La saga de los números

Números, Conjuntos y Demostraciones

Antonio Córdoba Barba

Per a la formiga
de la chicharra

. . . fiz este libro, compuesto de las más apuestas palabras que yo pude, et entre las palabras entremetí algunos enxiemplos de que se podrían aprovechar los que las oyeren. Et esto fiz según la manera que facen los físicos. . . Et a esta semejanza. . . será fecho este libro, et los que lo leyeren, si por su voluntad tomaren placer de las cosas provechosas, que y fallaren, serles ha bien, et aun los que tan bien non entendieren, non podrán excusar que en leyendo este libro, por las palabras falagueras et apuestas que en él fallarán, que non hayan a leer las cosas aprovechosas que son y mezcladas, et aunque ellos non lo deseen, aprovecharse han dellas. . .

Infante Juan Manuel
(Prólogo de *El conde Lucanor*)

Índice general

— 0 —

Prólogo o epílogo: La vida es un número

Llévaste dos mil suspiros.
Que, a ser de fuego, pudieran
abrasar a dos mil Troyas,
si dos mil Troyas hubieran.

Miguel de Cervantes
(El Quijote)

Cuenta la leyenda que, mientras paseaba, Pitágoras reparó en el sonido producido al golpear sobre el yunque los martillos de un herrero; tres de ellos sonaban acompasados pero había un cuarto que desafinaba notoriamente. Pitágoras se interesó por el fenómeno y requirió los martillos que pesó y midió tratando de encontrar algún tipo de explicación. Luego experimentó con la vibración de las cuerdas, observando los cambios de sonido producidos al variar sus longitudes y creando un instrumento, el monocordio, con el que logró establecer una teoría musical basada en fracciones numéricas sencillas, que es la escala que ahora llamamos pitagórica. Hay quien ve en este episodio el comienzo de la ciencia griega, al introducir la idea, entonces novedosa, de que las leyes de la naturaleza pueden ser descritas por medio de las matemáticas. Pitágoras y su escuela fueron mucho más allá y elaboraron una cosmogonía basada en los números enteros que, decían, eran la esencia de todo lo que es.

Son historias de hace unos veintiséis siglos. Años más tarde tuvo lugar una de las primeras revoluciones científicas de las que se tiene noticia, siendo su protagonista Hipaso de Metaponto que era también miembro de la escuela pitagórica. Se trata del descubrimiento de los números irracionales y, en particular, de que la diagonal de un cuadrado de lado 1 tiene una longitud que es inconmensurable con la unidad (la raíz cuadrada de 2 no es racional o cociente de dos enteros), lo que fue una deducción revolucionaria que vino a perturbar profundamente la explicación pitagórica del mundo. Según la leyenda Hipaso pagó con su vida haber hecho tamaña observación: otros miembros de la escuela lo echaron por la borda del barco en el que viajaban cuando Hipaso les mostró la prueba.

No existen documentos fehacientes que certifiquen la verdad de estas historias, por lo que no conviene tomarlas al pie de la letra. Empero, el descubrimiento de los irracionales supuso una crisis profunda en la matemática del período clásico griego, como puede observarse en los *Elementos* de Euclides que, aunque es una publicación muy posterior, recoge el saber matemático de aquellos tiempos. Luego, ya en la etapa alejandrina, Arquímedes supo cómo tratar las magnitudes irracionales, y calcular las primeras cifras decimales de $\pi = 3{,}1415\ldots$ basándose en una fórmula recursiva que relaciona entre sí a los perímetros de los polígonos regulares de n y $2n$ lados inscritos en una circunferencia de radio unidad. Ahora una sencilla calculadora de bolsillo nos permite fácilmente añadir otras cifras a ese desarrollo aplicando la misma fórmula de Arquímedes. Con la ayuda de ordenadores potentes, y con algoritmos algo más sofisticados, se han logrado calcular cientos de miles de millones de cifras decimales de π, aunque eso no quita ningún mérito a la proeza de Arquímedes, quien hizo sus cálculos "a la griega", sin computadores y sin nuestro eficiente y cómodo sistema decimal de numeración.

La lengua y las matemáticas son los pilares de la ilustración y desempeñan un papel fundamental en la educación primaria y secundaria. En contra de cierta opinión demasiado generalizada, me parece que los conceptos y los problemas matemáticos considerados en esos niveles son relativamente sencillos e intuitivos. Y es por esa razón que pueden ser abordados con cierta profundidad sirviendo para entrenar la mente en el arte del razonamiento preciso. Dicho en la jerga moderna, son útiles para instalar el sistema operativo en el cerebro humano, algo que resultaría mucho más difícil de conseguir a través de otras disciplinas, que están menos estructuradas y cuyos conceptos son más complejos y difusos.

Desde Galileo viene diciéndose que las matemáticas son el lenguaje en el que se expresa la naturaleza. También suele afirmarse que un matemático muestra su habilidad a través de la claridad y la precisión. Comparado con los modos de expresión de otras ciencias, más barrocos y caóticos, el lenguaje de la nuestra resulta sobrio y, desde luego, preciso. No obstante, puede llegar a convertirse en una barrera difícil de franquear para la generalidad de los ciudadanos que carece de la destreza adecuada en el manejo de los modos de razonamiento y de los conceptos involucrados. Cuando los expertos de otras materias científicas divulgan sus resultados suelen eliminar todas las ecuaciones de sus modelos, pero eso no es razonable hacerlo si de lo que se trata es, precisamente, de acercar las matemáticas a los ciudadanos. La divulgación de nuestra investigación es, intrínsecamente, una tarea tan difícil que esta acaba siendo invisible a la sociedad, a pesar de que sus resultados son necesarios tanto para la ciencia y la tecnología como para el desempeño

de muchas actividades cotidianas. La gente, y los medios de comunicación, no suelen ser muy conscientes de su utilidad. Por el contrario, todo profesor de matemáticas ha sido alguna vez preguntado con cierto retintín: ¿Y para qué sirve lo que haces? Una de las respuestas más originales la dio A. Wiles en una entrevista que le hicieron en Barcelona en el año 2000. Contestó a la gallega, con otra pregunta: ¿Y para qué sirve el castellano? Aunque el lenguaje de las matemáticas y las matemáticas como idioma de la ciencia son temas recurrentes a lo largo de este libro, su primer capítulo está dedicado, precisamente, a establecer unas mínimas bases de partida, a saber: principio de inducción, teoría ingenua de conjuntos y cálculo de proposiciones.

Los números llamados naturales, tales como $1, 2, 3, \ldots, 100, \ldots, 1999, \ldots$ son piezas fundamentales de nuestro idioma que nos sirven para contar los elementos de un conjunto (uno, dos, tres, ..., cien, ..., mil novecientos noventa y nueve, ...) en su versión cardinal, o para darles un orden (primero, segundo, tercero, ..., centésimo, ..., milésimo noningentésimo nonagésimo nono, ...) en su función ordinal. El cero, la ausencia de cantidad, ha sido el último en incorporarse al conjunto que designaremos con la letra $\mathbb{N}$ y que será el principal protagonista del segundo capítulo. Aparte del orden natural del que está dotado, existe en $\mathbb{N}$ la relación de divisibilidad, que es un orden parcial. En el capítulo 2 se estudian las propiedades de la divisibilidad de los números naturales: números primos y números compuestos, algoritmo de Euclides, máximo común divisor y mínimo común múltiplo, criba de Eratóstenes, Teorema Fundamental de la Aritmética, teorema de Chebychev y teorema (postulado) de Bertrand.

La suma de dos números naturales es otro número natural, pero, en general, ese no es el caso respecto de su resta o diferencia. Dentro del conjunto $\mathbb{N}$ solo podemos restar de un número mayor, el minuendo, otro menor, el sustraendo. Sin embargo, existen numerosas situaciones en las que es importante poder restar de un número menor otro mayor. Por ejemplo: si gastamos más dinero del que poseemos, nos endeudamos, entramos en números rojos en nuestra cuenta corriente o en saldo negativo. Negativo es precisamente la palabra clave, y un paso importante de las matemáticas de la infancia consistió en ampliar el conjunto $\mathbb{N}$ de los naturales para conseguir

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

que es el conjunto de los enteros: positivos, negativos y cero.

La letra $\mathbb{Z}$ mayúscula es la notación usual para designar al conjunto de todos los enteros. Seguramente por influencia alemana, ya que *Zahl* significa número en alemán. En $\mathbb{Z}$ tenemos la libertad suficiente para poder restar siempre: $5 - 3 = 2$, $3 - 5 = -2$, $5 - (-3) = 8$. Sin embargo, la división es otra historia: para poder dividir de forma indiscriminada dos números

enteros hay que inventar el conjunto $\mathbb{Q}$ de los números racionales. Pero luego querremos más y desearemos poder extraer siempre raíces cuadradas o cúbicas, lo que nos llevará a estudiar el conjunto de los números reales, $\mathbb{R}$, y el de los complejos, $\mathbb{C}$.

En cada uno de estos pasos ganamos libertad y potencia de cálculo. Con los números reales aprendemos a trabajar con el infinito (sumar y multiplicar infinitos números) que es la esencia del cálculo diferencial y que nos transportará allende el horizonte matemático de la infancia. Pero eso es la historia de muchos siglos y a la que han contribuido hombres y mujeres de todas las épocas y culturas de la humanidad: babilonios, griegos, indios, árabes, europeos, americanos...

El tercer capítulo estará dedicado a la construcción de los números enteros y a la aritmética modular: clases residuales, pequeño teorema de Fermat, sistemas de congruencias y ecuaciones diofánticas. El capítulo cuarto versará sobre los números racionales y los desarrollos decimales: densidad y numerabilidad. El capítulo quinto contiene la construcción de los números reales: el continuo, aproximación por racionales y fracciones continuas, criterios de irracionalidad (los casos de e y π). El sexto lo constituye el estudio de los números complejos: raíces de la unidad, representación polar, la exponencial, el logaritmo y la fórmula de Euler.

La primera parte del libro se ocupa pues de los números que, junto con las figuras, aritmética y geometría, son los objetos de estudio fundamentales de las matemáticas y sobre los que posteriormente se construyen y conforman muchas otras teorías.

