusión. Si x es un número complejo, n es un número natural y $w^n = x$, entonces todas las raíces n-ésimas de x son de la forma $z.w$, donde z es una raíz n-ésima de 1.

En forma polar es sencillo encontrar las soluciones. Si $x = (r\,;\,\alpha)$, $w = (s\,;\,\beta)$ y $w^n = x$, entonces $w^n = (s^n; n\beta)$. Por lo tanto, debe ser $s^n = r$ y $n\beta = \alpha$ (como ángulos). La primera igualdad es equivalente a $s = \sqrt[n]{r}$; como r es un número real positivo, tiene una única raíz real positiva $\sqrt[n]{r}$, que es s. Con respecto a la igualdad $n\beta = \alpha$, vale la misma salvedad que hicimos para las raíces n-ésimas de la unidad: la igualdad entre ángulos debe entenderse teniendo en cuenta que sumar o restar vueltas enteras (múltiplos de 2π) no afecta la igualdad. Entonces, debe ser $n\beta = \alpha + 2k\pi$, esto es, $\beta = \frac{\alpha + 2k\pi}{n}$. Y como con las raíces de la unidad, variando k entre 0 y $n - 1$ obtenemos todos los valores posibles para β.

Conclusión. Si $x = (r\,;\,\alpha)$ y n es un número natural, las raíces n-ésimas de x son los complejos:

$$(\sqrt[n]{r}\,;\,\frac{\alpha + 2k\pi}{n}), \quad \text{para } k = 0, \cdots, n-1$$

Como ejemplo, calculemos en forma polar las raíces sextas de $(64\,;\,\pi)$. Primero, el módulo de las raíces sextas será $\sqrt[6]{64} = 2$. Y luego, el argumento será $\frac{\pi + 2k\pi}{6}$. En este caso particular las podemos listar y escribir en forma binómica:

k	forma polar	forma binómica
$k = 0$	$(2\,;\,\frac{\pi}{6})$	$2 \cdot (\frac{\sqrt{3}}{2} + \frac{1}{2}i) = 2\sqrt{3} + i$
$k = 1$	$(2\,;\,\frac{\pi+2\pi}{6})$	$2 \cdot i = 2i$
$k = 2$	$(2\,;\,\frac{\pi+4\pi}{6})$	$2 \cdot (-\frac{\sqrt{3}}{2} + \frac{1}{2}i) = -2\sqrt{3} + i$
$k = 4$	$(2\,;\,\frac{\pi+6\pi}{6})$	$2 \cdot (-\frac{\sqrt{3}}{2} - \frac{1}{2}i) = -2\sqrt{3} - i$
$k = 5$	$(2\,;\,\frac{\pi+8\pi}{6})$	$2 \cdot (-i) = -2i$
$k = 6$	$(2\,;\,\frac{\pi+10\pi}{6})$	$2 \cdot (\frac{\sqrt{3}}{2} - \frac{1}{2}i) = 2\sqrt{3} - i$

Ejercicio 6.7. Calcular las raíces octavas de $(256\ ;\ 4\pi/3\ )$ en forma polar y en forma binómica. Calcular las raíces octavas de $-8 - 8\sqrt{3}i$ (sugerencia: pasar primero $-8 - 8\sqrt{3}i$ a su forma polar).

□ 10. Soluciones de ecuaciones de grados 2 y 3

Como vimos, los números complejos permiten encontrar raíces cuadradas de números negativos. Pero también permiten encontrar raíces de órdenes más altos, tanto de números reales como de números complejos. E incluso con números complejos se pueden resolver ecuaciones polinomiales. Veamos el ejemplo de una ecuación de grado 2. Dados tres números a, b y c, se quieren encontrar los x tales que:

$$ax^2 + bx + c = 0$$

En $\mathbb{R}$ es bien conocida la fórmula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Esta fórmula da las soluciones en $\mathbb{R}$ cuando $b^2 - 4ac \geq 0$, pero si $b^2 - 4ac < 0$ entonces la ecuación no tiene soluciones reales. Sin embargo, en los complejos podemos tomar raíces cuadradas de números negativos, y la misma fórmula sigue valiendo tomando cualquiera de las dos raíces cuadradas de $b^2 - 4ac$. Incluso podrían ser a, b y c complejos y la fórmula nos da las soluciones complejas.

Pongamos un ejemplo concreto: las soluciones de $2x^2 + 3x + 2 = 0$ son:

$$x = \frac{-3 \pm \sqrt{9 - 4 \cdot 4}}{4}$$

$$x = \frac{-3 \pm \sqrt{-7}}{4}$$

Es decir

$$x = -\frac{3}{4} + \frac{\sqrt{7}}{4}i \ \text{ y}$$

$$x = -\frac{3}{4} - \frac{\sqrt{7}}{4}i$$

Ejercicio 6.8. Verificar que reemplazando x por $-\frac{3}{4} + \frac{\sqrt{7}}{4}i$ o por $-\frac{3}{4} - \frac{\sqrt{7}}{4}i$ se tiene $2x^2 + 3x + 2 = 0$.

Otro ejemplo: buscamos las soluciones de $x^2 - 3x + (3 + i) = 0$. Antes de hacer las cuentas, observemos que $(1 - 2i)^2 = 1 - 4 - 4i = -3 - 4i$. Entonces, las soluciones son:

$$x = \frac{3 \pm \sqrt{9 - 4 \cdot (3 + i)}}{2}$$

$$x = \frac{3 \pm \sqrt{-3 - 4i}}{2}$$

$$x = \frac{3 \pm (1 - 2i)}{2}$$

Es decir,

$$x = \frac{4-2i}{2} \quad \text{y} \quad x = \frac{2+2i}{2}$$

ó

$$x = 2 - i \quad \text{y} \quad x = 1 + i$$

Observación. Las raíces de -3 - 4*i*, que son 1 - 2*i* y -1 + 2*i*, se pueden obtener de manera analítica, aunque no lo hagamos aquí.

Las ecuaciones de grado 3 también se pueden resolver, aunque la fórmula que da las soluciones es algo más complicada. Damos aquí solo una idea de cómo se encuentran. Si la ecuación es $x^3 + px + q = 0$, definimos *u* y *v* por:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

En realidad, hay tres valores distintos para *u* y tres valores distintos para *v*. Se deben tomar *u* y *v* de manera tal que $uv = -\frac{p}{3}$. Por otra parte, tomamos $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Entonces las tres soluciones de la ecuación son:

$$x = u + v,$$
$$x = wu + w^2v$$
$$x = w^2u + wv$$

Ejercicio 6.9. Encontrar las soluciones de $x^3 + 9x - 6 = 0$.

Ejercicio 6.10. Encontrar las soluciones de $x^3 = 15x + 4$. Observar que $x = 4$ es una solución. ¿Cuál de las soluciones encontradas es?

No toda ecuación de grado 3 tiene la forma $x^3 + px + q = 0$. Una ecuación general de grado 3 es de la forma $ax^3 + bx^2 + cx + d = 0$. Sin embargo, dividiendo la ecuación por *a* y reemplazando *x* por $y - \frac{b}{3a}$, obtenemos una ecuación en la incógnita *y* de la forma $y^3 + py + q = 0$.

También hay una fórmula como éstas, con raíces, para las soluciones de ecuaciones de grado 4. Tanto la fórmula general para ecuaciones de grado 3 como la de ecuaciones de grado 4 fueron encontradas en el siglo XVI por los italianos Scipione del Ferro[16], Tartaglia[17], Cardano[18] y Ferrari[19]. Viendo que estas ecuaciones se podían resolver, los matemáticos buscaron infructuosamente por siglos una fórmula similar a éstas para

[16] (1465-1526), de Bologna, fue posiblemente el primero en resolver algunas de las ecuaciones de grado 3.

[17] (1500-1557), de Brescia, resolvió de manera independiente a del Ferro las ecuaciones de grado 3 con raíces reales. Su verdadero nombre era Nicolo Fontana.

[18] (1501-1576), de Milán. Dio una forma general para las ecuaciones de grado 3. Al hacerlo, introdujo los números negativos de manera sistemática y los complejos.

[19] (1522-1565), de Bologna, alumno de Cardano. Encontró la solución de las ecuaciones de grado 4.

las ecuaciones de grado 5. A comienzos del siglo XIX, Niels Henrik Abel[20] y Evariste Galois[21] demostraron que una fórmula así es imposible para ecuaciones de grado ≥ 5.

□ 11. Fractales

En esta sección, para cada complejo c vamos a considerar la función $f(z) = z^2 + c$. Comenzamos con $z = 0$ y le aplicamos la función repetidas veces. Por ejemplo, si $c = 4$, nos queda $z = 0$, $f(0) = 0^2 + 4 = 4$, $f(4) = 4^2 + 4 = 20$, $f(20) = 20^2 + 4 = 404$, etc.

Para que sea más cómodo de leer, escribimos $m_{n,c}$ el n-ésimo término que resulta comenzando con c. Es decir, lo que calculamos arriba es $m_{1,4} = 4$, $m_{2,4} = 20$, $m_{3,4} = 404$. Definido recursivamente es:

$$m_{1,c} = c,$$
$$m_{n+1,c} = m_{n,c}^2 + c$$

Si $c = -1$ obtenemos $m_{1,-1} = -1$, $m_{2,-1} = (-1)^2 - 1 = 0$, $m_{3,-1} = 0^2 - 1 = -1$, $m_{4,-1} = (-1)^2 - 1 = 0$, etc. En las tablas siguientes calculamos los primeros resultados para distintos valores de c (algunos números los aproximamos para que quepan en la tabla).

$m_{1,c} = c$	4	2	1	−1	$-1 + 0{,}5\,i$	0,5
$m_{2,c}$	20	6	2	0	$-0{,}25 - 0{,}5\,i$	0,75
$m_{3,c}$	404	38	5	−1	$-1{,}1875 + 0{,}75\,i$	1,0625
$m_{4,c}$	163220	1446	26	0	$-0{,}152344 - 1{,}28125\,i$	1,62891
$m_{5,c}$	26640768404	2090918	677	−1	$-2{,}61839 + 0{,}890381\,i$	3,15334

$m_{1,c} = c$	−0,5	$-0{,}5 + i$	i	$-0{,}2 + 0{,}1\,i$
$m_{2,c}$	−0,25	$-1{,}25$	$-1 + i$	$-0{,}17 + 0{,}06\,i$
$m_{3,c}$	−0,4375	$1{,}0625 + i$	$-i$	$-0{,}1747 + 0{,}0796\,i$
$m_{4,c}$	−0,308594	$-0{,}371094 + 3{,}125\,i$	$-1 + i$	$-0{,}175816 + 0{,}0721878\,i$
$m_{5,c}$	−0,40477	$-10{,}1279 - 1{,}31934\,i$	$-i$	$-0{,}1743 + 0{,}0746165\,i$
$m_{6,c}$	−0,336161	$100{,}334 + 27{,}7242\,i$	$-1 + i$	$-0{,}175187 + 0{,}0739887\,i$

Puede observarse que para algunos valores de c, como para $c = 4$ o $c = 2$, la sucesión crece muy rápidamente (en el lenguaje de sucesiones, *diverge*). Para otros valores, como $c = -1$ o $c = i$, la sucesión oscila entre distintos números. Para otros valores, como $c = -0{,}5$, la sucesión se acerca cada vez más a un número (*converge*, en el lenguaje de sucesiones).

En algunos casos es fácil decir a qué se acerca la sucesión. En el caso de $c = -0{,}5$, por ejemplo, se acerca cada vez más a un número w. Ese número w debe ser tal que si le aplicamos la función nos vuelva a dar w. Es decir, $f(w) = w$. Como para $c = -0{,}5$ la función toma la forma $f(z) = z^2 - 0{,}5$, debe ser $w^2 - 0{,}5 = w$, o en otros términos $w^2 - w - 0{,}5 = 0$. Las soluciones de esta ecuación son:

$$w = \frac{1 \pm \sqrt{1+2}}{2}, \quad \text{es decir } w = \frac{1+\sqrt{3}}{2} \quad \text{o} \quad w = \frac{1-\sqrt{3}}{2}$$

[20] (1802-1829), noruego. Demostró la imposibilidad de resolver las ecuaciones de grado 5 con radicales. Los grupos conmutativos se llaman abelianos en su honor.

[21] (1811-1832), francés. Mostró lo mismo que Abel de manera independiente. Al hacerlo, dio comienzo a la teoría de grupos.