Empero, sería erróneo pensar que el mero cálculo con los números y saber operar con rapidez y precisión constituya el objetivo principal de la actividad matemática. Si interrogásemos a un grupo de investigadores acerca de su trabajo, probablemente obtendríamos respuestas muy diversas pero todos dirían que tratan de encontrar ideas nuevas para resolver problemas difíciles. Que las matemáticas persiguen la verdad y la belleza en la orfebrería de las ideas entrelazadas por cadenas precisas de razonamientos, y que las demostraciones matemáticas han originado tantas astucias ingeniosas de la razón que es difícil encontrarles parangón en otras actividades humanas. Si los poetas crean belleza con las palabras, y los pintores con la forma y el color, la materia prima de la belleza matemática son las ideas.

Mariposa de luz,
la belleza se va cuando yo llego
a su rosa.
Corro, ciego, tras ella...
la medio cojo aquí y allá...
¡Sólo queda en mi mano
la forma de su huida!

J. R. Jiménez

El capítulo séptimo está dedicado a las relaciones de orden: órdenes buenos, axioma de elección, lema de Zorn y los ordinales. El octavo es una recapitulación sobre el concepto de número natural y la teoría de conjuntos: los cardinales, las paradojas, el sistema axiomático de Zermelo-Fraenkel y el significado del teorema de Gödel. Finalmente, el capítulo noveno se ocupa de los polinomios: división de polinomios, Teorema Fundamental del Álgebra, números algebraicos, números trascendentes y la cuadratura del círculo.

En el origen de este libro estuvo la asignatura "Conjuntos y Números" del primer curso de las licenciaturas de Matemáticas e Informática que se enseña en la Universidad Autónoma de Madrid. Los alumnos que cursan la "doble titulación" suelen ser un conjunto notable, despierto y curioso, con un espléndido expediente de bachillerato, aunque a veces adolecen de lagunas aritméticas y lógicas que hubieran parecido muy extrañas en un estudiante de características similares de tiempos pasados. Con un contenido aritmético y lógico matemático se pretende en ese curso que los alumnos aprendan el arte de las demostraciones rigurosas y la redacción de textos matemáticos coherentes. Hay pues unos contenidos precisos, pero el libro no es un tratado de Teoría de los Números, ni mucho menos de Lógica Matemática, sino tan solo un paseo por algunos de sus, quizás, más bellos y asequibles jardines con el objetivo de ilustrar los modos de pensar, de demostrar, de escribir las matemáticas y, sobre todo, de estimular lecturas de otros textos más específicos y profundos. Está dirigido pues a un lector interesado y despierto, provisto de lápiz, papel y ánimo para hacer los ejercicios a modo de pruebas y pistas de la trama general, que sigue la senda de la construcción de los números, y la búsqueda de la piedra filosofal, en ese empeño de finales del XIX y principios del siglo XX que fue la construcción con cimientos sólidos del edificio matemático, reduciéndolo a la aritmética y a la teoría de conjuntos, y cuyos protagonistas fueron, entre otros, Frege, Cantor, Russell, Hilbert, von Neumann, Zermelo y Gödel. Algunas secciones tienen una cierta complejidad (la prueba de las estimaciones de Chebychev, la irracionalidad de $\zeta(3)$, las equivalencias entre el axioma de elección, el principio de buena ordenación y el lema de Zorn, o la trascendencia de e y de π), pero la mayoría pueden ser comprendidas sin más requisitos que las matemáticas del bachillerato.

En una primera lectura pueden evitarse perfectamente esos apartados más complicados y reservarlos para segundas o terceras visitas. Un ejemplo de esta situación se encuentra en el capítulo último, en el que se presenta con detalle algo tan básico como es el algoritmo de la división de los polinomios para seguir luego con el Teorema Fundamental del Álgebra y la trascendencia del número π que, naturalmente, son de otro calado.

Es un hecho que da que pensar el que estas teorías, que tuvieron su origen en algo tan alejado de las aplicaciones como eran los problemas de los fundamentos de las matemáticas, hayan resultado luego tan importantes para la creación y el desarrollo de los modernos computadores. Habida cuenta de los orígenes de este libro, no debe extrañar que de una manera recurrente se ponga el énfasis en la interfaz entre las matemáticas y la computación.

Me gustaría también haber sido capaz de transmitir la satisfacción que me ha producido enseñar estas materias a un grupo tan inquieto de alumnos que me han hecho recordar aquellos años sesenta en los que estudié el bachillerato en el Instituto Alfonso X "El sabio" de mi ciudad natal. A través de una de mis profesoras, que puso a mi disposición su espléndida biblioteca particular, descubrí a Bertrand Russell y sus escritos sobre los fundamentos de las matemáticas y tuve acceso al *Álgebra Moderna* de G. Birkhoff y S. Mac Lane, que había sido traducido por la editorial Vicens Vives, y a la edición de la editorial Eudeba de la *Topología General* de J. Kelley. También al *Análisis Matemático* de J. Rey Pastor, P. Pi Calleja y C. A. Trejo, cuyo magnífico primer capítulo es un ameno recorrido por la construcción de las distintas clases de números.

Este libro es un pequeño homenaje personal a aquellas lecturas de mi juventud con la pretensión, quizás desmesurada, de ser ese texto que me hubiese gustado leer entonces. También lo es para el grupo de amigos quinceañeros con los que compartí gustos literarios, musicales y deportivos, y que toleraban con buen humor mis pedantes peroratas en torno a las paradojas de la teoría de conjuntos, del teorema de incompletitud de Gödel y la divisibilidad infinita del continuo.

Han ocurrido tantas transformaciones desde los años cincuenta que ahora nos puede parecer increíble que en el Puente Tocinos, un pueblo de la huerta murciana cercano a la ciudad, el tendido de la compañía local de electricidad fuese entonces tan precario que el suministro se interrumpía sistemáticamente los días ventosos, cuando las copas de las cañas liseras de los costones de las acequias rozaban los cables. La caída de tensión vespertina era tan notoria que los motores eléctricos dejaban de funcionar en el taller de mi padre, haciendo necesario encender los diversos candiles, quinqués, petromares y carburadores que abundaban en todas las casas. En ese taller, en el

que pasé muchas horas felices de mi infancia, se hablaba con frecuencia de los desastres de la guerra pasada, pero también de los avances tecnológicos (los aviones, los sputniks, la energía atómica) de los que se compartía una visión muy positiva, otorgándoles el papel protagonista del progreso que mis mayores habían aprendido a asignarles en la escuela republicana. Es seguro que debo mi interés por la ciencia a haber escuchado de niño aquellas conversaciones en las que llegué después a participar.

Sostenía mi padre que nuestras penurias eléctricas podrían solucionarse estableciendo un sistema de saltos de agua en el río (algo que entonces no era tan descabellado sugerir como lo sería ahora, cuando el Segura se ha convertido en una cloaca casi estanca a su paso por la ciudad). Con los rudimentos de Física aprendidos en mis manuales de bachiller, objetaba yo que la energía total del agua del río era la que era y que, por más saltos que intercaláramos, nunca podríamos conseguir la necesaria para iluminar a toda la huerta. Pero mi padre creía que, aunque más débiles, siempre podríamos añadir más y más saltos pudiéndose hacer muy grande la suma de sus energías. Cuando ahora se me presenta la ocasión de explicar en clase las paradojas de Zenón de Elea, Aquiles y su tortuga y la divisibilidad infinita del continuo, la nostalgia me trae el eco de aquellas conversaciones.

Antes de que yo alcanzase la edad de escolarización mi madre, que era maestra de escuela, me llevaba consigo a sus clases, en las que me tocaba desempeñar el arriesgado papel de "hijo de la maestra" por diversos pueblos murcianos de nombre tan sonoro como "El Llano de Brujas", "Los Infiernos", "Ricote", "El Mirador", "La Era Alta", "Algezares", o "San Pedro del Pinatar". Aunque yo fuese capaz de memorizar los poemas que tanto le gustaban a mi madre, creo que enseguida comprendí que sus alumnas dominaban los sotanillos del idioma con mucha mayor gracia y habilidad de las que estaban a mi alcance. Empero, no sé cómo, descubrí que con las cuentas era distinto, y ahí tenía yo una oportunidad de hacerme valer ante aquellas niñas maravillosas. Eso me llevó a aprender Aritmética a una edad muy temprana y a comprobar que las Matemáticas pueden ser una buena base para la amistad y el galanteo. Pero también a comprobar que el lenguaje preciso no está reñido en absoluto con la búsqueda de la belleza en la expresión y que la Aritmética y la Geometría exigen una buena dosis de fantasía.

Años después, siendo ya profesor en la Universidad de Princeton, oí contar a un compañero del Departamento la historia de un alumno de doctorado que le había comunicado su intención de abandonar la tesis, para dedicarse a escribir novelas, a la ficción, y cómo él pensaba que había tomado una decisión correcta, por cuanto era evidente que ese alumno carecía de la imaginación necesaria para la creación matemática.

Banda de Möbius benedettina

Es obvio que ando escaso de dinero
y que nadie en el barrio me conoce.
Transparente resulto a las miradas,
de las bellas que pasan junto a mí.

Pero ven, deja que te muestre,
mira y verás:

Si cortamos una cinta bien larga
y pegamos sus bordes con cuidado,
surgirá un mundo de solo una cara
donde, alegres, vivir desorientados.

¿Qué hace a un teorema ser profundo e importante? ¿Qué dosis de verdad y de belleza en el engarce de las ideas convierten su demostración en ese glorioso e incorruptible hito del pensamiento?

¿Qué es lo que hace a un poema ser completo? ¿Que no podamos sustraer ni añadir una palabra sin destrozarlo, y que no se reduzca a unos pocos versos brillantes junto a otros anodinos?

El aire se serena
y viste de hermosura y luz no usada
Salinas, cuando suena
la música extremada
por vuestra sabia mano gobernada.

Fray Luis de León

Enhiesto surtidor de sombra y sueño
que acongojas al cielo con tu lanza.
Chorro que a las estrellas casi alcanza
devanado a sí mismo en loco empeño.

Gerardo Diego

To see a world in a grain of sand
and a heaven in a wild flower,
hold infinity in the palm of your hand
and eternity in an hour.

William Blake

Nadie rebaje a lágrima o reproche
esta declaración de la maestría
de Dios, que con magnífica ironía
me dio a la vez los libros y la noche.