Mirando los primeros valores de la tabla de la columna $c = -0{,}5$, observamos que la sucesión se acerca a $\frac{1-\sqrt{3}}{2} \sim -0{,}366025403784439$. Es importante hacer una salvedad aquí: estamos usando conceptos del análisis matemático, como sucesión, límite, etcétera. En rigor, es necesario *demostrar* que la sucesión correspondiente a -0,5 converge a $\frac{1-\sqrt{3}}{2}$. Como el objeto de esta sección es otro, pasamos por alto estas demostraciones.

Sin embargo, el análisis que hicimos para -0,5 no se puede hacer para todos los valores de c. Como dijimos, el comportamiento de estas sucesiones depende mucho del valor inicial c, y a veces pequeños cambios en c significan grandes cambios en la sucesión. Pero podemos hacer algunas consideraciones, que dejamos como ejercicio.

Ejercicio 6.11. Probar por inducción que si $|c| > 2$ entonces $|m_{n,c}| \geq |c|$ para todo $n \in \mathbb{N}$. Sugerencia: usar que $|m_{n+1,c}| = |m^2_{n,c}+c| \geq |m^2_{n,c}|-|c| = |m_{n,c}|^2-|c|$. Aquí se usa la desigualdad triangular de la sección 3.

Ejercicio 6.12. Probar por inducción que, si $|c| \leq 2$ y para algún $n \in \mathbb{N}$ vale que $|m_{n,c}| > 2$, entonces $|m_{k,c}| > 2$ para todo $k \geq n$.

La conclusión es que si para algún n es $|m_{n,c}| > 2$ entonces para todo $k \geq n$ será $|m_{k,c}| > 2$. Es decir, que si queremos estudiar el comportamiento de $m_{n,c}$ para valores grandes de n, debemos mirar si $|m_{n,c}|$ es mayor a 2 para algún n. El conjunto de los números complejos c tales que $|m_{n,c}| \leq 2$ para todo $n \in \mathbb{N}$ recibe el nombre de *conjunto de Mandelbrot*, en honor al matemático Benoît Mandelbrot, que en 1980 fue uno de los primeros en estudiar conjuntos de este tipo.

Usualmente, se pueden tomar varios valores de c en el plano complejo y calcular $m_{n,c}$ para valores de $n \leq$ que alguna cota N fija de antemano. Para cada c, se pinta el punto correspondiente de negro si $|m_{n,c}| \leq 2$ para todo $n \leq N$, y se pinta de otro color si para algún $n \leq N$ se tiene $|m_{n,c}| > 2$. Se puede incluso pintar de distintos colores en función de cuál es el menor n tal que $|m_{n,c}| > 2$. De esta manera, se obtiene un dibujo aproximado del conjunto de Mandelbrot. Es aproximado porque pintamos de negro un punto si $|m_{n,c}| \leq 2$ para $n \leq N$ pero no calculamos qué pasa si $n > N$. Es posible que estemos pintando de negro, como si perteneciera al conjunto, a un punto que en realidad no pertenece. Si hacemos más grande el número N obtendremos una aproximación mejor al conjunto de Mandelbrot. Vemos el resultado de cambiar N en la figura 11. Las figuras de esta sección fueron hechas con Gnofract 4D, accesible en http://gnofract4d.sourceforge.net.

El conjunto de Mandelbrot es el más popular de los *fractales*. Los fractales son conjuntos "autosimilares". Esto es, tienen sectores que, cuando se los agranda, se asemejan al conjunto original. A su vez, estos sectores tienen nuevos sectores que se asemejan al original, y así siguiendo.

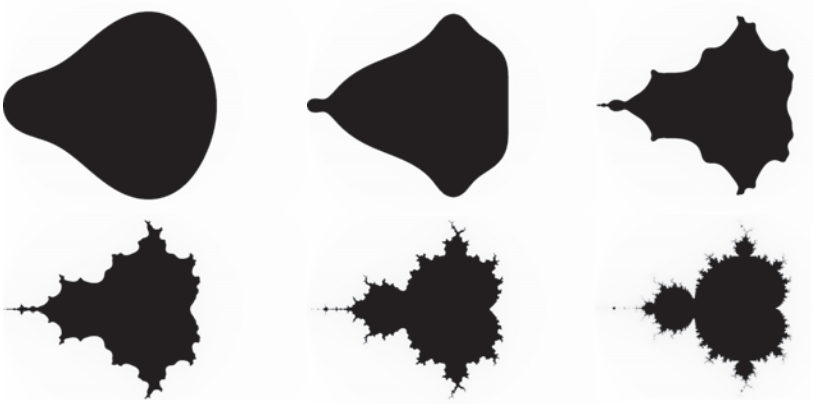


Figura 11. *Aproximaciones del conjunto de Mandelbrot con distintos valores de N: 3, 4, 6, 8, 12 y 24.*

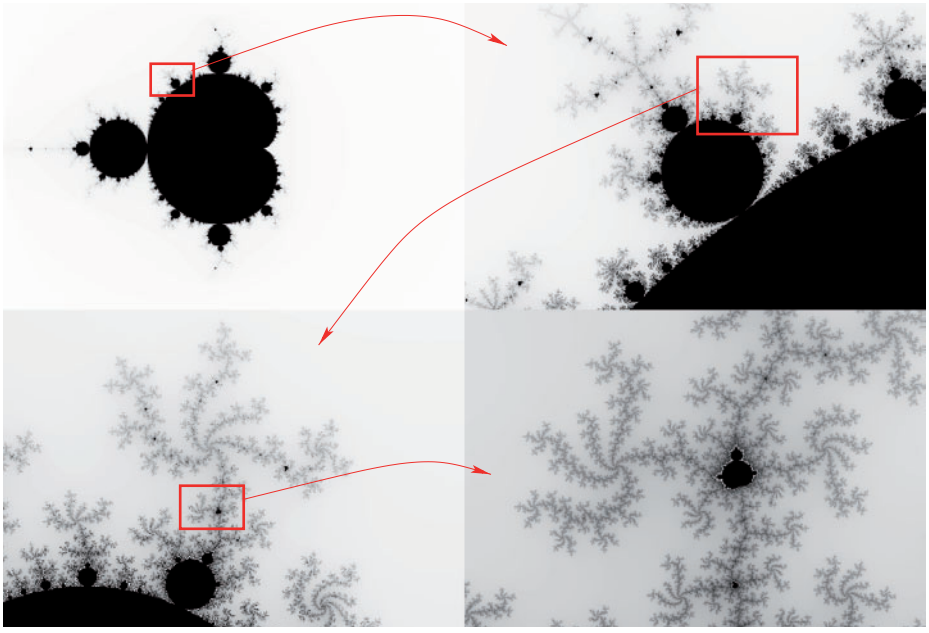


Figura 12. *El conjunto de Mandelbrot y la autosimilaridad. Con distintos tonos de gris se pintan los puntos según para qué n es* $|m_{n,c}| > 2$.

Ejercicio 6.13. (Para el lector que sabe programar). 1. Hacer un programa que dibuje aproximaciones del conjunto de Mandelbrot, variando el valor de N.

2. Modificar el programa cambiando la función f por $f(z) = z^3+c$ y observar el resultado. ¿Resulta también un conjunto autosimilar?

7. Ejercicios resueltos

□ CAPÍTULO 0. Conjuntos y relaciones

Ejercicio 1.
La lista (1) es el conjunto de alumnos que pueden integrar ambos equipos, o sea los alumnos que tienen entre 14 y 16 años y también tienen entre 15 y 17 años, es decir que pertenecen a $\mathcal{A} \cap \mathcal{B}$.

La lista (2) es el conjunto de aquellos alumnos que puedan integrar alguno de los equipos. Esto es, son los alumnos que tienen entre 14 y 16 años o entre 15 y 17 años. Éste es el conjunto $\mathcal{A} \cup \mathcal{B}$.

La lista (3) es el conjunto de alumnos que puede integrar sólo el equipo de fútbol. Esto es, son los alumnos que están en la lista del equipo de fútbol (con lo cual tienen entre 14 y 16 años), pero no están en la lista del equipo de básquet (con lo cual no tienen entre 15 y 17 años). Éste es el conjunto $\mathcal{A} \setminus \mathcal{B}$.

Análogamente, la lista (4) es el conjunto de alumnos que pueden integrar sólo el equipo de básquet. Este es el conjunto $\mathcal{B} \setminus \mathcal{A}$.

Ejercicio 2. Queremos obtener el conjunto de combinaciones de ropa para Lorena como un producto cartesiano de conjuntos. Para abreviar, escribiremos por *JA* el jean azul, por *JG* el jean gris, por *PB* el pantalón blanco, por *MB* la musculosa blanca, por *MN* la musculosa negra, por *RR* la remera rosa, por *RC* la remera celeste, por *S* el par de sandalias y por *Z* el par de zapatos. Luego, el conjunto de combinaciones de ropa es:

$$\{JA,\ JG,\ PB\} \times \{MB,MN,RR,RC\} \times \{S,Z\}$$

Expresado por extensión, es el siguiente conjunto de 24 elementos:

$$\begin{array}{l}\{(JA,MB,S),\ (JA,MB,Z),\ (JA,MN,S),\ (JA,MN,Z)\\ (JA,RR,S),\ (JA,RR,Z),\ (JA,RC,S),\ (JA,RC,Z)\\ (JG,MB,S),\ (JG,MB,Z),\ (JG,MN,S),\ (JG,MN,Z)\\ (JG,RR,S),\ (JG,RR,Z),\ (JG,RC,S),\ (JG,RC,Z)\\ (PB,MB,S),\ (PB,MB,Z),\ (PB,MN,S),\ (PB,MN,Z)\\ (PB,RR,S),\ (PB,RR,Z),\ (PB,RC,S),\ (PB,RC,Z)\}\end{array}$$

Ejercicio 3. El conjunto $\mathcal{A}$ es el conjunto de cantidades de goles, por lo tanto es el conjunto $\mathbb{N} \cup \{0\}$. La operación utilizada para calcular el número de goles luego de dos fechas es la suma $+ : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$. Se debe sumar el número de goles del primer partido (que es un elemento del conjunto $\mathcal{A}$) con el número de goles del segundo partido (que es otro elemento del conjunto $\mathcal{A}$).

Ejercicio 4. Comencemos viendo si la operación $\circ$ es conmutativa. Para esto debemos verificar si es cierto que $a \circ b = b \circ a$ para todo par de elementos a, b del conjunto $\{0, 1, 2, 3, 4\}$. Si miramos las distintas posibilidades, tenemos que:

$0 \circ 1 = 0 = 1 \circ 0$	$1 \circ 3 = 3 = 3 \circ 1$
$0 \circ 2 = 0 = 2 \circ 0$	$1 \circ 4 = 4 = 4 \circ 1$
$0 \circ 3 = 0 = 3 \circ 0$	$2 \circ 3 = 1 = 4 \circ 2$
$0 \circ 4 = 0 = 4 \circ 0$	$2 \circ 4 = 3 = 4 \circ 2$
$1 \circ 2 = 2 = 2 \circ 1$	$3 \circ 4 = 2 = 4 \circ 3$

Esto muestra que la operación es conmutativa. La operación no es asociativa, ya que $(2 \circ 2) \circ 3 = 2 \circ 3 = 1$, mientras que $2 \circ (2 \circ 3) = 2 \circ 1 = 2$. Por último, es claro que la operación tiene elemento neutro, ya que $a \circ 1 = 1 \circ a = a$ para todo $a \in \{0, 1, 2, 3, 4\}$ como puede verse en la tabla que define $\circ$.

La operación - claramente no es conmutativa ya que $0 - 1 = 4$, mientras que $1 - 0 = 1$. Tampoco es asociativa, ya que $(0 - 1) - 2 = 4 - 2 = 2$, mientras que $0 - (1 - 2) = 0 - 4 = 1$. Por último, la operación - no tiene neutro, pues si e es un neutro para la operación, valdría que $e - 0 = 0 - e = 0$. Mirando la tabla, vemos que el único número e tal que $0 - e = 0$ es $e = 0$. Pero $0 - 1 = 4 \neq 1$, luego no puede existir un elemento neutro.

Ejercicio 5. Debemos hallar una fórmula cerrada para la sucesión cuyos términos son 1, 2, 1, 2, 1, 2, ... Vimos que la sucesión $a_n = (-1)^n$ toma valores -1, 1, -1, 1, -1, 1, ... Si a cada miembro de esta sucesión le sumamos 3, obtenemos la sucesión 2, 4, 2, 4, 2, 4, ... Esta nueva sucesión no es exactamente la sucesión que estamos buscando, pero es el doble de ella. Luego la sucesión:

$$b_n = \frac{1}{2} \cdot (3 + (-1)^n)$$

cumple lo pedido.