Jorge L. Borges

Juntar la poesía con las matemáticas puede parecer un oxímoron a la mayoría de los ciudadanos, que asocian estas últimas no con la búsqueda de algún tipo de belleza, sino más bien con una especie de tortura mental sufrida durante los años de aprendizaje escolar. Sin embargo, desde Galileo sabemos que las matemáticas son el lenguaje en el que se expresa la naturaleza, y que la descripción del universo requiere de ellas y de su capacidad para crear las definiciones, las metáforas precisas, y las reglas del razonamiento con las que engarzar las ideas que nos llevan a demostrar la verdad. Es cierto que los poemas no se hacen solo con ideas, sino con palabras, y que únicamente con

metáforas es difícil llegar a nada en la ciencia. Pero toda demostración de un hecho matemático profundo, que haya necesitado de nuevas e ingeniosas astucias de la razón, exigirá un lenguaje preciso y bello y la adquisición de alguna forma de nombrar los conceptos creados. En poesía el lenguaje suele estar dominado por un sentimiento musical inconsciente: rimas, explícitas u ocultas, y ritmos sostenidos, sin necesidad alguna de justificación, como música de las esferas, de las impresiones y de los sentimientos personales.

La lengua hablada es un instrumento práctico cuya finalidad es la comprensión. Si nos detenemos a seguir en el diccionario de la RAE la estela de una definición, lo más probable es que enseguida lleguemos a un círculo vicioso, algo que resultaría sumamente odioso e intolerable en cualquier teoría matemática. No obstante, ha habido siempre matemáticos con un cierto "estro poético" y, recíprocamente, encontramos también a muchos poetas que han sido fascinados por las matemáticas. Un ejemplo notable es Omar Jayyam, astrónomo, asesor político y, sobre todo, poeta y matemático cuya vida, que transcurrió en Persia entre los siglos XI y XII, ha sido novelada por Amin Maalouf en su excelente libro *Samarkanda*. Jayyam se interesó por la ecuación cúbica a la que supo resolver por métodos geométricos. En poesía nos han llegado sus *Rubaiyat*, que es una colección de deliciosas cuartetas, tales como:

Un jardín, una cimbreante doncella,
un cántaro de vino, mi deseo y mi amargura.
He aquí mi paraíso y mi infierno.
Pero ¿quién ha recorrido el cielo y el infierno?

Un poco de pan, un poco de agua fresca
la sombra de un árbol y tus ojos.
Ningún sultán más feliz que yo.
Ningún mendigo más triste.

El mundo inabarcable: un grano de polvo en el vacío.
Toda la ciencia del hombre: palabras.
Los pueblos, las bestias y las flores de los siete climas: sombras.
El fruto de tu constante meditación: la nada.

En cada teorema existe la voluntad implícita de expresar un hecho matemático relevante con un mínimo de hipótesis, necesarias y suficientes a ser posible, en unos términos diáfanos, sin adjetivos innecesarios, pero con la adecuada riqueza de argumentos indirectos y construcciones delicadas como tan bien expresan los versos de Robert Browning, que hemos traducido con cierta libertad:

Oh, the little more,
and how much it is!
And the little less,
and how many worlds away!

¡Oh, el poquito más,
y cuánto más es!
¡Y el poquito menos,
y cuantos mundos
se nos van con él!

Pensemos en el soneto que exige la presentación de un asunto y el desarrollo de una idea acabando, a ser posible, con un pensamiento brillante; dentro de catorce versos endecasílabos rimados en consonante y con acento en la sexta sílaba, si es que lo queremos de arte mayor. Estructurado en forma de dos cuartetos acompasados de igual rima, seguidos de dos tercetos entrelazados, con o sin estrambote.

Un soneto me manda hacer Violante:
en mi vida me he visto en tal aprieto;
catorce versos dicen que es soneto;
burla burlando van los tres delante.

Yo pensé que no hallara consonante,
y estoy a la mitad de otro cuarteto;
como me vea en el primer terceto,
no hay cosa en los cuartetos que me espante.

Por el primer terceto voy entrando,
y parece que entré con pie derecho,
pues fin con este verso le voy dando.

Ya estoy en el segundo, y aún sospecho
que voy los trece versos acabando.
Contad si son catorce, y está hecho.

Lope de Vega

Posiblemente sea la poesía el género literario que mejor se ajusta al estilo de las Matemáticas. Entre los grandes poetas encontramos versos inspirados en ellas, que son testimonio fehaciente de cómo sus autores se dejaron seducir por su belleza. He aquí algunos ejemplos:

A ti, maravillosa disciplina,
media, extrema razón de la hermosura
que claramente acata la clausura
viva en la malla de tu ley divina.
A ti cárcel feliz de la retina,
áurea sección, celeste cuadratura,
misteriosa fontana de mesura
que el universo armónico origina.

Rafael Alberti
(La divina proporción)

Digno de admiración es el número Pi
tres coma catorce
todas sus siguientes cifras son también iniciales,
quince, noventa y dos porque nunca termina.
No se deja abarcar sesenta y cinco
treinta y cinco con la mirada,

Wislawa Szymborska
(El número Pi)

¡Sí, todo con exceso:
la luz, la vida y el mar!
Plural todo, plural,
luces, vidas y mares.
A subir, a ascender
de docenas a cientos,
de cientos a millar,
en una jubilosa
repetición sin fin,
de tu amor, unidad.
Tablas, plumas y máquinas,
todo a multiplicar,
caricia por caricia,
abrazo por volcán.
Hay que cansar los números.
Que cuenten sin parar,
que se embriaguen contando,
y que no sepan ya
cuál de ellos será el último:
¡qué vivir sin final!

Pedro Salinas
(La voz a ti debida)

¡Qué sed
de saber cuánto!
¡Qué hambre
de saber
cuántas
estrellas tiene el cielo!

Nos pasamos
la infancia
contando piedras, plantas,
dedos, arenas, dientes,
la juventud contando
pétalos, cabelleras.
Contamos
los colores, los años,
las vidas y los besos,
en el campo
los bueyes, en el mar
las olas. Los navíos
se hicieron cifras que se fecundaban.

Pablo Neruda
(Oda a los Números)

¿Cómo será que pueda
libre de esta prisión volar al cielo,
Felipe, y en la rueda
que huye más al suelo,
contemplar la verdad pura sin velo?

Por qué tiembla la tierra,
por qué los hondos mares se embravecen
do sale a mover guerra
el cierzo, y por qué crecen
las aguas del océano y descrecen.

De do manan las fuentes:
quién ceba y quién bastece de los ríos
las perpetuas corrientes;
de los helados fríos
veré las causas y de los estíos.

Las soberanas aguas
del aire en la región quién las sostiene:
de los rayos las fraguas;
do los tesoros tiene
de nieve Dios, y el trueno donde viene.

Quién rige las estrellas
veré, y quién las enciende con hermosas
y eficaces centellas;
por qué están las dos osas
de bañarse en el mar siempre medrosas.

Veré este fuego eterno,
fuente de vida y luz, do se mantiene;
y por qué en el invierno
tan perezoso viene.
Por qué en las noches largas se detiene.

Fray Luis de León
(Oda a Felipe Ruiz)

Son más que notables los versos de estos poetas, describiendo los de Fray Luis todo un programa de investigación científica. Aunque podríamos objetar que no están, quizás, entre los más logrados de sus autores; que la razón áurea no es, después de todo, algo tan importante en matemáticas o que el poema sobre π es un poco tramposo en alguno de sus versos, porque aún no sabemos de la normalidad del desarrollo decimal aludido. ¡*Vanitas, vanitatis et omnia vanitas*! La relación entre la poesía y las matemáticas no puede ser reducida a una mera antología de poemas con contenido matemático, por muy inspirados que estos nos parezcan.

Podemos llevar también la analogía al terreno de las relaciones y comportamientos que se estilan entre poetas y matemáticos. Tratándose de artistas que buscan la belleza a través de las palabras, las metáforas y la creación de lenguaje, cabría esperar entre los poetas un trato exquisito, elegante y cortés. Nada más alejado de la realidad: son de sobra conocidos los insultos mutuos entre Quevedo, Lope y Góngora, las opiniones nada piadosas que J. R. Jiménez tenía de los poetas de su tiempo o las todavía recientes de J. A. Valente. No parece que el club de los poetas sea especialmente indulgente consigo mismo. Entre los matemáticos, gente especializada en la pulcritud del razonamiento, en la búsqueda de la verdad y de la belleza de las ideas, que forman una élite planetaria un tanto ácrata y alejada de las convenciones sociales, con una historia rica en episodios interesantes y mentes generosas y bellas, han habido también personajes vanidosos y mendaces, y se han dado los comportamientos más mezquinos, propios de un colectivo que, como ocurre con los poetas, es el principal, si no el único, observador y lector de sí mismo. No obstante, siempre resulta conveniente recordar con Gimferrer que hasta la poesía tiene sus reglas y las matemáticas sus licencias.

Quod erat demostrandum

Las demostraciones matemáticas constituyen una de las más altas cimas del pensamiento humano. Hasta mediados del siglo pasado era común sostener que una prueba rigurosa consiste en una cadena de razonamientos engarzados, pero de manera tal que los eslabones puedan ser todos comprobados por cualquier persona que tenga el tiempo y el entrenamiento adecuados. Los *Elementos de Euclides contienen numerosos ejemplos a los que, como dijo Hardy, el paso del tiempo no ha podido añadir una sola arruga a la lozanía de su belleza y precisión. Pero la noción de demostración no ha permanecido estática a lo largo de los tiempos, sino que se han ido creando nuevas y más poderosas estrategias, introduciendo conceptos nuevos y herramientas idóneas que nos dotan de una mayor libertad y potencia de razonamiento. La crisis del pensamiento griego a la que antes aludíamos, producida por el descubrimiento pitagórico de que la longitud de la diagonal del cuadrado unidad no es un número racional, está recogida en los Elementos en forma*

de demostración: si suponemos que x, la raíz cuadrada de 2, fuese igual a la fracción irreducible a/b tendríamos la igualdad $2b^2 = a^2$, de la que deducimos la paridad del número $a = 2c$ y, por tanto, la igualdad $2c^2 = b^2$ que, a su vez, exige la paridad de b y esto contradice que a y b sean primos entre sí. El principio del tercero excluido no nos deja otra salida que concluir la irracionalidad de la raíz cuadrada de dos. Se trata de un razonamiento breve, sencillo, elegante e ingenioso: ¡mejor imposible!

Siguiendo el rastro de esta historia llegamos a finales del siglo XIX *cuando Cantor observó que los números racionales son biyectables con los naturales (son numerables o pueden ponerse en fila de uno en uno, estricta formación), pero que eso no es posible hacerlo con todos los números reales, racionales e irracionales. Una consecuencia inmediata es que los racionales son un conjunto pequeño, de medida nula entre los reales: si con los ojos bien cerrados escogemos un número al azar, lo más probable es que sea irracional; pero si lo hacemos con poca precaución será un gran enigma saber si lo es o no.*

Según A. Turing un número es computable si podemos escribir un algoritmo, o programa de ordenador, que calcule cualquiera de sus cifras decimales: los racionales son computables, pero también lo son el número π y la raíz cuadrada de 2. Ahora bien, como los programas son textos finitos escritos con un número finito de símbolos (los caracteres de un idioma: español, inglés, java, fortran, lisp, etc.), una consecuencia de la teoría de Cantor es que el conjunto de los programas, y por tanto el de los números computables, es numerable. Por la misma razón son numerables los números definibles, o nombrables, que son aquellos que podemos identificar con un texto finito. Hay definibles que no son computables, pero aquellos forman también un conjunto de medida cero: eligiendo un número al azar tenemos una probabilidad muy alta (de hecho igual a 1) de que no sea definible. Pero nadie puede señalar a uno de ellos, porque señalarlo, nombrarlo o identificarlo lo impide su propia naturaleza.

Las ideas de Turing tienen otras muchas consecuencias interesantes, pero señalemos ahora tan solo la sutileza del argumento: prueba la existencia de los números que no son definibles observando que la probabilidad de encontrarlos en la recta real es estrictamente positiva y, al mismo tiempo, demuestra rigurosamente que nunca podremos identificar allí a uno concreto de ellos.

Los matemáticos tendemos a creer en el principio de la razón suficiente formulado por Leibniz y pretendemos encontrar demostraciones de todo. No nos basta con entender muchos ejemplos y no quedamos satisfechos hasta obtener la prueba del caso general. Algunas demostraciones involucran largas cadenas de razonamientos de manera indirecta y complicada. Un ejemplo es

el teorema de Carleson sobre la convergencia en casi todo punto de las series de Fourier de las funciones de cuadrado integrable; otro es la prueba de A. Wiles del último teorema de Fermat. También tenemos el anuncio reciente hecho por Perelmann de la verificación de la conjetura de Poincaré, que está todavía en periodo de análisis y comprobación por los topólogos.[*] *Los dos primeros, y el tercero si recibe el "nihil obstat", son casos de demostraciones que cumplen todos los requisitos del rigor, que exhiben grandes dosis de ingenio y son elegantes y bellas a su manera, pero que son muy complejas. Tanto, que dudo de la existencia de un solo matemático que pueda verificar con detalle, por sí mismo, esas tres pruebas en un plazo prudente de tiempo. Por el contrario, las dos últimas, que son también las más recientes, han necesitado del trabajo conjunto de grupos de expertos para obtener el certificado de garantía (lo que se considera ya realizado en el caso del Fermat, pero que está todavía en marcha en el de Poincaré). Un tratamiento aparte merece el "teorema de clasificación de los grupos finitos simples" cuya demostración se ha plasmado en más de 10.000 páginas, en cientos de artículos escritos por cientos de matemáticos. No es este prólogo el lugar adecuado para glosar esos resultados, pero digamos que son importantes y fundamentales, por lo que darán lugar a muchos otros teoremas que estarán basados en ellos. Teniendo en cuenta que la probabilidad de que un error se deslice en un texto matemático extenso no es del todo despreciable, estos ejemplos sugieren varias preguntas acerca de qué es una prueba; o por qué algunas tan complejas son realmente necesarias y cuál es su verdadero interés y fiabilidad. Sobre todo al hilo de la siguiente vuelta de tuerca que ha dado este asunto con la aparición de las demostraciones basadas en, o ayudadas por, el computador; como es el caso de la prueba del teorema de los cuatro colores, obtenida por Appel y Haken en 1976, y la solución de la conjetura de Kepler que se debe a Hales y que acaba de aparecer publicada en Annals of Mathematics (noviembre de 2005), aunque data de 1998.*

Su notoriedad está justificada por el tiempo transcurrido entre la formulación del problema y su solución (ciento cincuenta años tiene el primero y unos cuatro siglos el segundo), por tener enunciados asequibles a la mayoría de los ciudadanos, por la cantidad y calidad de los matemáticos que intentaron su demostración y, finalmente, porque esta ha necesitado, en ambos teoremas, de cálculos masivos que, uno por uno, verifican una cantidad enorme de casos cuya comprobación directa está varios órdenes de magnitud por encima de las posibilidades humanas. ¿Cuántos colores son necesarios y suficientes para colorear cualquier mapa del plano de manera que regiones conexas adyacentes tengan distinto color? ¿Cuál es la manera más eficiente de empaquetar esferas del mismo tamaño? La aparente sencillez de estas preguntas explican tanto su popularidad como el gancho que han tenido entre varias

[*] En el ICM de 2006, celebrado en Madrid, se otorgó a G. Perelmann la Medalla Field por su demostración de la conjetura de Poincaré.

generaciones de matemáticos, no siendo una sorpresa que hayan trascendido a la opinión pública las vicisitudes de sus soluciones que exhiben una desproporción manifiesta entre la tarea desarrollada con los métodos tradicionales de las matemáticas y la parte reservada al computador, por lo que hemos de hablar de demostraciones basadas en, más que ayudadas por, el computador. Aparte de su valor intrínseco, estos episodios han servido para estimular una interesante polémica en la que, desde un principio, se han manifestado diversidad de opiniones: hay quien cree que no son verdaderas demostraciones porque involucran muchos pasos que no pueden ser verificados directamente por el cerebro humano, ya que su validez reside en algo tan elusivo como es la corrección del programa informático y la eficiencia de las máquinas que lo desarrollan. Por el contrario, hay quien opina que no son menos válidas que otros tipos de pruebas y que no hay más razones para dudar de la capacidad de los computadores para hacer correctamente cálculos enormes, que de la eficiencia de la mente humana para engarzar cadenas largas de razonamientos sin equivocarse. Naturalmente han surgido programas que comprueban la validez de otros programas y, a su vez, la posibilidad de crear programas que garanticen a estos, y así sucesivamente. ¿Cuál es la probabilidad de que un computador cometa un error inesperado? ¿Cuántas pruebas en distintos ordenadores debemos hacer para dar por válida una demostración? Son todas ellas preguntas naturales que surgen al hilo de estos resultados y a las que podemos añadir también otras más tradicionales y platónicas, a las que los ordenadores han añadido nuevos matices: ¿las matemáticas se crean o se descubren? ¿Son una ciencia de observación, como la astronomía, o la irrupción de los computadores las convertirá en experimentales? ¿Qué es una demostración? ¿Hay maneras objetivas de estimar la belleza y la profundidad de un razonamiento?

Una realidad que nos resulta ahora muy evidente es el cambio experimentado por las aplicaciones de las matemáticas al resto de las ciencias, y a nuestra vida cotidiana, que han propiciado los computadores. También han aparecido áreas nuevas de actividad con el adjetivo de computacional (álgebra computacional, geometría computacional), o se han desarrollado teorías de análisis numérico en direcciones que adquieren su sentido por la existencia de potentes ordenadores. Un ejemplo interesante lo encontramos en la teoría de los números o aritmética superior, que hasta ayer mismo estaba considerada como la quintaesencia de la matemática pura, cuyos teoremas profundos y bellos carecían de aplicaciones prácticas. Resulta que los números primos, cuya sucesión ha fascinado a los matemáticos desde los griegos de hace más de veintiséis siglos, se encuentran ahora en el centro de muchas aplicaciones por cuanto en sus propiedades está basada la seguridad de las comunicaciones en Internet. Disponer de primos muy grandes, de más de cien cifras, es fundamental para la seguridad, mientras que encontrar algoritmos rápidos de factorización es tarea de quienes desean espiar nuestras comunicaciones,

y resulta que cualquiera de estos empeños sería inviable sin la ayuda del computador. Afortunadamente para la seguridad, resulta asequible a nuestros ordenadores encontrar primos de cientos de cifras, o al menos que lo sean con una probabilidad grande, pero se trata todavía de una misión imposible para ellos descomponer, en un tiempo razonable, un número que sea producto de dos de esos primos y sobre cuyos factores no tengamos información alguna. De manera que una antigua rama de las matemáticas se ha visto revitalizada y cambiado la índole de sus problemas en contacto con las nuevas posibilidades de computación.

Existen ya en el mercado varios paquetes de programas que llevan a cabo manipulaciones simbólicas en Álgebra y en Cálculo Diferencial. No obstante, me parece que todavía carecemos de "genuinos matemáticos artificiales" que puedan manejar el amplio espectro de razonamientos rigurosos que dominan los expertos de cada área. Y posiblemente nunca los tengamos, porque una cosa son las demostraciones formales y otra muy distinta son las obtenidas, en asociaciones e inspiraciones insospechadas, con el rico y variable arsenal de argumentos rigurosos que la mente humana ha creado y seguirá creando. Aunque no me cabe la menor duda de que el ordenador, con su enorme capacidad combinatoria, abastecido del conjunto de proposiciones conocidas y de las reglas formales de derivación de teoremas, será cada vez más capaz de contribuir, no solo con resultados rutinarios o esperados, sino incluso aportando combinaciones nuevas que no hayan sido previstas por los humanos. Sin embargo, el progreso en esa dirección es más arduo de lo que se pensaba hasta hace poco, habiéndose experimentado un cierto retroceso cuando se encontró un error en la demostración de la conjetura de Robbins (¿son booleanas las álgebras de Robbins?) que pareció haber llevado a cabo un programa de ordenador, pero en el que posteriormente se detectó un error que obligó a retirar el anuncio de la prueba. De haberse esta confirmado habríase tratado del primer teorema demostrado por un computador que no habían sabido probar antes los artistas del área con los medios tradicionales. Pero la frustración que supuso el hallazgo de un error en el programa fue un jarro de agua fría para quienes pretenden con ahínco desarrollar la llamada "inteligencia artificial fuerte".