□ CAPÍTULO 1. Números naturales

Ejercicio 1.1.

$$\begin{aligned}(a+b)^3 &= (a+b)^2 \cdot (a+b) \\ &= (a^2 + 2ab + b^2) \cdot (a+b) \\ &= a^3 + a^2b + 2a^2b + 2ab^2 + b^2a + b^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3\end{aligned}$$

Ejercicio 1.2. Tenemos que probar por inducción que $1 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ para todo natural n. Entonces, debemos probar $P(1)$ primero. Cuando $n = 1$, el miembro izquierdo de la igualdad, $1 + 2^2 + \ldots + n^2$ es simplemente 1. El miembro derecho, por otra parte, es $\frac{n(n+1)(2n+1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1$, por lo que la igualdad vale. Ahora, debemos suponer que es cierta $P(n)$ y probar $P(n + 1)$. Pero $P(n + 1)$ afirma que:

$$1 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$$

es decir, $1 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$.

La hipótesis inductiva, $P(n)$, nos permite escribir:

$$\begin{aligned} 1 + 2^2 + \cdots + n^2 + (n+1)^2 &= (1 + 2^2 + \cdots + n^2) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n^2+n)(2n+1)}{6} + n^2 + 2n + 1 \\ &= \frac{(2n^3 + n^2 + 2n^2 + n) + 6(n^2 + 2n + 1)}{6} \\ &= \frac{(2n^3 + 3n^2 + n) + (6n^2 + 12n + 6)}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

Por otra parte:

$$\begin{aligned} \frac{(n+1)(n+2)(2n+3)}{6} &= \frac{(n^2+3n+2)(2n+3)}{6} \\ &= \frac{2n^3 + 3n^2 + 6n^2 + 9n + 4n + 6}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

lo que finalmente prueba $P(n + 1)$.

Ejercicio 1.3. Probamos primero $P(10)$; es decir, que vale $2^{10} \geq 10^3$. Como $2^{10} = 1.024$ y $10^3 = 1.000$, $P(10)$ es verdadera. Ahora, si vale $P(n)$, debemos probar que vale $P(n + 1)$, esto es, que $2^{n+1} \geq (n + 1)^3$. Es decir, debemos probar que $2 \cdot 2^n \geq n^3+3n^2+3n+1$. Como vale $P(n)$, podemos escribir $2 \cdot 2^n = 2^n+2^n \geq n^3+2^n$, por lo que para probar $P(n + 1)$ es suficiente que probemos que $2^n \geq 3n^2 + 3n + 1$ para todo $n \geq 10$. Ésta es una nueva afirmación, que probamos por inducción en la sección 3 del capítulo 1.

Ejercicio 1.4. Si $n = 3$, tenemos que probar que $3^3 \geq 2^4 + 3$, es decir, que $27 \geq 19$, cosa que es cierta. Y si vale la afirmación $P(n)$, debemos probar $P(n+1)$, es decir que $3^{n+1} \geq 2^{n+2} + n + 1$. Pero:

$$\begin{aligned} 3^{n+1} &= 3 \cdot 3^n \\ &= 3^n + 3^n + 3^n \geq 2^{n+1} + n + 2^{n+1} + n + 3^n \\ &\geq 2 \cdot 2^{n+1} + n + n + 3^n \geq 2^{n+2} + n + n + 3^i \end{aligned}$$

Como $n + 3^n \geq 1$, entonces

$$3^{n+1} \geq 2 \cdot 2^{n+2} + n + 1$$

Ejercicio 1.5. Utilizaremos el lenguaje Python para mostrar las definiciones, que es el que hemos estado usando en los ejemplos. El siguiente algoritmo calcula, dado n, el número de Lucas n-ésimo L_n.

```
def lucas(n):
   if n==1:
        return 2
   elif n==2:
        return 1
   else:
        return lucas(n-1) + lucas(n-2)
```

El siguiente algoritmo calcula dado n, la variante del número de Lucas n-ésimo L'_n.

```
def variantelucas(n):
   if n==1:
        return 1
   elif n==2:
        return 5
   else:
        return variantelucas(n-1) + variantelucas(n-2)
```

Ejercicio 1.6. Calculamos los primeros términos de la sucesión:

$$a_3 = 4\sqrt{4} + 1 = 9,\ a_4 = 4\sqrt{9} + 4 = 16,\ a_5 = 4\sqrt{16} + 9 = 25$$

Podemos conjeturar, entonces, que $a_n = n^2$ (al menos esto es cierto para los primeros cinco términos de la sucesión). Para demostrar que esta conjetura es cierta, debemos probar que para todo n natural es cierta la afirmación $P(n) : a_n = n^2$. Ya sabemos que $P(1)$ y $P(2)$ son ciertas. Y si son ciertas las afirmaciones $P(k)$ para todo $k < n$, debemos probar que vale $P(n)$. Pero $a_n = 4\sqrt{a_{n-1}} + a_{n-2} = 4\sqrt{(n-1)^2} + (n-2)^2 = 4(n-1) + (n^2 - 4n + 4) = n^2$, que es precisamente la afirmación $P(n)$.

Ejercicio 1.7. La afirmación a probar es $P(n) : a_n \leq 3^n$. Para $n = 1$ la afirmación dice $2 \leq 3$, que vale. Para $n = 2$ la afirmación dice $3 \leq 3^2 = 9$, que también vale. Entonces, si son ciertas las afirmaciones $P(k)$ con $k < n$, probemos $P(n)$. Tenemos:

$$a_n = 2a_{n-1} + a_{n-2} \leq 2 \cdot 3^{n-1} + 3^{n-2} < 2 \cdot 3^{n-1} + 3^{n-1} = 3 \cdot 3^{n-1} = 3^n$$

Ejercicio 1.8. Vamos a empezar con un caso más sencillo. Si hay 4 piedritas, Martín puede sacar 1, 2 ó 3, y van a quedar, respectivamente, 3, 2 ó 1. En cualquier caso, Pablo quita las que quedan y gana. Esto muestra que si comienzan con 4 piedritas y comienza a jugar Martín, entonces Pablo tiene una estrategia ganadora. En realidad, lo que prueba esto es más general: no depende ni de Pablo, ni de Martín. Si hay 4 piedritas, aquél al que no le toca jugar tiene una estrategia ganadora. Por lo tanto, si cualquier jugador logra dejar 4 piedritas, va a ganar. Y esto es lo que sucede con 8 piedritas: Martín puede sacar 1, 2 ó 3 piedritas y van a quedar respectivamente 7, 6 ó 5. Entonces, Pablo puede sacar las que sobran y dejar 4 piedritas. Y ganará en la jugada siguiente. La respuesta, entonces, es afirmativa: si le toca jugar a Martín y hay 8 piedritas, Pablo tiene una estrategia ganadora: dejar 4 piedritas.

Entonces, hemos visto que si un jugador logra dejar 4 piedritas, tiene una estrategia ganadora. Y lo mismo pasa si logra dejar 8 piedritas. O 12, porque en este caso logrará dejar 8 en la jugada siguiente. Esto da un indicio de que si un jugador deja un múltiplo de

4 piedritas, tiene una estrategia ganadora. Por el contrario, si un jugador deja una cantidad que no es múltiplo de 4, el otro jugador logrará dejar un múltiplo de 4 y podrá ganar.

En otras palabras, nuestra afirmación $P(n)$ es que si Martín debe empezar con n piedritas entonces Pablo tiene una estrategia ganadora en el caso en que n sea múltiplo de 4, y Martín tiene una estrategia ganadora en otro caso. Es claro que esta afirmación es cierta si $n = 1$, $n = 2$ ó $n = 3$, porque Martín simplemente saca todas las piedritas y gana. Y si $n = 4$, ya hemos visto que es Pablo quien tiene una estrategia ganadora, es decir que vale $P(4)$. Supongamos ahora que vale $P(k)$ para todo $k < n$. Si n no es múltiplo de 4, al dividirlo por 4 puede tener resto 1, 2, ó 3. Es decir, n puede ser de la forma $4m + 1$, $4m + 2$ ó $4m + 3$. En cualquiera de estos casos, Martín quita respectivamente 1, 2 ó 3 piedritas y deja $4m$, es decir un múltiplo de 4. La hipótesis inductiva $P(4m)$ dice que es Martín quien tiene una estrategia ganadora. Por otra parte, si n es múltiplo de 4, entonces $n = 4m$. Martín puede quitar 1, 2 ó 3 piedritas, y Pablo quitará 3, 2 ó 1 respectivamente, dejando $4m - 4 = 4(m - 1)$, que es un múltiplo de 4 menor que n. Entonces, Pablo tendrá una estrategia ganadora.

Ejercicio 1.9. La afirmación vale cuando $n = 1$, pues en este caso $2^n - 1 = 2 - 1 = 1 = H_1$. Y si vale que $H_n = 2^n - 1$, entonces $H_{n+1} = 2 \cdot (2^n - 1) + 1 = 2 \cdot 2^n - 2 + 1 = 2^{n+1} - 1$, que es precisamente la afirmación para $n + 1$.

□ CAPÍTULO 2. Números enteros

Ejercicio 2.1. Los números impares son aquellos que no son divisibles por 2. Por lo tanto, se los puede describir como los $n \in \mathbb{Z}$ tales que $2 \nmid n$. Otra posibilidad es decir que son aquellos números de la forma $2k + 1$, donde k recorre todos los números enteros. Esto es así porque los números de la forma $2k$ son pares (y son todos los pares), por lo que al sumarles una unidad a los pares nos quedan los impares.

Ejercicio 2.2. El número $(\text{DEBE1CAFE})_{16}$ es igual a

$$\begin{aligned}(\text{E})_{16} \cdot 16^0 + (\text{F})_{16} \cdot 16^1 + (\text{A})_{16} \cdot 16^2 + (\text{C})_{16} \cdot 16^3 + (1)_{16} \cdot 16^4 + (\text{E})_{16} \cdot 16^5 + \\ + (\text{B})_{16} \cdot 16^6 + (\text{E})_{16} \cdot 16^7 + (\text{D})_{16} \cdot 16^8 = \\ = 14 \cdot 16^0 + 15 \cdot 16^1 + 10 \cdot 16^2 + 12 \cdot 16^3 + 1 \cdot 16^4 + 14 \cdot 16^5 + \\ + 11 \cdot 16^6 + 14 \cdot 16^7 + 13 \cdot 16^8 \\ = 14 + 240 + 2.560 + 49.152 + 65.536 + 14.680.064 + \\ + 184.549.376 + 3.758.096.384 + 55.834.574.848 \\ = 59.792.018.174\end{aligned}$$

Ejercicio 2.3. Sea $d = (2^n + 7^n : 2^n - 7^n)$. Queremos probar que $d = 1$. Como $d \mid 2^n + 7^n$ y $d \mid 2^n - 7^n$, entonces $d \mid (2^n + 7^n) + (2^n - 7^n)$, es decir $d \mid 2 \cdot 2^n = 2^{n+1}$. Pero los únicos enteros que dividen a 2^{n+1} son los de la forma 2^j con $0 \le j \le n+1$. Por otra parte, también tenemos que $d \mid (2^n + 7^n) - (2^n - 7^n)$, es decir $d \mid 2 \cdot 7^n$. Como las únicas potencias de 2 que dividen a $2 \cdot 7^n$ son 2^0 y 2^1, hemos probado que $d = 1$ o $d = 2$. Pero $2^n + 7^n$ es impar, pues 2^n es par y 7^n es impar, así que no es cierto que $2 \mid 2^n + 7^n$. Esto prueba que $d = 1$.

EJERCICIO 3.1. Calculamos (84 : 270) aplicando el algoritmo de Euclides:

$$\begin{aligned} 270 &= 3 \cdot 84 + 18 \\ 84 &= 4 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

Entonces (84 : 270) = 6. Como 6 | 66, la ecuación $84 \cdot x + 270 \cdot y = 66$ tiene soluciones enteras. Para hallar una solución, escribimos a 6 como combinación lineal entera de 84 y 270:

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - 1 \cdot (84 - 4 \cdot 18) \\ &= 5 \cdot 18 - 1 \cdot 84 \\ &= 5 \cdot (270 - 3 \cdot 84) - 1 \cdot 84 \\ &= (-16) \cdot 84 + 5 \cdot 270 \end{aligned}$$

Multiplicamos la igualdad por 11, obteniendo que:

$$66 = (-176) \cdot 84 + 55 \cdot 270$$

Por lo tanto, $(x_0, y_0) = (-176, 55)$ es una solución particular de la ecuación.