No obstante el extraordinario crecimiento de la informática durante la segunda mitad del pasado siglo, que ha sido desde sus comienzos estimulado por las matemáticas pero a las que luego ha servido de maneras diversas, sugiere muchas preguntas: ¿Podrán en el futuro los ordenadores hacer conjeturas interesantes y probar teoremas? ¿Somos los matemáticos una especie en extinción? ¿Estarán las matemáticas del mañana plagadas de demostraciones que dependan de cálculos que solo pueden hacer las computadoras? ¿Tendremos textos llenos de enunciados que afirmen que bajo tales hipótesis, que sabemos ciertas con una probabilidad mayor que 0,9*, podemos demostrar que otra proposición es cierta con un error experimental del* 1 %*?*

¿Convertirán las computadoras en ciencia experimental a las matemáticas? ¿Podremos abordar rigurosamente los modelos más complejos de la ciencia? ¿Servirán los programas de demostración para liberarnos de las tareas más rutinarias y poder concentrarnos en los pasos realmente difíciles y creativos, inasequibles a los ordenadores? ¿Aceptar la ayuda del ordenador es el típico pacto con el diablo, con el que ganamos un inmenso poder pero perdemos la noción de verdad? Habida cuenta de la enorme capacidad de la especie humana para encontrar incentivos económicos y motivos de querella, hay ya también quien se ha preguntado si llegará el día en el que un tribunal de justicia tendrá que decidir sobre la validez y corrección de una prueba matemática.

Si parafraseando el famoso discurso de J. F. Kennedy cambiamos el sentido de la pregunta y nos interrogamos ahora sobre qué han hecho los matemáticos por los computadores, la respuesta es mucho más sencilla: casi todo. Un hito es el trabajo de A. Turing del año 1936 que hemos mencionado antes y en el que se aborda el significado del término "computable". Con ese fin Turing describe un ordenador virtual, o máquina de Turing, que es el primer diseño teórico de lo que ahora entendemos por un computador. Luego J. von Neumann colaboró decisivamente en el proyecto ENIAC con objeto de construir efectivamente una tal máquina, ante el escepticismo de sus colegas físicos y matemáticos del Institute for Advanced Study, según he oído contar muchas veces durante mis estancias en aquel lugar. Ambos, Turing y Von Neumann, participaban en el programa formalista de Hilbert, que era el intento más serio de "salvar los muebles" después del demoledor impacto que la aparición de las antinomias o paradojas había tenido en los planes de Frege y Cantor, entre otros, de fundamentar rigurosamente las matemáticas en la teoría de los conjuntos.

Según Hilbert, en un lenguaje formal tenemos un alfabeto, unos signos ortográficos (paréntesis, punto, coma, espacio en blanco, etc.), unos conectivos lógicos ("y", "o", "negación", "implicación", "igual") y unos cuantificadores (existe, para todo). Con ellos se pueden escribir fórmulas siguiendo unas reglas estrictas de construcción. Algunas de estas fórmulas bien hechas son elegidas como los axiomas de la teoría, a la que también hay que dotar de unas reglas de inferencia que permitan obtener unas fórmulas de otras. Una demostración "formal" es una sucesión finita de tales fórmulas de manera que cada una de ellas ora es un axioma, ya se deduce de las anteriores aplicando las reglas de inferencia. La última obtenida es el teorema cuya demostración consiste exactamente en esa misma sucesión de fórmulas. Observemos lo revolucionario que este punto de vista resultaba en sus comienzos y, sin embargo, lo natural que ahora nos parece por su semejanza con los mecanismos de los lenguajes de programación con los que estamos tan familiarizados.

Siguiendo el plan de Hilbert se introdujo el sistema de axiomas de Zermelo-Fraenkel como la base sólida sobre la que construir la teoría de conjuntos, y luego el resto de las matemáticas, evitando las antinomias de Russell y Cantor. Pero: ¿Es consistente o está exento de contradicciones? ¿Es completo en el sentido de que siempre sea demostrable una proposición o su contraria? Kurt Gödel encontró la respuesta a estas naturales preguntas con su famoso "teorema de incompletitud" que, "lasciate ogni speranza", resultó ser demoledora para el proyecto formalista: cualquier teoría axiomática, lo suficientemente rica para que podamos desarrollar la Aritmética dentro de ella, contendrá siempre proposiciones indecidibles.

Una cuestión fundamental que plantean las máquinas de Turing es el llamado problema de la parada. Dado un programa bien construido, aceptado por el compilador, puede ocurrir que transcurrido un cierto tiempo la máquina se detenga y nosotros obtengamos la respuesta que deseábamos. Pero puede también suceder lo contrario y que la máquina prosiga ad infinitum. De hecho no es nada difícil imaginar programas aritméticos en los que se den cada una de estas dos opciones. El problema de la parada consiste en diseñar un algoritmo que decida a priori, en tiempo finito, si los programas van o no van a detenerse. Turing demostró rigurosamente que no puede existir ese algoritmo y que ello es equivalente al teorema de incompletitud de Gödel. Los trabajos de Gödel y de Turing constituyen una magnífica etapa de la Lógica Matemática del pasado siglo a la que estas líneas no pueden, ni mucho menos, hacer justicia. Pero sí podemos constatar, una vez más, la influencia decisiva que sus teorías tuvieron en el nacimiento y evolución de los lenguajes de programación y en el diseño de los primeros ordenadores.

Las demostraciones "formales" de Hilbert son pues muy distintas de las que normalmente se publican en las revistas de matemáticas (salvo quizás las especializadas en Lógica). Estas suelen ser pruebas rigurosas basadas en implicaciones comprobadas, resultados previos y asociaciones de ideas que los expertos del área conocen y manejan con precisión. Convertirlas en pruebas formales sería un proceso largo y tedioso que, excepto en casos muy simples, nunca se ha llevado a cabo. Pero me parece que las diferencias que hay entre ambas son un punto importante a la hora de comprender lo que puede realizar un matemático, lo que hace un computador y qué posibilidades nuevas tiene el centauro matemático+computador, al menos cuando restringimos su horizonte a la demostración de nuevos teoremas. Los programas para jugar al ajedrez han establecido claramente que el ordenador será cada vez más poderoso, y superior a la mente humana, en lo que atañe a las demostraciones formales y el manejo de la combinatoria de conjuntos enormes de posibilidades. Pero, pensemos en el episodio de la bañera de Arquímedes, en la famosa manzana de Newton o en la inspiración que llevó a H. Lebesgue a crear su integral, observando la manera como los albañiles

disponían horizontalmente los ladrillos para formar un muro y, con toda la modestia que el caso requiere, permítaseme añadir cómo la visión del baile de los dragones, en la fiesta del año nuevo de 1973 en Chinatown (Chicago), me ayudó a lograr la demostración del ahora llamado teorema maximal de Kakeya, o cuando, en otra ocasión distinta, la contemplación de un cuadro de Malevich me sugirió ideas para entender el intrincado solapamiento de los paralelepípedos en el espacio. Eso, creo yo, son ejemplos de iluminaciones fecundas que los ordenadores no pueden experimentar.

Los nombres del infinito

Los nombres de muchas áreas matemáticas, tales como Ecuaciones en Derivadas Parciales, Álgebra Homológica o Procesos Estocásticos, parecen esotéricos arcanos para el común de los ciudadanos. Hay algunos, no obstante, que son especialmente bellos. Un ejemplo es el del Análisis Armónico, que trata de las series trigonométricas, y que fue uno de los motores del estudio de los conjuntos infinitos de puntos del espacio y del desarrollo de la teoría de funciones.

Verde, verde esmeralda,
azul turquesa, azul ultramar,
índigo, violeta:
síntesis de luz.
Ondas, vibraciones, trigonometría.
Espirales, remolinos, puntos de fuga.
Venus de proporciones divinas.
Fuego que da la vida,
el calor y el color.
Amarillo, naranja,
rojo, carmín.

Poder calcular eficientemente longitudes, áreas y volúmenes, ha sido un objetivo de la humanidad desde tiempos remotos. El gran Arquímedes fue, quizás, el primero en saber que el volumen de una esfera y su radio están relacionados por la fórmula que ahora conocemos: $V = \frac{4}{3}\pi R^3$. *En su obra se encuentran métodos ingeniosos para cuadrar el segmento de parábola, estimar las cifras decimales de* π *y calcular el área y el volumen de conos, cilindros y esferas.*

¿Qué es la pendiente de una montaña? ¿Tiene velocidad el agua de un torrente? ¿Puede medirse la superficie de una coliflor? ¿Cuál es la región plana de área menor dentro de la que es posible darle la vuelta a una aguja? ¿Acaso poseen dirección los vientos? A pesar de su apariencia sencilla, incluso ingenua, estas y parecidas preguntas han estimulado en el pasado, y

lo continúan aún haciendo, el desarrollo de profundas y bellas teorías. Aparte del ya citado Arquímedes, las obras de Newton, Leibniz, Euler, Lagrange, Fourier, Dirichlet, Riemann, Cantor, Lebesgue, Sobolev y Zygmund, entre otras figuras históricas, nos enseñan a precisar los conceptos, el lenguaje y los resultados necesarios para darles respuesta.

Puede decirse que hacia comienzos del siglo XIX *la mayoría de los matemáticos creía que una función continua tenía que ser diferenciable excepto, quizás, en unos pocos puntos, y que toda superficie habría de tener un plano tangente. Que todo esto resultara ser falso produjo un gran interés, pero también sorpresa, e incluso aprensión, entre los expertos de finales de ese siglo, como atestiguan los comentarios de Hermite: "Esa plaga odiosa de funciones continuas que carecen de derivadas en todos los puntos". Y de Poincaré: "Hemos visto una multitud de ejemplos cuyo único propósito es parecerse lo menos posible a funciones decentes y útiles".*

El Análisis Armónico logró entender muchas de estas cuestiones, pero el origen de las series trigonométricas se remonta al Almagesto de Claudio Ptolomeo, siglo II, *y al problema de la cuerda vibrante, analizado por Daniel Bernoulli y Leonhard Euler en el siglo* XVIII. *Luego vinieron Fourier (que había participado en las campañas de Napoleón en Egipto) y Dirichlet quienes ensancharon el concepto de función más allá de las expresiones analíticas de Euler y Lagrange. Un hito es la tesis de B. Riemann, Sobre la representación de una función por medio de una serie trigonométrica, que llevó a generalizar las nociones de derivada y de integral. Luego llegaron Lebesgue, Sobolev y tantos otros que continuaron la obra de Riemann, configurando ese monumento intelectual que es el Cálculo del siglo* XX. *Pero también Cantor, quien profundizó en el estudio de la unicidad de los desarrollos trigonométricos, dando lugar a la teoría de conjuntos y de los cardinales transfinitos. Y de allí a los problemas de los fundamentos de las matemáticas que están en el origen de esa maravilla del espíritu que es el teorema de Gödel, con sus implicaciones filosóficas y sus consecuencias para la teoría de la computación.*

Las obras que citamos a continuación son de consulta recomendada para quien desee conocer la historia de las series trigonométricas, mereciendo una mención especial Trigonometric Series de Antoni Zygmund, que ha ejercido una influencia fundamental y ayudado a crear toda una escuela sin la cual es imposible entender el desarrollo del Análisis Armónico contemporáneo. Personalmente debo a Zygmund, mi bisabuelo en matemáticas y a quien traté de cerca durante mis años en Chicago, muchas anécdotas sobre los artistas del siglo pasado y sus logros, pero siempre desde su visión particular que colocaba a las series trigonométricas en el centro del universo matemático.

(1) J. Fourier (1822), Theorie analytique de la chaleur.

(2) B. Riemann (1854), Über die Darstellbarkeit einer Funktion durch eine trigonometrische Reihe.

(3) *H. Lebesgue (1904), Leçons sur l'integration et la recherche des fonctions primitives.*

(4) *A. Zygmund (1959), Trigonometric Series.*

(5) *E. Stein (1993), Harmonic analysis: Real variable methods, orthogonality and oscillatory integrals.*

Según Fourier, toda función periódica "arbitraria" (de periodo 1) puede ser escrita por medio de una serie trigonométrica:

$$f(x) = \frac{1}{2}a_0 + \sum_{n\geq 1} \left\{a_n \cos(2\pi nx) + b_n \operatorname{sen}(2\pi nx)\right\}$$

en la que los coeficientes vienen dados por la siguiente fórmula integral:

$$a_n = 2\int_0^1 f(x)\cos(2\pi nx)\,\mathrm{d}x\,, \qquad b_n = 2\int_0^1 f(x)\operatorname{sen}(2\pi nx)\,\mathrm{d}x.$$

Fourier, quien es descrito por sus biógrafos como un gran friolero, llegó a la conclusión anterior en su trabajo de modelización de la propagación del calor. Aunque recibió el premio de la Academia Francesa de Ciencias, los académicos, sin embargo, no se creyeron del todo su hipótesis sobre los desarrollos trigonométricos. De manera que tuvo que esperar bastantes años para publicar su monografía, lo que hizo al ser elegido académico. Pero no se trataba de una oposición banal ya que su teoría requería profundizar en los conceptos de función, derivada e integral. El Análisis Matemático del siglo XX *debe mucho al empeño de Fourier y a su perseverancia en la defensa de aquel proyecto.*

En su afamada tesis de habilitación, B. Riemann consideró series trigonométricas generales cuyos coeficientes son números arbitrarios. Es decir, sin que vengan necesariamente dados por una función integrable a través de las fórmulas de Fourier. El problema sutil que Riemann propuso es el siguiente: dada la serie $\frac{1}{2}a_0 + \sum_{n\geq 1}\{a_n\cos(2\pi nx) + b_n\operatorname{sen}(2\pi nx)\}$*, supongamos que en todo punto* $x \in [0,1]$ *se tiene la identidad:*

$$0 = \lim_{N\to\infty} S_N(x) = \lim_{N\to\infty}\Big[\frac{1}{2}a_0 + \sum_{1}^{N}\left\{a_n\cos(2\pi nx) + b_n\operatorname{sen}(2\pi nx)\right\}\Big]$$

¿Son necesariamente nulos todos los coeficientes: $a_n = b_n = 0\,, \forall n$*?*

La respuesta obtenida por Riemann es afirmativa. Pero la demostración es muy ingeniosa y abrió nuevos caminos al Análisis Matemático. Observemos que si supiésemos de antemano que se trata de la serie de Fourier de una función integrable, entonces la solución es mucho más fácil. Lo que convierte a la pregunta de Riemann en algo delicado es el hincapié en que estemos

ante una serie trigonométrica general, sin que dispongamos de ninguna información sobre sus coeficientes. A continuación vamos a describir, a grandes rasgos, la arquitectura de la demostración, dejando al lector la tarea de completar los argumentos que, por otro lado, pueden ser encontrados en las referencias (2) y (4).

Paso 1º: Riemann demuestra que la convergencia de la serie en todo punto implica que

$$\lim_{n\to\infty} \{|a_n| + |b_n|\} = 0.$$

Paso 2º: Consiste en una doble integración. Es decir, consideramos la función

$$F(x) = \frac{1}{4}a_0x^2 - \sum_{n\geq 1} \frac{1}{4\pi^2n^2}\{a_n\cos(2\pi nx) + b_n\,\mathrm{sen}(2\pi nx)\}$$

obtenida integrando formalmente dos veces, término a término, la serie trigonométrica original, para observar que F es una función continua, por ser la serie del segundo miembro uniformemente convergente.

Paso 3º: Generaliza la noción de derivada. Según Riemann, la función continua $G(x)$ tiene una derivada segunda en el punto x si existe el límite siguiente:

$$\mathrm{D}_2G(x) \overset{\text{def}}{\equiv} \lim_{h\to 0} \frac{G(x+h) + G(x-h) - 2G(x)}{h^2}.$$

Observemos que si G tiene derivada segunda en el sentido de Newton y Leibniz, es decir, si existe $G''(x)$, entonces también existe $\mathrm{D}_2G(x)$ y se verifica la igualdad $\mathrm{D}_2G(x) = G''(x)$.

Por cuanto la existencia de $G''(x)$ nos permite escribir

$$\begin{aligned}\frac{G(x+h)+G(x-h)-2G(x)}{h^2} &= \frac{1}{h^2}\Big(\big[G(x)+G'(x)\cdot h+\frac{1}{2}G''(x)h^2+o(h^2)\big]\\ &\quad +\big[G(x)-G'(x)\cdot h+\frac{1}{2}G''(x)h^2+o(h^2)\big]-2G(x)\Big)\\ &= G''(x)+o(h)\end{aligned}$$

Sin embargo, hay funciones tales como

$$f(x) = \begin{cases} 0\,, & \text{si } x = 0 \\ x^2\,\mathrm{sen}\left(\frac{1}{x}\right), & \text{si } x \neq 0 \end{cases}$$

que carece de derivada segunda ordinaria en el origen, pero que sí la tiene en el sentido de Riemann. Es decir, se trata de una genuina extensión de la noción de derivada segunda.

Paso 4º: Se comprueba que si D_2G *existe y es estrictamente positiva en un intervalo, entonces* G *ha de ser convexa en el mismo. Es decir:*

$$G(x) \leq \frac{G(x+h)+G(x-h)}{2}.$$

Análogamente, si $\mathrm{D}_2G < 0$ *entonces* G *es cóncava:*

$$G(x) \geq \frac{G(x+h)+G(x-h)}{2}.$$

Finalmente si $\mathrm{D}_2G \equiv 0$ *entonces* $G + \varepsilon x^2$ *es convexa para todo* $\varepsilon > 0$. *Luego también lo es* G *por ser un límite uniforme de funciones convexas. Pero, de manera similar,* $G(x) - \varepsilon x^2$ *es cóncava, y tomando límites cuando* ε *tiende a cero obtenemos que la función* G *debe ser cóncava. En conclusión, si* $\mathrm{D}_2G \equiv 0$ *idénticamente en un intervalo entonces* G *es al mismo tiempo cóncava y convexa, luego es lineal.*

Paso 5º: Para concluir la demostración observemos que la hipótesis

$$0 = \lim_{N\to\infty} S_N(x) = \lim_{N\to\infty} \Big[\frac{1}{2}a_0 + \sum_1^N \big\{a_n \cos(2\pi nx) + b_n \operatorname{sen}(2\pi nx)\big\}\Big],$$

$\forall x \in [0,1]$ *implica que la función* F, *definida en el Paso* 2^o, *tiene una derivada segunda generalizada igual a cero en todos los puntos de la recta real. Por lo tanto es lineal, y eso fuerza la anulación del término independiente* ($a_0 = 0$) *y que tengamos la identidad:*

$$\sum_{n\geq 1} \frac{1}{4\pi^2 n^2}\big\{a_n \cos(2\pi nx) + b_n \operatorname{sen}(2\pi nx)\big\} \equiv 0.$$

Pero, en la igualdad anterior, la serie de la izquierda converge uniformemente y es, por tanto, la serie de Fourier de la función de la derecha. Luego todos los coeficientes son iguales a cero.

El capítulo siguiente de esta historia se debe a G. Cantor, quien supuso la convergencia a cero de la serie trigonométrica excepto, quizás, por un conjunto finito de puntos para los que carecemos de información:

$$\lim_{N\to\infty} S_N(x) = 0\,, \qquad \forall x \in [0,1] \setminus \{x_1, x_2, \ldots, x_r\}.$$

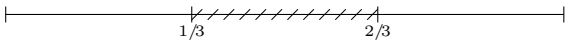
Cantor demostró que, también en este caso, la serie de partida ha de tener todos sus coeficientes nulos. ¿Qué ocurre si eliminamos un conjunto infinito? Se trata de una pregunta natural, pero muy difícil, que da lugar a una interesante definición. Diremos que U es un conjunto de unicidad si toda serie trigonométrica que converge puntualmente a cero en el complementario $[0,1] \setminus U$, ha de tener, necesariamente, todos los coeficientes nulos. Con los métodos analíticos actuales resulta fácil comprobar que un conjunto de unicidad es de medida (Lebesgue) igual a cero. Pero el recíproco es falso: hay conjuntos de medida cero que no son de unicidad. En estos comienzos del siglo XXI *sigue siendo un problema abierto caracterizarlos adecuadamente. No obstante, G. Cantor demostró un resultado muy interesante: una condición suficiente para que U sea de unicidad, es que $U^{(n)}$, el conjunto derivado de orden n, sea vacío para algún entero positivo n. Recordemos que*

$$U^{(1)} = \Big\{ x \mid \big[(x-\varepsilon, x) \cup (x, x+\varepsilon)\big] \cap U \neq \emptyset \,, \forall \varepsilon > 0 \Big\}$$

es el conjunto de los puntos de acumulación de U, y, en general, $U^{(n)}$ es el conjunto de los puntos de acumulación de $U^{(n-1)}$.

Es muy notable que un problema tan concreto sobre los desarrollos trigonométricos llevase a Cantor a introducir conceptos tales como el de conjunto derivado o el de punto de acumulación, y a crear la teoría de los conjuntos y de los cardinales transfinitos de la que surgió, entre otros, el problema de la hipótesis del continuo. Un objeto importante es el conjunto ternario de Cantor, que no es numerable, puesto que su cardinal es el de todos los números reales, pero que, sin embargo, tiene medida igual a cero.