Así, todas las soluciones de la ecuación son los pares de enteros (x, y) de la forma $x = -176 + \frac{84}{6} \cdot k$, $y = 55 - \frac{270}{6} \cdot k$ con $k \in \mathbb{Z}$, es decir:

$$x = -176 + 14 \cdot k, \quad y = 55 - 45 \cdot k \qquad \text{con } k \in \mathbb{Z}$$

EJERCICIO 3.2.

- Criterio de divisibilidad por 3: *un número natural n es múltiplo de* 3 *si y sólo si la suma de sus dígitos es múltiplo de* 3. La demostración de este criterio es igual a la dada en el texto para el criterio de divisibilidad por 9, teniendo en cuenta que $10 \equiv 1$ (mód 3).

- Criterio de divisibilidad por 4: *un número natural n es múltiplo de* 4 *si y sólo si el número formado por las dos últimas cifras de n (decenas y unidades) es múltiplo de* 4.

  Si $n = (n_s \ldots n_2 n_1 n_0)_{10}$ es la representación decimal de n, entonces $n = n_s \cdot 10^s + \ldots + n_2 \cdot 10^2 + n_1 \cdot 10 + n_0$. Ahora, como $10^2 = 100 \equiv 0$ (mód 4), tenemos que $10^k \equiv 0$ (mód 4) para todo $k \geq 2$. Por lo tanto,

$$n \equiv n_1 \cdot 10 + n_0 \pmod 4$$

  Luego, n tiene el mismo resto en la división por 4 que el número cuya representación decimal es $(n_1 n_0)_{10}$; en particular, n es múltiplo de 4 si y sólo si $(n_1 n_0)_{10}$ lo es.

- Criterio de divisibilidad por 5: *un número natural es múltiplo de* 5 *si y sólo si termina en* 0 *ó en* 5. En efecto, si $n = (n_s \ldots n_1 n_0)_{10}$, entonces $n = n_s \cdot 10^s + \ldots + n_1 \cdot 10 + n_0 \equiv n_0$ (mód 5), ya que $10^k \equiv 0$ (mód 5) para todo $k \geq 1$. Entonces será divisible por 5 si y sólo si n_0 lo es; como $0 \leq n_0 \leq 9$, esto equivale a que $n_0 = 0$ ó $n_0 = 5$.

- Criterio de divisibilidad por 8: *un número natural n es múltiplo de* 8 *si y sólo si el número formado por las tres últimas cifras de n (centenas, decenas y unidades) es múltiplo de* 8. La demostración de este criterio es igual a la del criterio de divisibilidad por 4, teniendo en cuenta que $10^3 \equiv 0$ (mód 8).

- Criterio de divisibilidad por 11: *un número natural es múltiplo de* 11 s*i y sólo si la suma alternada de sus dígitos es múltiplo de* 11. Si $n = (n_s \ldots n_1 n_0)_{10}$, como $10 \equiv -1$ (mód 11), resulta que

$$\begin{aligned} n &= n_s \cdot 10^s + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10 + n_0 \\ &\equiv_{(11)} n_s \cdot (-1)^s + \cdots + n_2 \cdot (-1)^2 + n_1 \cdot (-1) + n_0 \\ &= n_s \cdot (-1)^s + \cdots + n_2 - n_1 + n_0 \end{aligned}$$

Luego, n es múltiplo de 11 si y sólo si lo es $n_0 - n_1 + n_2 - \ldots + (-1)^s \cdot n_s$ (los dígitos con subíndice par se suman y los de subíndice impar, se restan).

Ejercicio 3.3.

(a) Aplicando el algoritmo de Euclides a 17 y 45, obtenemos que $1 = (17 : 45) = 8 \cdot 17 - 3 \cdot 45$. En consecuencia, $(8 \cdot 20,\ 3 \cdot 20) = (160,\ 60)$ es una solución particular a la ecuación diofántica $17 \cdot x - 45 \cdot y = 20$. Por lo tanto, las soluciones de la ecuación $17 \cdot x \equiv 20$ (mód 45) son los enteros x tales que $x \equiv 160$ (mód 45), o equivalentemente, $x \equiv 25$ (mód 45).

(b) Como $(84 : 270) = 6$, la ecuación dada es equivalente a $(84/6) \cdot x \equiv 66/6$ (mód 270/6), es decir, $14 \cdot x \equiv 11$ (mód 45). Aplicando el algoritmo de Euclides a 14 y 45, obtenemos que $1 = (-16) \cdot 14 + 5 \cdot 45$. Multiplicando por 11, resulta que $11 = (-176) \cdot 14 + 55 \cdot 45$. Como $-176 \equiv 4$ (mód 45), las soluciones de la ecuación dada son los enteros x tales que $x \equiv 4$ (mód 45).

(c) La ecuación $28 \cdot x \equiv 30$ (mód 60) no tiene soluciones, ya que $(28 : 60) = 4$ y 4 no divide a 30.

Ejercicio 3.4. El problema equivale a encontrar las soluciones $a \in \mathbb{Z}$ de la ecuación $45 \cdot a \equiv 9$ (mód 27). Como $(45 : 27) = 9$, podemos dividir toda la ecuación por 9, obteniendo $5 \cdot a \equiv 1$ (mód 3), y como $5 \equiv -1$ (mód 3) nos queda la ecuación $-a \equiv 1$ (mód 3), que es equivalente a:

$$a \equiv 2 \pmod 3$$

Luego, los enteros a tales que el resto de la división de $45 \cdot a$ por 27 es 3 son los de la forma $a = 3 \cdot k + 2$ con $k \in \mathbb{Z}$.

Ejercicio 3.5. Las tablas de suma y producto pedidas son las siguientes:

- En $\mathbb{Z}_2$:

$+_2$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$\cdot_2$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

- En $\mathbb{Z}_4$:

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\cdot_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

- En $\mathbb{Z}_7$:

$+_7$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

$\cdot_7$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Ejercicio 3.6.

1. Para cada $a \in \mathbb{Z}_7$, $a \neq 0$, buscamos $x \in \mathbb{Z}_7$ tal que $a \cdot x = 1$ en $\mathbb{Z}_7$. Podemos hacer esto mirando la tabla del producto de $\mathbb{Z}_7$ construida en el ejercicio 3.5 (para hallar el inverso de a, miramos la fila encabezada por a y buscamos el elemento que corresponde a la columna donde está ubicado el 1 en dicha fila): $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ y $6^{-1} = 6$.
2. Sabemos que $a \in \mathbb{Z}_{14}$ tiene inverso multiplicativo si y sólo si $(a : 14) = 1$, es decir, si y sólo si a no es múltiplo ni de 2 ni de 7. Por lo tanto, los elementos de $\mathbb{Z}_{14}$ que tienen inverso multiplicativo son: 1, 3, 5, 9, 11, 13. Como en $\mathbb{Z}_{14}$ vale que $1 \cdot 1 = 1$, $13 \cdot 13 = 1$, $3 \cdot 5 = 1$ y $9 \cdot 11 = 1$, tenemos que los inversos multiplicativos de estos elementos son:

$$1^{-1} = 1,\ 3^{-1} = 5,\ 5^{-1} = 3,\ 9^{-1} = 11,\ 11^{-1} = 9,\ 13^{-1} = 13 \text{ en } \mathbb{Z}_{14}.$$

Ejercicio 3.7.

- $5 \cdot x = 4$ en $\mathbb{Z}_{14}$: esta ecuación tiene una única solución en $\mathbb{Z}_{14}$, ya que 5 tiene inverso multiplicativo en $\mathbb{Z}_{14}$ (ver ejercicio 3.6). La solución es $x = 5^{-1} \cdot 4 = 3 \cdot 4 = 12 \in \mathbb{Z}_{14}$.
- $6 \cdot x = 10$ en $\mathbb{Z}_{21}$: como $(6 : 21) = 3$, que no divide a 10, esta ecuación no tiene solución.
- $20 \cdot x = 12$ en $\mathbb{Z}_{24}$: como $(20 : 24) = 4$, que divide a 12, esta ecuación tiene 4 soluciones en $\mathbb{Z}_{24}$. Para hallarlas resolvemos la ecuación $5 \cdot x = 3$ en $\mathbb{Z}_6$ (que se obtiene dividiendo todo por $(20 : 24) = 4$); esta ecuación tiene como única solución a $x_0 = 3$ en $\mathbb{Z}_6$. Luego, las 4 soluciones de la ecuación original en $\mathbb{Z}_{24}$ son $x = 3 + 6 \cdot k$ con $k = 0, 1, 2, 3$, es decir:

  - $x = 3$
  - $x = 3 + 6 = 9$

- $x = 3 + 2 \cdot 6 = 15$
- $x = 3 + 3 \cdot 6 = 21$

Ejercicio 3.8. Llamemos c al costo en pesos de la cena. Según el enunciado, si cada una de las 10 personas presentes al comienzo pone la misma cantidad de dinero, pagan los c pesos y les quedan, además, 6 pesos. Como el total reunido sería un múltiplo de 10, esto nos dice que $c + 6 \equiv 0$ (mód 10) o, equivalentemente, que:

$$c \equiv 4 \pmod{10}$$

Análogamente, si al repartir entre 11 personas, pagan c pesos y quedan 10 es porque $c + 10 \equiv 0$ (mód 11), o sea, equivalentemente:

$$c \equiv 1 \pmod{11}$$

En definitiva, el costo c de la cena es una solución del sistema de ecuaciones:

$$\begin{cases} c \equiv 4 & (\text{mód } 10) \\ c \equiv 1 & (\text{mód } 11) \end{cases}$$

De la primera ecuación, deducimos que $c = 10 \cdot k + 4$ para algún entero k. Reemplazando en la segunda, nos queda que $k \in \mathbb{Z}$ debe cumplir $10 \cdot k + 4 \equiv 1$ (mód 11), o sea que debe ser solución de:

$$10 \cdot k \equiv -3 \pmod{11}$$

Como $10 \equiv -1$ (mód 11) esta ecuación es equivalente a que $-k \equiv -3$ (mód 11), es decir:

$$k \equiv 3 \pmod{11}$$

Luego k es de la forma $k = 11 \cdot q + 3$, con $q \in \mathbb{Z}$, y en consecuencia, el costo de la cena es un entero de la forma:

$$\begin{aligned} c &= 10 \cdot k + 4 \\ &= 10 \cdot (11 \cdot q + 3) + 4 \\ &= 110 \cdot q + 34 \end{aligned}$$

Dado que sabemos que el dinero reunido fue más de 100, el mínimo valor posible de la cena es $c = 144$.

Ejercicio 3.9.

1. Un entero x tiene resto 1 en la división por 3, si y sólo si $x \equiv 1$ (mód 3). Análogamente, su resto en la división por 5 es 2, si y sólo si $x \equiv 2$ (mód 5), y su resto en la división por 7 es 5 si y sólo si $x \equiv 5$ (mód 7). Luego, los enteros buscados son las soluciones del siguiente sistema de ecuaciones de congruencia:

$$\begin{cases} x \equiv 1 & (\text{mód } 3) \\ x \equiv 2 & (\text{mód } 5) \\ x \equiv 5 & (\text{mód } 7) \end{cases}$$

Como los módulos que aparecen son coprimos de a pares, por el teorema chino del resto, el sistema tiene una única solución x_0 módulo $3 \cdot 5 \cdot 7 = 105$ y podemos hallarla aplicando el algoritmo visto en la sección 6 del capítulo 3.

De la primera ecuación, deducimos que $x = 3 \cdot Q_1 + 1$ con $Q_1 \in \mathbb{Z}$. Ahora, buscamos Q_1 de manera que se cumpla la segunda ecuación, es decir:

$$3 \cdot Q_1 + 1 \equiv 2 \pmod 5$$

o, equivalentemente, $3 \cdot Q_1 \equiv 1$ (mód 5). Resolviendo esta ecuación (por ejemplo, multiplicando ambos miembros por 2), obtenemos que:

$$Q_1 \equiv 2 \pmod 5$$

Es decir, $Q_1 = 5 \cdot Q_2 + 2$ y, en consecuencia, $x = 3 \cdot (5 \cdot Q_2 + 2) + 1 = 15 \cdot Q_2 + 7$ con $Q_2 \in \mathbb{Z}$. Finalmente, determinamos los enteros Q_2 que hacen que se cumpla la tercera ecuación:

$$15 \cdot Q_2 + 7 \equiv 5 \pmod 7$$

o, equivalentemente, $Q_2 \equiv 5$ (mód 7). Por lo tanto, Q_2 se escribe como $Q_2 = 7 \cdot Q_3 + 5$ con $Q_3 \in \mathbb{Z}$; luego, $x = 15 \cdot (7 \cdot Q_3 + 5) + 7 = 105 \cdot Q_3 + 82$, con $Q_3 \in \mathbb{Z}$. En resumen, los enteros que cumplen las condiciones pedidas son los $x \in \mathbb{Z}$ tales que $x \equiv 82$ (mód 105).

2. Un entero x tiene resto 8 en la división por 12 y resto 6 en la división por 20, si y sólo si:

$$\begin{cases} x \equiv 8 & (\text{mód } 12) \\ x \equiv 6 & (\text{mód } 20) \end{cases}$$

Ahora:

$$x \equiv 8 \pmod{12} \iff \begin{cases} x \equiv 8 & (\text{mód } 4) \\ x \equiv 8 & (\text{mód } 3) \end{cases} \iff \begin{cases} x \equiv 0 & (\text{mód } 4) \\ x \equiv 2 & (\text{mód } 3) \end{cases}$$

$$x \equiv 6 \pmod{20} \iff \begin{cases} x \equiv 6 & (\text{mód } 4) \\ x \equiv 6 & (\text{mód } 5) \end{cases} \iff \begin{cases} x \equiv 2 & (\text{mód } 4) \\ x \equiv 1 & (\text{mód } 5) \end{cases}$$

La primera de las ecuaciones obtenidas dice que x debe ser múltiplo de 4, mientras que la tercera dice que debe tener resto 2 en la división por 4. Como no existen enteros que cumplan estas dos condiciones simultáneamente, el sistema no tiene soluciones, es decir, no existe ningún entero que tenga resto 8 en la división por 12 y resto 6 en la división por 20.

Ejercicio 3.10. Para hallar el resto en la división de $a \in \mathbb{Z}$ por $m \in \mathbb{N}$ buscamos el único entero r tal que $0 \leq r < m$ y $a \equiv r$ (mód m).

- $a = 129^{111}$, $m = 7$. Como $129 \equiv 3$ (mód 7), tenemos que:

$$129^{111} \equiv 3^{111} \pmod 7$$

Por otro lado, como 7 es primo y $111 \equiv 3$ (mód 6), por el pequeño teorema de Fermat, sabemos que:

$$3^{111} \equiv 3^3 \pmod 7$$

Finalmente, dado que $3^3 = 27 \equiv 6$ (mód 7), concluimos que:

$$129^{111} \equiv 6 \pmod 7$$

y entonces 6 es el resto de la división de 129^{111} por 7.

- $a = 129^{111}$, $m = 35$: En este caso, no podemos aplicar directamente el pequeño teorema de Fermat porque $m = 35 = 5 \cdot 7$ no es primo. Ahora bien, si hallamos r_1 y r_2 tales que:

$$\begin{cases} a \equiv r_1 & (\text{mód } 7) \\ a \equiv r_2 & (\text{mód } 5) \end{cases}$$

por el teorema chino del resto, podremos encontrar un único r tal que $0 \leq r < 7 \cdot 5 = 35$ con la propiedad:

$$\begin{cases} r \equiv r_1 & (\text{mód } 7) \\ r \equiv r_2 & (\text{mód } 5) \end{cases}$$

y tal que cualquier otra solución del sistema, en particular a, es congruente a r módulo 35. Esto implica que r es el resto de a en la división por 35.

Por el primer inciso de este ejercicio, sabemos que $a \equiv 6$ (mód 7). Para calcular el resto de a en la división por 5, observemos que $129 \equiv -1$ (mód 5), y entonces:

$$129^{111} \equiv (-1)^{111} \pmod 5$$

Luego, $a \equiv -1 \equiv 4$ (mód 5). Tenemos entonces que:

$$\begin{cases} a \equiv 6 & (\text{mód } 7) \\ a \equiv 4 & (\text{mód } 5) \end{cases}$$

Resolviendo este sistema de ecuaciones de congruencia nos queda que:

$$a \equiv 34 \pmod{35}$$

Es decir, que el resto de la división de 129^{111} por 35 es 34.

□ CAPÍTULO 4. Números racionales

Ejercicio 4.1. Queremos verificar que el producto de números naturales pensados como fracciones coincide con el producto usual. Para ello, si $a, b \in \mathbb{N}$, las fracciones que les asociamos son $\frac{a}{1}$, $\frac{b}{1}$. Al producto de ambos, $a \cdot b$, le asociamos la fracción $\frac{a \cdot b}{1}$ que coincide con el producto $\frac{a}{1} \cdot \frac{b}{1}$.

Ejercicio 4.2. Debemos probar que si $\frac{a}{b}$ es irreducible, y $\frac{c}{d}$ es una fracción equivalente a $\frac{a}{b}$, entonces existe un número entero m tal que $c = a \cdot m$ y $d = b \cdot m$. La definición de la relación de equivalencia dice que:

$$\frac{a}{b} \sim \frac{c}{d} \text{ si y sólo si } a \cdot d = b \cdot c.$$

Como $\frac{a}{b}$ es irreducible, mcd(a, b) = 1. Luego $b \mid a \cdot d$ y es coprimo con a, con lo cual, por la Proposición 2.4, tenemos que $b \mid d$. O sea existe $m \in \mathbb{Z}$ tal que $d = b \cdot m$. Reemplazando en la igualdad anterior tenemos que:

$$a \cdot b \cdot m = b \cdot c.$$

Cancelando b (que es no nulo), tenemos que:

$$a \cdot m = c$$

como queríamos probar.

Ejercicio 4.3. Queremos ver que si las fracciones $\frac{a}{b}$ y $\frac{c}{d}$ son equivalentes a las fracciones $\frac{\tilde{a}}{\tilde{b}}$ y $\frac{\tilde{c}}{\tilde{d}}$ respectivamente, entonces la fracción $\frac{a \cdot c}{b \cdot d}$ es equivalente a la fracción $\frac{\tilde{a} \cdot \tilde{c}}{\tilde{b} \cdot \tilde{d}}$. Por definición tenemos:

$$\begin{aligned} a \cdot \tilde{b} &= \tilde{a} \cdot b \\ c \cdot \tilde{d} &= \tilde{c} \cdot d. \end{aligned}$$

También por definición, $\frac{a \cdot c}{b \cdot d} \sim \frac{\tilde{a} \cdot \tilde{c}}{\tilde{b} \cdot \tilde{d}}$ si y sólo si:

$$a \cdot c \cdot \tilde{b} \cdot \tilde{d} = \tilde{a} \cdot \tilde{c} \cdot b \cdot d$$

Esta igualdad se obtiene simplemente multiplicando las dos igualdades anteriores.

Ejercicio 4.4.

- Dadas las fracciones $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{c_1}{d_1}, \frac{c_2}{d_2}$, podemos suponer que sus denominadores son positivos. Luego, de la definición:

$$\frac{a_1}{b_1} < \frac{c_1}{d_1} \quad \text{implica que } a_1 \cdot d_1 < b_1 \cdot c_1 \tag{9}$$
$$\frac{a_2}{b_2} < \frac{c_2}{d_2} \quad \text{implica que } a_2 \cdot d_2 < b_2 \cdot c_2 \tag{10}$$

  Queremos probar que $\frac{a_1}{b_1} + \frac{a_2}{b_2} < \frac{c_1}{d_1} + \frac{c_2}{d_2}$. Por definición de suma, queremos ver que $\frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} < \frac{c_1 \cdot d_2 + c_2 \cdot d_1}{d_1 \cdot d_2}$. Como los denominadores son positivos, la definición de que una fracción sea menor que la otra dice que esto es equivalente a:

$$(a_1 \cdot b_2 + a_2 \cdot b_1) \cdot d_1 \cdot d_2 < (c_1 \cdot d_2 + c_2 \cdot d_1) \cdot b_1 \cdot b_2$$

Esto se obtiene multiplicando la desigualdad (9) por el número natural $b_2 \cdot d_2$, la desigualdad (10) por el número natural $b_1 \cdot d_1$ y sumándolas.

- Nuevamente podemos asumir que los denominadores de las fracciones son positivos. La definición de que una fracción sea menor que la otra implica que $\frac{a}{b} < \frac{c}{d}$ si y sólo si:

$$a \cdot d < b \cdot c. \tag{11}$$

Por definición de producto de fracciones, $\frac{e}{f} \cdot \frac{a}{b} = \frac{e \cdot a}{f \cdot b}$ y $\frac{e}{f} \cdot \frac{c}{d} = \frac{e \cdot c}{f \cdot d}$.

La primera fracción es menor que la segunda si y sólo si:

$$e \cdot a \cdot f \cdot d < e \cdot c \cdot f \cdot b.$$

Esto se obtiene multiplicando la desigualdad (11) por el número natural $e \cdot f$ (usamos que $e/f > 0$ para poder asegurar que e es un número natural).

Ejercicio 4.5.
- $3{,}25 = 3 \cdot 10^0 + 2 \cdot 10^{-1} + 5 \cdot 10^{-2} = 3/1 + 2/10 + 5/100 = 325/100 = 13/4$.
- $4{,}3 = 4 \cdot 10^0 + 3 \cdot 10^{-1} = 4/1 + 3/10 = 43/10$.
- $3{,}14 = 314/100 = 157/50$.

Ejercicio 4.6. La expresión decimal de un número racional cualquiera es de la forma

$$d_n \cdot 10^n + \cdots + d_1 \cdot 10^1 + d_0 \cdot 10^0 + d_{-1} \cdot 10^{-1} + d_{-2} \cdot 10^{-2} + \cdots$$

donde cada número d_i está entre 0 y 9 y corresponden a los dígitos de la representación decimal. Este número lo escribimos por:

$$d_n \ldots d_1 d_0, d_{-1} d_{-2} \ldots$$

Además, los números con índice negativo son finitos o se repiten. Si multiplicamos dicho número por 10, obtenemos el número:

$$d_n \cdot 10^{n+1} + \cdots + d_1 \cdot 10^2 + d_0 \cdot 10^1 + d_{-1} \cdot 10^0 + d_{-2} \cdot 10^{-1} + \cdots$$

o sea obtenemos el número que escribimos por:

$$d_n \ldots d_1 d_0 d_{-1}, d_{-2} \ldots$$

Es claro que el efecto de mutiplicar el número por 10 fue simplemente mover la coma un lugar hacia la derecha.

Ejercicio 4.7. Utilizando el algoritmo, para calcular la expresión decimal de 1/8, calculamos:

$$\begin{aligned} 1 &= 0 \cdot 8 + 1 \\ 10 &= 1 \cdot 8 + 2 \\ 20 &= 2 \cdot 8 + 4 \\ 40 &= 5 \cdot 8 + 0. \end{aligned}$$

Luego, 1/8 = 0,125.

Ejercicio 4.8. El número racional 26,2914 se puede representar por la fracción 262.914/10.000 = 131.457/5.000 , siendo esta última irreducible.

El número racional 290,4377 se puede representar por la fracción 2.904.377/10.000, que es irreducible.

El número racional 946,17482 se puede representar por la fracción 94.617.482/10.0000 = 473.087.41/50.000, siendo esta última irreducible.

Ejercicio 4.9. El denominador de la fracción irreducible 8.729/2.000 es 2.000, que se factoriza como $2^4 \cdot 5^3$. Luego la potencia más grande es 4, con lo cual si multiplicamos por 10^4 obtenemos el número entero $5 \cdot 8\,729 = 43.645$. Así, 8.729/2.000 = 4,6345.

El denominador de la fracción irreducible 101/2.500 es 2.500, que se factoriza como $2^2 \cdot 5^4$. Luego la potencia más grande es 4 con lo cual, si multiplicamos por 104, obtenemos el número entero $2^2 \cdot 101 = 404$. Así, 101 / 2.500 = 0,0404.

El denominador de la fracción irreducible 19.283/6.250 es 6.250, que se factoriza como $2 \cdot 5^5$. Luego la potencia más grande es 5 con lo cual, si multiplicamos por 10^5, obtenemos el número entero $2^4 \cdot 19.283 = 308.528$. Así, 19.283/6.250 = 3,08528

Ejercicio 4.10. El ejercicio consiste sólo en una observación. No tiene respuesta.