En su construcción se comienza por dividir el intervalo unidad en tres partes iguales:



A continuación eliminamos el trozo de en medio $[\frac{1}{3}, \frac{2}{3})$. Luego se repite el proceso con los dos intervalos restantes

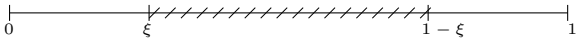
$$\begin{aligned} \big[0, \tfrac{1}{3}\big) &= \big[0, \tfrac{1}{9}\big) \cup \big[\tfrac{1}{9}, \tfrac{2}{9}\big) \cup \big[\tfrac{2}{9}, \tfrac{1}{3}\big), \\ \big[\tfrac{2}{3}, 1\big) &= \big[\tfrac{2}{3}, \tfrac{7}{9}\big) \cup \big[\tfrac{7}{9}, \tfrac{8}{9}\big) \cup \big[\tfrac{8}{9}, 1\big). \end{aligned}$$

Para eliminar los de en medio $[\frac{1}{9}, \frac{2}{9})$, $[\frac{7}{9}, \frac{8}{9})$ y así sucesivamente. El conjunto $\mathcal{C}$ es lo que queda del intervalo $[0,1)$ después de repetir el proceso anterior una cantidad numerable de veces.

Otra caracterización interesante de $\mathcal{C}$ se consigue escribiendo en base 3 el desarrollo decimal de los números del intervalo $[0,1)$. Obtenemos expresiones: $0, x_1 x_2 x_3 \ldots$, donde los dígitos x_j son 0, 1, 2. Pues bien, $\mathcal{C}$ consiste precisamente de aquellos desarrollos decimales en los que no aparece el dígito 1, y su cardinal es el mismo que el de todos los números reales. La hipótesis del continuo, que fue uno de los problemas recogidos por Hilbert en su famoso

discurso del año 1900, se pregunta, precisamente, por la existencia de un cardinal infinito estrictamente mayor que el de los naturales y menor que el de los reales.

En el año 1922, Alexander Rajchman demostró que el conjunto ternario de Cantor es de unicidad. Su alumno A. Zygmund se doctoró en 1923 con una tesis sobre esta teoría, y posteriormente escribió el libro Trigonometric Series, que está dedicado a Rajchman, su maestro, y a Marcinkiewicz, su discípulo, desaparecidos ambos trágicamente durante la segunda guerra mundial. Del año 1955 es el siguiente resultado de R. Salem y A. Zygmund: Dado $\xi < \frac{1}{2}$ *consideremos el conjunto de Cantor* $\mathcal{C}_\xi$ *de razón de disección* ξ*. Es decir, obtenido por el mismo procedimiento que* $\mathcal{C}$ *sin más que sustituir* $1/3$ *por* ξ *en el método de construcción.*



Teorema. $\mathcal{C}_\xi$ *es de unicidad si y solo si* $\theta = \frac{1}{\xi}$ *es un número de Pisot.*

Un número real algebraico, θ*, es de Pisot si sus conjugados* $\theta_1 = \theta$*,* $\theta_2, \ldots, \theta_n$ *verifican que*

$$|\theta| > 1\,, \quad |\theta_j| < 1\,, j = 2, \ldots, n.$$

Fueron definidos por su relación con los problemas de distribución uniforme módulo 1, y son ejemplos de reales tales que las partes fraccionarias de sus potencias enteras no están uniformemente distribuidas en el intervalo unidad. La demostración del teorema de Salem y Zygmund es muy bella, puesto que conecta de forma precisa dos conceptos tan diferentes, a priori, como son la unicidad de las series y los números de Pisot. Contiene argumentos de la Teoría de los Números, del Análisis Armónico y de la Probabilidad. Los lectores interesados pueden encontrar los detalles en (4).

Paul Cohen fue alumno de Zygmund en la Universidad de Chicago. Su tesis doctoral (1958) versó sobre el problema de la unicidad, como expresa su título: Topics in the theory of uniqueness of trigonometric series. En el año 1963 logró demostrar la independencia de la hipótesis del continuo respecto del sistema de axiomas de Zermelo–Fraenkel más el axioma de elección. Completó así los resultados previos de Gödel y recibió por ello la Field Medal, que es el premio que se otorga cada cuatro años, durante el Congreso Internacional de Matemáticas, a creadores que han realizado una obra importante antes de cumplir los cuarenta. En alguna ocasión he oído decir a varios analistas armónicos, pertenecientes a promociones anteriores a la mía en la Universidad de Chicago, que a Zygmund no le parecía bien que alguien como P. Cohen dispersara su gran talento fuera de las series trigonométricas, investigando problemas de lógica matemática. Parece ser que las relaciones entre maestro y discípulo se enfriaron un tanto por esa razón, aunque eso ocurrió antes de que Cohen resolviese el famoso problema de Hilbert.

Estas historias nos hacen constatar, una vez más, la perspicacia y la profundidad del trabajo de Riemann: generalizó la noción de derivada, e introdujo una nueva integral que permite integrar funciones que poseen un conjunto infinito de discontinuidades, siempre que este sea de medida cero. Planteó el problema sutil de la unicidad de las series trigonométricas, que dio lugar a la teoría de conjuntos y de cardinales infinitos de Cantor, por las que llegamos a los teoremas de Cohen y de Gödel. Pero aún no sabemos su final, por cuanto sigue en pie el problema de caracterizar a los conjuntos de unicidad y, además, está por hacer la correspondiente teoría en dimensiones mayores.

Ocurre a menudo que la importancia de un problema se debe más a los universos que ha originado a su alrededor, que al mero interés de la cuestión específica por él suscitada. Los profesores sabemos bien que la originalidad mostrada por algunos alumnos al abordar un problema, y la habilidad para encontrar caminos nuevos que rodeen las dificultades, en lugar de toparse con ellas frontalmente, no siempre van unidas a la erudición. A veces sucede que un matemático que no es experto en el área específica dentro de la que se ha formulado una pregunta, puede, sin embargo, contestarla. Al ser capaz de encontrar un nuevo enfoque, quizás inspirado en los usados en otras materias, pero que despeja los obstáculos contra los que se habían estrellado los especialistas.

Perseguí un enigma,
le ofrecí mi tiempo.
Inventé estrategias que
llevose el viento.

Formulé preguntas,
coseché el silencio.
Inicié mil cuentas
que jamás luz vieron.

Se esfumó mi esfuerzo
en tan vano empeño:
ni obtuve la prueba,
ni el gran contraejemplo.

Lo que yo he buscado
se hallará muy lejos.

De todas las extensiones del concepto de número, la que atañe a los reales (racionales + irracionales) es quizás la que resulta ser conceptualmente más difícil. Existen básicamente dos maneras distintas de hacerlo, ambas del siglo XIX*, una debida a Cantor y basada en la noción de clases de equivalencia de sucesiones de Cauchy de números racionales, y otra debida a Dedekind y que hace uso de la noción de cortadura. En este texto he optado por la vía de Cantor por parecerme más natural llegar al concepto de número real a través de sus sucesivas aproximaciones racionales.*

Un resultado fundamental de Cantor es que $\mathbb{R}$*, el conjunto de los números reales, no es numerable, no es biyectable con los naturales, mientras que el conjunto* $\mathbb{Q}$ *de los racionales sí que lo es. Como señalamos antes este resultado implica que* $\mathbb{Q}$ *es un subconjunto de medida cero en* $\mathbb{R}$*: si escogemos un número al azar en la recta real, con probabilidad igual a 1 será irracional. No obstante, demostrar que un número es racional o irracional puede ser una tarea muy difícil, en la que las matemáticas han progresado poco. Aunque el número* π *fue detectado por los griegos, hubo que esperar al Siglo de las Luces para que Lambert demostrase que es irracional, como también se hizo entonces con el número* e*, base de los logaritmos neperianos o naturales. Pero si nos preguntamos acerca de* $e+\pi$*,* $e\cdot\pi$ *o* π^e *nos encontraremos en terra incognita, como ocurre también con la constante de Euler-Mascheroni:*

$$\gamma = \lim_{N\to\infty}\Big(\sum_1^N \frac{1}{k} - \log N\Big) = 0{,}5772156649\ldots$$

que aparece en tantas fórmulas y de la que todavía ignoramos su carácter racional o irracional.

Parece ser que Jacob Bernoulli fue el primer matemático que expresó su interés por saber el valor exacto de la suma

$$\sum_1^\infty \frac{1}{n^2}$$

sobre la que escribió lo siguiente: "sería muy grande nuestro agradecimiento si alguien nos comunicara este cálculo que, hasta ahora, ha eludido nuestros esfuerzos". Sin embargo, es muy probable que el problema le viniese de su mentor Leibniz, a quien Huygens había propuesto calcular la suma de los recíprocos de los números triangulares, lo que hizo con la observación

$$\sum_1^\infty \frac{1}{n(n+1)} = \sum_1^\infty \Big(\frac{1}{n} - \frac{1}{n+1}\Big) = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \frac{1}{4} + \ldots = 1.$$

Según parece, llevar a cabo esa suma satisfizo tanto a Leibniz que le hizo interesarse por las matemáticas con el resultado que todos conocemos. Pero, volviendo a la pregunta de Jacob Bernoulli, fue Euler, un discípulo de su hermano Johan Bernoulli, quien encontró la solución: $\displaystyle\sum_1^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$.

Que el número π*, la razón de la circunferencia al diámetro, esté relacionado con los enteros a través de la fórmula de Euler es algo tan interesante y misterioso, que cada generación de matemáticos ha encontrado su propia interpretación y algunas otras demostraciones. En el capítulo 5 se presenta la que yo obtuve recientemente, que es especialmente sencilla y puede entenderse por cualquiera que sepa integrar funciones elementales. También*

contiene ese capítulo la prueba de la irracionalidad de $\zeta(3)$, siendo todavía un problema abierto el decidir el carácter, racional o irracional, de los valores de la función ζ en los impares 5, 7, ...

Los desarrollos decimales que son periódicos desde un término en adelante se corresponden con los números racionales. Los irracionales tienen desarrollos que no son periódicos y algunos, como es el caso de π, parecen ser "caóticos" en el sentido de que contienen series de dígitos de cualquier especie, como reza el poema que la premio Nobel de Literatura Wislawa Szymborska le dedicó al número π y que reproducimos completo en el capítulo 5. Se trata, sin embargo, de un problema todavía abierto decidir si el número π es, o no es, un número normal. Es decir, un número tal que cada sucesión finita de dígitos que escribamos aparezca en su desarrollo "decimal" con la frecuencia que le corresponde por su longitud. De nuevo resulta relativamente fácil demostrar que casi todos los números, es decir salvo un conjunto de medida cero, son normales en cualquier base de numeración, pero no sabemos señalar "eficientemente" a uno concreto de ellos. Como cualquier idioma tiene un conjunto finito de letras y signos ortográficos, incluyendo uno para los espacios en blanco, podemos escribir cualquier texto como una sucesión finita de dígitos. Disponiendo de un número normal (por ejemplo π, si fuese verdadero lo que se afirma en el poema de la Szymborska) en su desarrollo decimal encontraremos cualquier texto, aunque quizás echándole mucha paciencia al asunto: el número del carnet de identidad de usted, su fecha de nacimiento, la novela Pedro Páramo, el Quijote..., ¡todo! Es decir, la biblioteca de Babel de los relatos de Borges.