Ejercicio 4.11. Para calcular la expresión decimal de un número racional $\frac{a}{b}$, con a y b positivos, vimos que debemos calcular el cociente y resto de dividir por b distintos números. Si dos restos se repiten, encontramos el período. La longitud del período es justamente el número de divisiones que hicimos entre el primero y el segundo de los restos iguales. Como el resto de dividir por b es un elemento entre 0 y b - 1, al calcular b + 1 divisiones, hay dos restos iguales. Esto dice que la longitud del período es a lo sumo b. Pero podemos decir algo más: si el resto en algún momento es 0, la expresión decimal es finita (dado que todos los sucesivos restos también serán cero). En este caso, podemos decir que el período es 0, y es a lo sumo b - 1 (porque b es no nulo). Si los restos de las divisiones son siempre no nulos, ellos son todos elementos entre 1 y b - 1. Luego el período tiene longitud a lo sumo b - 1 como queríamos ver.

Ejercicio 4.12. Para calcular la longitud del período de 1/9.091 sin calcularlo explícitamente, miramos la menor potencia r tal que $10^r \equiv 1$ (mód 9.091). Hacemos una tabla de las potencias

Potencia	Congruencia Módulo 9091	Potencia	Congruencia Módulo 9091
1	10	6	9081
2	100	7	8991
3	1000	8	8091
4	909	9	8182
5	9090	10	1

Luego el período tiene longitud 10. Si uno quiere verificarlo, su expresión decimal es $0,\overline{0001099989}$.

Ejercicio 4.13.

- Si $1/p$ tiene período de longitud 2, el primo p cumple que $10^2 \equiv 1$ (mód p). Luego p debe dividir a $10^2 - 1 = 99$. Como $99 = 3^2 \cdot 11$, las únicas posibilidades son $p = 3$ o $p = 11$. Pero $p = 3$ no sirve, porque $3 \mid 10^1 - 1$ (lo que implica que $1/3$ tiene período de longitud 1, como ya habíamos visto). Luego el único primo es $p = 11$. Efectivamente, $1/11 = 0,\overline{09}$, como habíamos visto.
- Para período de longitud 3, miramos la factorización de $10^3 - 1 = 999 = 3^3 \cdot 37$. Nuevamente $p = 3$ no sirve porque tiene período 1, con lo cual la única posibilidad es $p = 37$. Además, como $37 \nmid 9 = 10^1 - 1$ y $37 \nmid 99 = 10^2 - 1$, podemos asegurar que la longitud del período es exactamente 3.
- Para período de longitud 4, miramos la factorización de $10^4 - 1 = 9.999 = 3^2 \cdot 11 \cdot 101$. Como $3 \mid 9 = 10 - 1$, y $11 \mid 99 = 10^2 - 1$, ninguno de ellos nos sirve. Como $101 \nmid 9 = 10 - 1$, $101 \nmid 99 = 10^2 - 1$, $101 \nmid 999 = 10^3 - 1$, podemos asegurar que $1/101$ tiene período de longitud 4.
- Para período de longitud 5, miramos la factorización de $10^5 - 1 = 99.999 = 3^2 \cdot 41 \cdot 271$. En este caso, $p = 41$ y $p = 271$ sirven dado que ninguno de ellos divide a $10 - 1$, ni a $10^2 - 1$, ni a $10^3 - 1$, ni a $10^4 - 1$.
- Para período de longitud 6, miramos la factorización de $10^6 - 1 = 999.999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$. En este caso, $p = 7$ y $p = 13$ sirven porque ninguno de ellos divide a 9, ni a 99, ni a 999, ni a 9.999, ni a 99.999. Ya vimos en los casos anteriores que $1/3$ tiene período de longitud 1, $1/11$ tiene período de longitud 2 y $1/37$ tiene período de longitud 3.

□ CAPÍTULO 5: Números reales

Ejercicio 5.1. Supongamos primero que $|x| \leq a$. Si $x \geq 0$, entonces $|x| = x$, y luego $x \leq a$. Como $-a \leq 0$ se tiene que $-a \leq x \leq a$. Si $x < 0$, entonces $|x| = -x$. Por hipótesis se tiene que $-x \leq a$ lo que implica $-a \leq x$. Como $x \leq 0$ y $0 \leq a$ llegamos a que $x \leq a$ lo que implica $-a \leq x \leq a$.

Ahora, supongamos que $-a \leq x \leq a$. Luego, $x \leq a$ y $-a \leq x$. Por lo tanto, $x \leq a$ y $-x \leq a$. Como $|x| = x$ o $|x| = -x$ se deduce en ambos casos que $|x| \leq a$.

Ejercicio 5.2. Supongamos por el absurdo que exista una fracción $\frac{p}{q}$ tal que $(\frac{p}{q})^2 = 2^{2n+1}$. Luego $\frac{p^2}{q^2} = 2^{2n+1}$. Como $2^{2n+1} = 2^{2n} \cdot 2$, entonces $\frac{p^2}{q^2 \cdot 2^{2n}} = 2$ lo que implica $(\frac{p}{q \cdot 2^n})^2 = 2$. Luego $x = \frac{p}{q \cdot 2^n}$ es un número racional tal que $x^2 = 2$, llegando de esta manera a una contradicción.

Ejercicio 5.3. Sea n un número natural. Como $n < n+1$, por la definición del orden en los números racionales, se tiene que $\frac{1}{n+1} < \frac{1}{n}$. Luego, la sucesión $a_n = \frac{1}{n}$ es estrictamente decreciente.

Se tiene que $2^n < 2^n + 2^n = 2^{n+1}$. Nuevamente por la definición del orden entre fracciones, resulta que $\frac{1}{2^{n+1}} < \frac{1}{2^n}$. Luego, la sucesión $a_n = \frac{1}{2^n}$ es estrictamente decreciente.

Tenemos que $c_n = \frac{n}{n+1} = 1 - \frac{1}{n+1}$. Como $\frac{1}{n+2} < \frac{1}{n+1}$, entonces multiplicando esta desigualdad por -1 llegamos a que $-\frac{1}{n+1} < -\frac{1}{n+2}$. Sumando 1 en ambos miembros se obtiene $1 - \frac{1}{n+1} < 1 - \frac{1}{n+2}$ y luego $\frac{n}{n+1} < \frac{n+1}{n+2}$, lo que prueba que $c_n < c_{n+1}$ y por lo tanto c_n es estrictamente creciente.

Ejercicio 5.4. Tomar la sucesión constante $a_n = 1$ para todo $n \geq 1$.

Ejercicio 5.5.
1. Si $(a_n)_{n\geq 1}$ es creciente, entonces a_1 es una cota inferior de $(a_n)_{n\geq 1}$.
2. Si $(a_n)_{n\geq 1}$ es decreciente, entonces a_1 es una cota superior de $(a_n)_{n\geq 1}$.

Ejercicio 5.6. Se tiene $0 \leq \frac{n}{n+1} \leq 1$ para todo número natural n. También, $0 \leq \frac{1}{2^n} \leq 1$ para todo número natural n. Por último, $-1 \leq (-1)^n \leq 1$ para todo número natural n.

Ejercicio 5.7.
1. Sean $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ dos sucesiones crecientes y acotadas. Como $a_n \leq a_{n+1}$ y $b_n \leq b_{n+1}$ para todo n, se sigue que $a_n + b_n \leq a_{n+1} + b_{n+1}$. Luego $(a_n + b_n)_{n\geq 1}$ es creciente. Sean c, d, e, f números racionales tales que $c \leq a_n \leq d$ y $e \leq b_n \leq f$ para todo $n \geq 1$. Sumando miembro a miembro se tiene que $c + d \leq a_n + b_n \leq e + f$, lo que prueba que $(a_n + b_n)_{n\geq 1}$ es acotada.
2. Sean $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ dos sucesiones crecientes y acotadas de términos positivos. Como $a_n \leq a_{n+1}$, $b_n \leq b_{n+1}$, $a_n > 0$ y $b_n > 0$ para todo n se sigue que $a_n \cdot b_n \leq a_{n+1} \cdot b_n \leq a_{n+1} \cdot b_{n+1}$ lo que implica $a_n \cdot b_n \leq a_{n+1} \cdot b_{n+1}$. Sean c, d números racionales tales que $0 < a_n \leq c$ y $0 < b_n \leq d$ para todo n. Entonces $0 < a_n \cdot b_n \leq c \cdot d$ para todo n. Luego $(a_n \cdot b_n)_{n\geq 1}$ es creciente y acotada.

Ejercicio 5.8. Primero debemos probar que si $k \in \mathbb{N}$, la sucesión definida por $x_1 = 1$, $x_{n+1} = \frac{3kx_n - x_n^3}{2k}$ es creciente y acotada. Más aún, la sucesión x_n satisface que $x_n^2 \leq k$. Probemos esta desigualdad y el hecho de que x_n es creciente por inducción: el caso $n = 1$ es cierto pues al ser k un número natural, $x_1 = 1 \leq k$. Supongamos que es cierto para n, o sea que $x_n^2 \leq k$, y veamos que vale para $n + 1$, o sea que:

$$x_{n+1}^2 = \frac{(3kx_n - x_n^3)^2}{4k^2} \leq k$$

Debemos ver entonces que $(3kx_n - x_n^3)^2 = 9k^2x_n^2 - 6kx_n^4 + x_n^6 \leq 4k^3$, equivalentemente, que $x_n^6 - 6kx_n^4 + 9k^2x_n^2 - 4k^3 \leq 0$. Como hicimos para $k = 2$, si llamamos $y = x_n^2 - k$ tenemos:

$$y^2 = x_n^4 - 2kx_n^2 + k^2,$$
$$y^3 = x_n^6 - 3kx_n^4 + 3k^2x_n^2 - k^3$$

por lo que:
$y^3 - 3ky^2 = x_n^6 - 3kx_n^4 + 3k^2x_n^2 - k^3 - 3k(x_n^4 - 2kx_n^2 + k^2) = x_n^6 - 6kx_n^4 + 9k^2x_n^2 - 4k^3$
Es decir, debemos probar que $y^3 - 3ky^2 \leq 0$, o, en otros términos, que $y^2(y - 3k) \leq 0$.

Pero observemos que la hipótesis inductiva es precisamente que $y \leq 0$, por lo que $y^2 \geq 0$ e $y - 3k \leq 0$, y así $y^2(y - 3k) \leq 0$.

Para ver que es creciente, debemos ver que:

$$x_{n+1} = \frac{3kx_n - x_n^3}{2k} \geq x_n$$

Equivalentemente, debemos ver que $3kx_n - x_n^3 \geq 2kx_n$ que es lo mismo que $kx_n \geq x_n^3$. Como por hipótesis inductiva x_n es creciente, el ser $x_1 = 1$ implica que $x_n \geq 0$. Luego, la desigualdad $kx_n \geq x_n^3$ se deduce inmediatamente del hecho de ser $x_n^2 \leq k$.

Por último, queremos ver que la sucesión x_n^2 converge a k. Esto es lo mismo que probar que $x_n^2 - k$ converge a 0. Llamemos $e_n = x_n^2 - k$. Entonces:

$$\begin{aligned} e_{n+1} &= \frac{(3kx_n - x_n^3)^2}{4k^2} - k \\ &= \frac{9k^2x_n^2 - 6kx_n^4 + x_n^6 - 4k^3}{4k^2} \\ &= \frac{e_n^2(e_n - 3k)}{4k^2} \end{aligned}$$

(observando que e_n es lo que antes llamamos y). Pero ya probamos que para todo n vale $1 \leq x_n^2 < k$, por lo que $1 - k \leq x_n^2 - k < 0$, es decir $1 - 4k \leq e_n - 3k < -3k$. En valor absoluto, tenemos $|e_n - 3k| \leq 4k - 1$, y esto dice que $|e_{n+1}| = e_n^2 \frac{|e_n - 3k|}{4k^2} \leq e_n^2 \frac{4k-1}{4k^2} < \frac{e_n^2}{k}$
Como $|e_n| \leq 1$, tenemos $e_n^2 \leq |e_n|$, por lo que:
$|e_{n+1}| \leq \frac{|e_n|}{k} \leq \frac{|e_{n-1}|}{k^2} \leq \frac{|e_{n-2}|}{k^3} \leq \cdots \leq \frac{|e_1|}{k^n} = \frac{k-1}{k^n}$, y esto demuestra que e_n converge a 0.

Ejercicio 5.9. Si $\frac{p}{q}$ es un número racional positivo, con p, q números naturales, entonces del ejercicio 5.8 sabemos que existen dos números reales positivos x, y tales que $x^2 = p$ e $y^2 = q$. Luego $(\frac{x}{y})^2 = \frac{x^2}{y^2} = \frac{p}{q}$.

Ejercicio 5.10. La relación es reflexiva, porque si $(a_n)_{n\geq 1}$ es una sucesión en *Sucec*($\mathbb{Q}$), entonces $\lim_{n\to\infty}(a_n - a_n) = \lim_{n\to\infty} 0 = 0$. Por otra parte, si $(b_n)_{n\geq 1}$ es otra sucesión en *Sucec*($\mathbb{Q}$) tal que $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$, entonces $\lim_{n\to\infty}(a_n - b_n) = 0$, y por lo tanto $\lim_{n\to\infty}(b_n - a_n) = \lim_{n\to\infty} -(a_n - b_n) = -0 = 0$. Esto dice que la relación es simétrica. Por último, si $(a_n)_{n\geq 1} \sim (b_n)_{n\geq 1}$ y $(b_n)_{n\geq 1} \sim (c_n)_{n\geq 1}$, entonces:

$$\begin{aligned} \lim_{n\to\infty}(a_n - c_n) &= \lim_{n\to\infty}(a_n - b_n) + (b_n - c_n) \\ &= \lim_{n\to\infty}(a_n - b_n) + \lim_{n\to\infty}(b_n - c_n) \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

lo que muestra que la relación es transitiva.

Ejercicio 5.11. Para probar esta identidad observemos primero que si n y m son dos números naturales y x es un número real positivo, entonces $\sqrt[n]{x^m} = (\sqrt[n]{x})^m$. En efecto,

$((\sqrt[n]{x})^m)^n = ((\sqrt[n]{x})^n)^m = x^m$ lo que prueba $\sqrt[n]{x^m} = (\sqrt[n]{x})^m$. De un modo similar se demuestra que $\sqrt[n]{\sqrt[m]{x}} = \sqrt[n\cdot m]{x}$

Sean $k = \frac{r}{s}$, $l = \frac{p}{q}$ números racionales, donde *s* y *q* son números naturales. La identidad es obvia si $k = 0$ o si $l = 0$. Supongamos que *k* y *l* son positivos, es decir $r > 0$ y $p > 0$. Luego $(a^k)^l = \sqrt[q]{(a^k)^p}$. Usando las identidades anteriores se obtiene $\sqrt[q]{(a^k)^p} = \sqrt[q]{(\sqrt[s]{a^r})^p} = \sqrt[q]{\sqrt[s]{a^{p\cdot r}}} = \sqrt[s\cdot q]{a^{p\cdot r}} = a^{k\cdot l}$. Si $k < 0$ ó $l < 0$ la identidad se prueba en forma análoga usando que $a^{-1} = \frac{1}{a}$.

□ CAPÍTULO 6. Números complejos

EJERCICIO 6.1.

$$z - w = -\frac{5}{2} + 4i \qquad w - z = \frac{5}{2} - 4i$$
$$2z = -4 + 12i \qquad 4w - 3z = (2 + 8i) - (-6 + 18i)$$
$$z \cdot w = -1 - 12 - 4i + 3i \qquad = 8 - 10i$$
$$= -13 - i \qquad z^2 = 4 - 36 - 2 \cdot 2 \cdot 6i$$
$$= -32 - 24i$$

EJERCICIO 6.2. $\overline{7 - 2i} = 7 + 2i$ (el conjugado del conjugado es el número original). $\overline{4} = 4$, $\overline{i} = -i$, $\overline{-i} = i$.

EJERCICIO 6.3.

$$(3+4i)\cdot(\frac{3}{25} - \frac{4}{25}i) = (3\cdot\frac{3}{25} - (-1)\cdot 4\cdot\frac{4}{25}) + (-3\cdot\frac{4}{25} + 4\cdot\frac{3}{25})i$$
$$= (\frac{9}{25} + \frac{16}{25}) + (-\frac{12}{25} + \frac{12}{25})i$$
$$= \frac{25}{25} + 0\ i$$
$$= 1$$

$$(\frac{18}{25} + \frac{1}{25}i)\cdot(3+4\ i) = (\frac{18}{25}\cdot 3 - \frac{1}{25}\cdot 4) + (\frac{18}{25}\cdot 4 + \frac{1}{25}\cdot 3)i$$
$$= (\frac{54}{25} - \frac{4}{25}) + (\frac{72}{25} + \frac{3}{25})i$$
$$= \frac{50}{25} + \frac{75}{25}i$$
$$= 2 + 3\ i$$

EJERCICIO 6.4.

$$\arg(4) = 0, \qquad \arg(1+i) = \frac{\pi}{4}, \qquad \arg(2+2i) = \frac{\pi}{4}, \qquad \arg(8i) = \frac{\pi}{2},$$
$$\arg(-8i) = \frac{3\pi}{2}, \qquad \arg(-7) = \pi, \qquad \arg(2-2i) = \frac{7\pi}{4}$$

EJERCICIO 6.5.

$$1 + i = (\sqrt{2}\,;\ \frac{\pi}{4}) \qquad 1 - i = (\sqrt{2}\,;\ \frac{7\pi}{4}) \qquad -1 + i = (\sqrt{2}\,;\ \frac{3\pi}{4})$$
$$-1 - i = (\sqrt{2}\,;\ \frac{5\pi}{4}) \qquad 2 + 2i = (2\sqrt{2}\,;\ \frac{\pi}{4}) \qquad -3 - 3i = (3\sqrt{2}\,;\ \frac{5\pi}{4})$$
$$4 - 4i = (4\sqrt{2}\,;\ \frac{7\pi}{4}) \qquad 4 = (4\,;\ 0) \qquad -5 = (5\,;\ \pi)$$

EJERCICIO 6.6. Como $2i - (-2 + i) = 2 + i$, entonces calculamos:

k	z_k	$z_k \cdot (2+i)$	$z_k \cdot (2+i) + (-2+i)$
0	1	$2+i$	$2i$
1	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$\frac{-2-\sqrt{3}}{2} + i\frac{-1+2\sqrt{3}}{2}$	$\frac{-6-\sqrt{3}}{2} + i\frac{1+2\sqrt{3}}{2}$
2	$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$	$\frac{-2+\sqrt{3}}{2} + i\frac{-1-2\sqrt{3}}{2}$	$\frac{-6+\sqrt{3}}{2} + i\frac{1-2\sqrt{3}}{2}$

Para el segundo problema, si $x_0 = 1 + i$, $x_1 = -3 + 2i$ y x_2 es el tercer vértice, entonces $\frac{x_2-x_0}{x_1-x_0}$ es una raíz cúbica de la unidad. Por lo tanto, hay dos soluciones:

$$x_2 = (-\frac{1}{2} + \frac{\sqrt{3}}{2}i) \cdot (x_1 - x_0) + x_0 \qquad \text{o bien} \qquad x_2 = (-\frac{1}{2} - \frac{\sqrt{3}}{2}i) \cdot (x_1 - x_0) + x_0$$
$$= (-\frac{1}{2} + \frac{\sqrt{3}}{2}i) \cdot (-4+i) + 1 + i \qquad = (-\frac{1}{2} - \frac{\sqrt{3}}{2}i) \cdot (-4+i) + 1 + i$$
$$= (3 - \frac{\sqrt{3}}{2}) + (\frac{1}{2} - 2\sqrt{3})i, \qquad = (3 + \frac{\sqrt{3}}{2}) + (\frac{1}{2} + 2\sqrt{3})i$$

Ejercicio 6.7. Una de las raíces es $(2\,;\,\frac{2\pi}{12}) = \sqrt{3} + i$. Las otras se obtienen multiplicando esta raíz por las raíces octavas de la unidad:

$$(1\,;\,\frac{\pi}{4}) \cdot (2\,;\,\frac{2\pi}{12}) = (2\,;\,\frac{5\pi}{12})$$
$$= (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) \cdot (\sqrt{3}+i)$$
$$= \frac{\sqrt{6}-\sqrt{2}}{2} + \frac{\sqrt{2}+\sqrt{6}}{2}i$$

$$(1\,;\,\frac{2\pi}{4}) \cdot (2\,;\,\frac{2\pi}{12}) = (2\,;\,\frac{8\pi}{12})$$
$$= i \cdot (\sqrt{3}+i)$$
$$= -1 + \sqrt{3}i$$

$$(1\,;\,\frac{3\pi}{4}) \cdot (2\,;\,\frac{2\pi}{12}) = (2\,;\,\frac{11\pi}{12})$$
$$= (-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i) \cdot (\sqrt{3}+i)$$
$$= \frac{-\sqrt{6}-\sqrt{2}}{2} + \frac{-\sqrt{2}+\sqrt{6}}{2}i$$

$$(1\,;\,\frac{4\pi}{4}) \cdot (2\,;\,\frac{2\pi}{12}) = (2\,;\,\frac{14\pi}{12})$$
$$= (-1) \cdot (\sqrt{3}+i)$$
$$= -\sqrt{3} - i$$

$$(1\,;\,\frac{5\pi}{4}) \cdot (2\,;\,\frac{2\pi}{12}) = (2\,;\,\frac{17\pi}{12})$$
$$= (-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i) \cdot (\sqrt{3}+i)$$
$$= \frac{-\sqrt{6}+\sqrt{2}}{2} - \frac{\sqrt{2}+\sqrt{6}}{2}i$$

$$(1\,;\,\tfrac{6\pi}{4})\cdot(2\,;\,\tfrac{2\pi}{12}) = (2\,;\,\tfrac{20\pi}{12})$$
$$= (-i)\cdot(\sqrt{3}+i)$$
$$= 1-\sqrt{3}i$$

$$(1\,;\,\tfrac{7\pi}{4})\cdot(2\,;\,\tfrac{2\pi}{12}) = (2\,;\,\tfrac{23\pi}{12})$$
$$= (\tfrac{\sqrt{2}}{2}-\tfrac{\sqrt{2}}{2}i)\cdot(\sqrt{3}+i)$$
$$= \tfrac{\sqrt{6}+\sqrt{2}}{2}+\tfrac{\sqrt{2}-\sqrt{6}}{2}i$$

Calculamos la forma polar de $-8-8\sqrt{3}i$: $|-8-8\sqrt{3}i| = \sqrt{8^2+8^2\cdot 3} = 8\sqrt{4} = 16$, y si $\alpha = \arg(-8-8\sqrt{3}i)$, entonces $\cos\alpha = \frac{-8}{16} = -\frac{1}{2}$ y sen $\alpha = \frac{-8\sqrt{3}}{16} = -\frac{\sqrt{3}}{2}$, por lo que $\alpha = \frac{4\pi}{3}$. Las formas polares de las raíces octavas son iguales a las anteriores, pero cambiando los módulos por $\sqrt{2}$ en lugar de 2: $(\sqrt{2}\,;\,\frac{2\pi}{12})$, $(\sqrt{2}\,;\,\frac{5\pi}{12})$, $(\sqrt{2}\,;\,\frac{8\pi}{12})$, $(\sqrt{2}\,;\,\frac{11\pi}{12})$, $(\sqrt{2}\,;\,\frac{14\pi}{12})$, $(\sqrt{2}\,;\,\frac{17\pi}{12})$, $(\sqrt{2}\,;\,\frac{20\pi}{12})$, $(\sqrt{2}\,;\,\frac{23\pi}{12})$

Ejercicio 6.8. Si $x = -\frac{3}{4}+\frac{\sqrt{7}}{4}i$, entonces $x^2 = \frac{9-7}{16} - 2\frac{3\sqrt{7}}{16}i = \frac{1}{8} - \frac{3\sqrt{7}}{8}i$ por lo que $2x^2+3x+2 = \frac{1}{4} - \frac{3\sqrt{7}}{4}i - \frac{9}{4} + \frac{3\sqrt{7}}{4}i + 2 = -\frac{8}{4}+2 = 0$.

Ejercicio 6.9. Calculamos *u* y *v*:

$$u = \sqrt[3]{\frac{6}{2}+\sqrt{\frac{36}{4}+\frac{729}{27}}} \qquad v = \sqrt[3]{\frac{6}{2}-\sqrt{\frac{36}{4}+\frac{729}{27}}}$$
$$= \sqrt[3]{3+\sqrt{9+27}} \qquad = \sqrt[3]{3-\sqrt{9+27}}$$
$$= \sqrt[3]{9} \qquad = \sqrt[3]{-3}$$
$$= -\sqrt[3]{3}$$

por lo que las soluciones son:

$$\sqrt[3]{9}-\sqrt[3]{3}$$
$$(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)\sqrt[3]{9} - (-\frac{1}{2}-\frac{\sqrt{3}}{2}i)\sqrt[3]{3} = \frac{-\sqrt[3]{9}+\sqrt[3]{3}}{2} + \frac{\sqrt{3}(\sqrt[3]{9}+\sqrt[3]{3})}{2}i$$
$$(-\frac{1}{2}-\frac{\sqrt{3}}{2}i)\sqrt[3]{9} - (-\frac{1}{2}+\frac{\sqrt{3}}{2}i)\sqrt[3]{3} = \frac{-\sqrt[3]{9}+\sqrt[3]{3}}{2} - \frac{\sqrt{3}(\sqrt[3]{9}+\sqrt[3]{3})}{2}i$$

Ejercicio 6.10. La ecuación $x^3 = 15x + 4$ es equivalente a $x^3 - 15x - 4 = 0$, por lo que nuevamente calculamos *u* y *v*:

$$u = \sqrt[3]{\frac{4}{2}+\sqrt{\frac{16}{4}+\frac{-3.375}{27}}} \qquad v = \sqrt[3]{\frac{4}{2}-\sqrt{\frac{16}{4}+\frac{-3.375}{27}}}$$
$$= \sqrt[3]{2+\sqrt{4-125}} \qquad = \sqrt[3]{2-\sqrt{4-125}}$$
$$= \sqrt[3]{2+11i} \qquad = \sqrt[3]{2-11i}$$

Como está dicho al presentar la fórmula, hay tres raíces posibles tanto para u como para v. Se deben tomar u y v de manera que su producto sea $-p/3 = 5$. Podemos tomar $\alpha = \arg(2 + 11i)$ y elegir $u = (\sqrt{5}\,;\ \frac{\alpha}{3})$ y $v = (\sqrt{5}\,;\ -\frac{\alpha}{3})$. Las soluciones son entonces:

$$\begin{aligned} u + v &= (\sqrt{5}\,;\ \frac{\alpha}{3}) + (\sqrt{5}\,;\ -\frac{\alpha}{3}) \\ &= 2\sqrt{5}\cos\frac{\alpha}{3} \end{aligned}$$

$$\begin{aligned} wu + w^2 v &= (\sqrt{5}\,;\ \frac{\alpha+2\pi}{3}) + (\sqrt{5}\,;\ -\frac{\alpha+2\pi}{3}) \\ &= 2\sqrt{5}\cos\frac{\alpha+2\pi}{3} \end{aligned}$$

$$\begin{aligned} w^2 u + wv &= (\sqrt{5}\,;\ \frac{\alpha+4\pi}{3}) + (\sqrt{5}\,;\ -\frac{\alpha+4\pi}{3}) \\ &= 2\sqrt{5}\cos\frac{\alpha+4\pi}{3} \end{aligned}$$

Las tres raíces son reales, aunque puede verse que la primera es la única positiva, por lo que debe ser igual a 4. Para ver que la segunda y la tercera son negativas, hay que comprobar que los ángulos $\frac{\alpha+2\pi}{3}$ y $\frac{\alpha+4\pi}{3}$ están entre $\frac{\pi}{2}$ y $\frac{3\pi}{2}$. Como $\alpha = \arg(2+11i)$, sabemos que $0 < \alpha < \frac{\pi}{2}$. Entonces, queremos comprobar que $\frac{\pi}{2} < \frac{\alpha+2\pi}{3} < \frac{3\pi}{2}$, pero esto es equivalente, multiplicando todo por 6, a $3\pi < 2\alpha + 4\pi < 9\pi$, y a su vez esto es equivalente, restando 4π, a $-\pi < 2\alpha < 5\pi$, que es cierto.

De la misma manera, queremos ver que $\frac{\pi}{2} < \frac{\alpha+4\pi}{3} < \frac{3\pi}{2}$, pero esto es equivalente, multiplicando todo por 6, a $3\pi < 2\alpha + 8\pi < 9\pi$, y a su vez esto es equivalente, restando 8π, a $-5\pi < 2\alpha < \pi$, que también es cierto.

Ejercicio 6.11. Debemos probar que para todo $n \in \mathbb{N}$ es $|m_{n,c}| \geq |c|$. Si $n = 1$, tenemos $m_{n,c} = m_{1,c} = c$, por lo que automáticamente vale $|m_{1,c}| \geq |c|$. Suponiendo ahora que vale que $|m_{n,c}| \geq |c|$, debemos probar que $|m_{n+1,c}| \geq |c|$.

Pero

$$\begin{aligned} |m_{n+1,c}| &= |m_{n,c}^2 + c| \geq |m_{n,c}^2| - |c| \\ &= |m_{n,c}|^2 - |c| \geq |c|^2 - |c| \end{aligned}$$

Por otra parte, como $|c| > 2$, resulta que $|c|^2 - |c| > 2|c| - |c| = |c|$, de donde se obtiene la desigualdad buscada.

Ejercicio 6.12. Ahora debemos probar la afirmación $|m_{k,c}| > 2$ para $k \geq n$. Si $k = n$, ya nos dicen que $|m_{k,c}| = |m_{n,c}| > 2$. Y si vale la afirmación $|m_{k,c}| > 2$, entonces $|m_{k+1,c}| = |m_{k,c}^2 + c| \geq |m_{k,c}^2| - |c| > 2^2 - |c| \geq 2^2 - 2 = 2$.

Ejercicio 6.13. Si bien los contenidos matemáticos para hacer el programa están incluidos en el libro, los contenidos de computación no lo están. Es por eso que se deja este ejercicio sin una respuesta, y se destina a quienes tengan este conocimiento.

APÉNDICE. Algoritmos

En este capítulo presentamos los algoritmos del libro en el lenguaje Python. Elegimos Python porque, entre otras cosas, permite definir en una misma instrucción más de una variable. Como ejemplo, si tenemos $a = 2$ y $b = 1$, luego de la instrucción:

```
a,b = a+b,a-b
```

los valores de a y b serán respectivamente 3 (porque 3 = 2+1) y 1 (porque 1 = 2 - 1).

□ 1. Algoritmo de división

Éste es el algoritmo de división que vimos en la sección 3.2 del capítulo 2. No es el algoritmo más rápido, porque va restando del número original el divisor, hasta que se queda con un resto pequeño.

```
def division(n,d):
   if d==0:
        return 0,0
   if (n>=0) and (d>0):
        q,r = 0,n
        while (r >= d):
        q,r = q+1,r-d
        return q,r
   if (n>=0) and (d<0):
        q,r = division(n,-d)
        return -q,r
   if (n<0) and (d>0):
        q,r = division(-n,d)
        if r==0:
            return -q,0
        else:
            return -q-1,d-r
   else:
        q,r = division(-n,-d)
        if r==0:
            return q,0
        else:
            return q+1,-r-d
```

En realidad, en Python ya hay una implementación del algoritmo de división. El cociente entre los números enteros a y b se obtiene con $\frac{a}{b}$, mientras que el resto se obtiene con `a%b`.

□ 2. Escritura en una nueva base

La función `baseb(n,b)` devuelve como secuencia la escritura del número *n* en base *b*, siguiendo el algoritmo de la sección 4 del capítulo 2.

```
def baseb(n,b):
   m = n
   s = [ ]
   while m != 0:
        q = m/b
        r = m%b
        s = [r] + s
        m = q
   return s
```

En Python se usa `!=` en lugar de ≠. La instrucción `s = [r] + s` agrega el número *r* al comienzo de la lista *s*.

□ 3. Algoritmo de Euclides

La función `mcd(a,b)` devuelve el máximo común divisor entre *a* y *b* siguiendo el algoritmo de Euclides de la sección 5.1 del capítulo 2.

```
def mcd(a,b):
   r1,r2 = a,b
   while r2 != 0:
        r = r1 % r2
        r1,r2 = r2,r
   return r1
```

La función `mcdcompleto(a,b)` devuelve tres números: *d, s, t*, donde

- *d* es el *mcd* entre *a* y *b*
- *s* y *t* son enteros que permiten escribir *d* en términos de *a* y *b*: $d = s \cdot a + t \cdot b$.

```
def mcdcompleto(a,b):
   r1,r2 = a,b
   s1,s2,t1,t2 = 1,0,0,1
   while r2 != 0:
        q = r1 / r2
        r = r1 % r2
        s1,s2 = s2,s1-q*s2
        t1,t2 = t2,t1-q*t2
        r1,r2 = r2,r
   return r1,s1,t1
```

El algoritmo funciona correctamente porque en cada paso se tiene que:

- $r_1 = s_1 \cdot a + t_1 \cdot b$, y
- $r_2 = s_2 \cdot a + t_2 \cdot b$.

En cada paso, se reemplazan r_1 y r_2 por r_2 y r, donde r es el resto de dividir r_1 por r_2, es decir, $r_1 = q \cdot r_2 + r$. Para seguir teniendo las igualdades anteriores, se calcula:

$$\begin{aligned} r &= r_1 - q \cdot r_2 = (s_1 \cdot a + t_1 \cdot b) - q \cdot (s_2 \cdot a + t_2 \cdot b) \\ &= (s_1 - q \cdot s_2) \cdot a + (t_1 - q \cdot t_2) \cdot b \end{aligned}$$

Además, esta igualdad vale en el primer paso, pues $r_1 = a = 1 \cdot a + 0 \cdot b$ y $r_2 = b = 0 \cdot a + 1 \cdot b$. Por lo tanto, vale hasta que se termina el algoritmo. Entonces, como en el último paso el *mcd* está en la variable r_1, los coeficientes s_1 y t_1 dan la combinación lineal buscada.

□ 4. Ecuaciones diofánticas y de congruencia

El siguiente algoritmo devuelve una solución de la ecuación $a \cdot x + b \cdot y = c$ si $mcd(a, b) \mid c$. Si no hay solución, devuelve el par `None,None`, que indica que no hay solución posible. Todas las soluciones (y la solución particular encontrada) se calculan como vimos en la sección 1 del capítulo 3.

```
def resolver(a,b,c):
   d = mcd(a,b)
   if (c%d) != 0:
        return None,None
   else:
        r,s,t = mcdcompleto(a,b)
        return s*c/d,t*c/d
```

El algoritmo que sigue busca las soluciones de la ecuación $a \cdot x \equiv b \pmod{m}$. Si no las hay, devuelve `None,None`. Si las hay, devuelve el par $x_0, \frac{m}{mcd(a,m)}$, mediante el cual se pueden encontrar todas las soluciones como $x \equiv x_0 \pmod{\frac{m}{mcd(a,m)}}$. Vimos esto en la sección 3 del capítulo 3.

```
def ecuacong(a,b,m):
   d = mcd(a,m)
   if (b%d) != 0:
        return None,None
   a,m,b = a/d, m/d, b/d
   s,t = resolver(a,m,b)
   return s % m, m
```

El siguiente algoritmo es una variante del presentado en la sección 6 del capítulo 3. Si se usa con listas, como en `teochino([14,17],[49,45])`, devuelve las soluciones del sistema:

$$\begin{cases} x \equiv 14 \text{ (mód 49)} \\ x \equiv 17 \text{ (mód 45)} \end{cases}$$

en la forma (602, 2.205), que significa que las soluciones son los enteros $x \equiv 602$ (mód 2.205).

Esta versión también se puede aplicar en el caso en que los módulos $m_1, \ldots, m_n$ no son coprimos de a pares. Como en este caso a veces no hay solución, si no la hay el algoritmo devuelve `None,None`.

```
def teochino(a,m):
   M = m[0]
   A = a[0]
   for i in range(len(m)-1):
      Q,n = ecuacong(M,a[i+1]-A,m[i+1])
      if Q==None:
         return None,None
      M,A = M*n,M*Q+A
   return A,M
```

□ 5. Desarrollo decimal de un número racional

Si a y b son números naturales, con el siguiente algoritmo devolvemos (e, Q_1, Q_2), donde $\frac{a}{b} = e, Q_1\overline{Q_2}$. Por ejemplo, decimal (19,14) devuelve:

```
(1, [3], [5, 7, 1, 4, 2, 8])
```

Significa que $\frac{19}{14} = 1,3\overline{571428}$. Entonces, el algoritmo presentado en la sección 3 del capítulo 4, es:

```
def decimal(a,b):
   e = a/b
   r = a%b
   R,Q = [ ],[ ]
   while r != 0:
      if r in R:
         return e,Q[:R.index(r)],Q[R.index(r):]
      R = R + [r]
      Q = Q + [(10*r)/b]
      r = (10*r) % b
   return e,Q,[ ]
```

El condicional `if r in R` es verdadero si el elemento r figura en la lista R. La función `R.index(r)` devuelve la posición en que se encuentra. Por último, `Q[:i]` da la lista Q desde el comienzo hasta la posición anterior a i, mientras que `Q[i:]` devuelve el resto.