En este capítulo he hecho un uso generoso de algunos ensayos que he ido escribiendo, tales como: "Historias analíticas de tangencias y cuadraturas", publicado dentro del volumen El lenguaje de las Matemáticas en sus Aplicaciones del Ministerio de Educación, Cultura y Deporte; "Las Matemáticas de la Ilustración", Saber/Leer; "La demostración de la Conjetura de Kepler", El País; "Poesía entre teoremas", Methode; "Un matemático en la Transición", Gaceta Matemática; y "El computador y las Matemáticas", Anthropos. El título de este Prólogo, "La vida es un número", fue el del Maratón de Matemáticas que dirigí en el año 2000 dentro del ciclo organizado por el Museo Nacional de Ciencia y Tecnología. Era también el de mi conferencia en ese maratón, que versó sobre la historia de los números. Al final, a modo de resumen o deconstrucción de la lección se me ocurrió leer el poema que, como allí expuse, había encontrado en un libro usado, en una librería de viejo sita en la calle 58 del barrio de Hyde-Park, Chicago, y que, encriptado con una clave numérica que hubo que descifrar, aparecía escrito en un idioma muy extraño, pero siguiendo las indicaciones de un texto de Borges resultó ser una traducción hebrea, con giros del árabe, de un manuscrito hallado en Manzanares El Real. Decía así:

La vida es un número

Pitágoras pensó un mundo perfecto,
donde todo es número y racional.
Pero Hipaso encontró un grave defecto,
del cuadrado unidad la diagonal.

Desde entonces muchos irracionales,
irrumpen en las cuentas, por doquier.
Aunque identificarse entre los reales
es algo que siempre evitan hacer.

Arquímedes escribió el Arenario,
calculando de π sus decimales.
Y Lambert, geómetra visionario
de la Ilustración, con mañas geniales
logró que π y e salieran del armario.

Lo que hicieron con gran osadía,
exhibiendo sus almas trascendentes,
mostrando que el círculo no podía
ser cuadrado al compás de los presentes.

Cantor supo ordenar los racionales
en fila de a uno, estricta formación.
Pero tratándose de irracionales
no cabe esperar tal numeración.

Cuando, con ambos ojos bien cerrados,
escoges al azar un valor real,
muy probable es que sea irracional.
Mas si lo haces con poca precaución,
será un gran enigma saber si es o no.

Hay reales que puedes computar,
leer sus cifras sin ningún titubeo,
pero muchos no se dejan nombrar,
ya sea en griego, latín o arameo.

Hay computables que, en la intimidad,
visten con cifras de curso legal,
practican virtud de ergodicidad,
dando una imagen decente y normal.

Pero en cuanto a π lanzas la cuestión:
Si en privado es normal o peculiar
y si a sus cifras puedes admirar.
Ágil se irá sin dar contestación.

Del cosmos nuestra teoría final,
todas las fuerzas más la gravitación,
remite de nuevo a la idea inicial.
Porque si las cuerdas quiero entender,
sus ecuaciones tendré que resolver.

De modo que Pitágoras, en cierta proporción,
pensando a su manera, también tenía razón.

Agradecimientos. *A Pedro Balodis, José Manuel Marco, Mavi Melián, Bernardo López, Fernando Chamizo y tantos otros compañeros en la docencia de Conjuntos y Números, quienes leyeron el original, hicieron oportunas y sabias sugerencias y enriquecieron la colección de ejercicios propuestos. A Javier Cilleruelo, cuya amistad me brinda una continua fuente de información aritmética, como bien muestran varios capítulos de este libro inspirados en La Teoría de los Números que ambos publicamos en 1992. A Daniel Ortega por haber llevado a cabo la transcripción a LaTeX mejorando tanto la presentación como, muchas veces, el contenido. Y a Amelia, mi mujer, quien limó algunos de los párrafos más cáusticos del manuscrito y, con paciencia y amor, hizo posible que yo tuviese el sosiego y el ánimo necesarios para escribirlo.*

— 1 —

El lenguaje de las Matemáticas

> Reductio ad absurdum *es una de las mejores armas de las matemáticas. Es un gambito mucho más sutil que cualquiera del ajedrez: Un jugador de ajedrez puede ofrecer el sacrificio de un peón o incluso de una figura, pero el matemático ofrece la partida completa.*
>
> G. H. Hardy

1.1. El principio de inducción

Los números llamados naturales tales como

$$1, 2, 3, \ldots, 100, \ldots, 1000, \ldots, 1994, \ldots$$

son los elementos fundamentales de nuestro lenguaje para contar los miembros de un conjunto (uno, dos, tres, ..., cien, ..., mil, ..., mil novecientos noventa y cuatro, ...) en su versión cardinal, o para darles un orden (primero, segundo, tercero, ..., centésimo, ..., milésimo, ..., milésimo noningentésimo nonagésimo cuarto, ...) en su función ordinal.

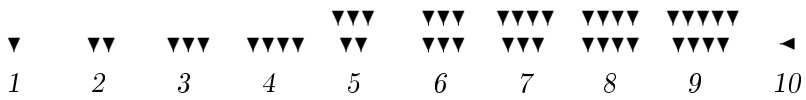
A través de abundantes documentos históricos puede rastrearse su presencia desde tiempos remotos. Sin embargo, el cero, la ausencia de cantidad, de tan dudosa reputación en las aulas, ha sido un concepto algo más elusivo y posterior. En lo sucesivo designaremos con la letra $\mathbb{N}$ *al conjunto de los número naturales más el cero:*

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

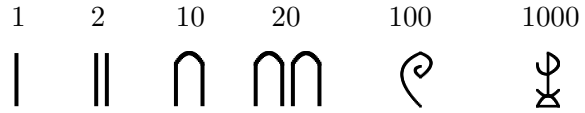
La Aritmética elemental, que es una parte muy importante de las Matemáticas de la infancia, trata, precisamente, de este conjunto de números y de sus relaciones y operaciones: suma, resta, multiplicación, división, congruencia y divisibilidad, entre otras muchas.

He aquí algunos ejemplos de representaciones de los números naturales en diversas civilizaciones:

1. ***Los números de los babilonios*** *(escritura cuneiforme):*



2. ***Los números de los egipcios*** *(en su escritura jeroglífica):*



3. ***La numeración romana****:*

I	*II*	*III*	*IV*	*V*	*VI*	*VII*	*VIII*	*IX*	*X*	*XX*	*XXX*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*20*	*30*

XL	*L*	*LX*	*LXXIII*	*C*	*D*	*M*	*MCMXCIV*
40	*50*	*60*	*73*	*100*	*500*	*1000*	*1994*

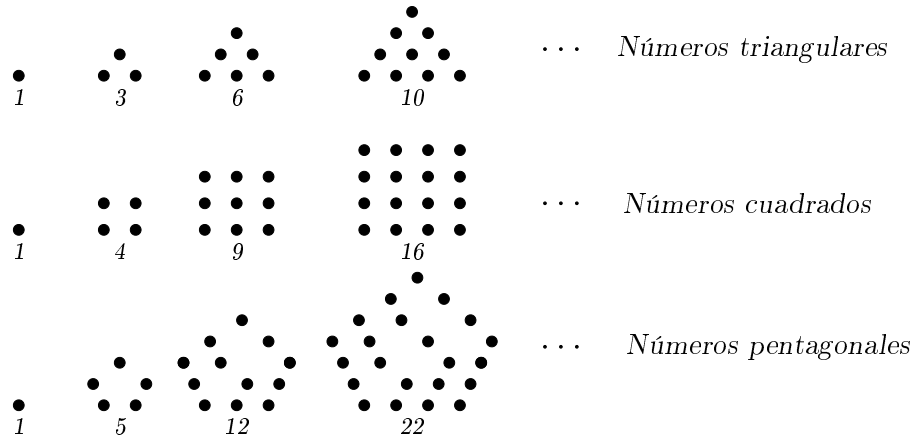
4. ***Los ordinales****: primero, segundo, tercero, cuarto, quinto, sexto, séptimo, octavo, noveno (nono), décimo, undécimo, duodécimo, decimotercero, decimocuarto, . . . , vigésimo, vigésimo primero, . . . , trigésimo, . . . , cuadragésimo, . . . , quincuagésimo, . . . , sexagésimo, . . . , septagésimo, . . . , centésimo, . . . , ducentésimo, . . . , tricentésimo, . . . , milésimo, . . . , milésimo noningentésimo nonagésimo nono, . . .*

Ejercicios

1) *Usar el diccionario, si es preciso, para escribir la forma ordinal de los números siguientes:* 239, 1973, 15631, 8395.

2) *Escribir los números (cardinales y ordinales) en diversas lenguas (inglés, francés, alemán, catalán, portugués, . . .).*

3) *Los pitagóricos representaban a los números con piedras (cálculos) en la arena, de donde procede la palabra "calcular":*



Calcular el quinto número triangular, y el sexto, y el milésimo noningentésimo nonagésimo nono. Hágase lo mismo para los pentagonales. ¿Cómo empezaría la sucesión de los números hexagonales?

El conjunto de los números naturales se encuentra en la raíz misma de la Ciencia, cuyo programa más reduccionista, tan caro a los matemáticos, tiene su expresión más extrema en la conocida frase de Leopold Kronecker: "Dios creó a los naturales, el resto es obra de los hombres".

La descripción de $\mathbb{N}$ *empieza por constatar la existencia del cero. Luego se observa que todo natural,* n*, tiene un único siguiente,* $S(n)$*:*

$$S(0) = 1,\ S(1) = 2,\ S(2) = 3,\ \ldots,\ S(10) = 11,\ \ldots$$

De manera que, por un lado, el cero no es siguiente de nadie, mientras que si $S(n) = S(m)$ *entonces* n *y* m *son el mismo natural. Una propiedad (en realidad un axioma) muy importante de los números naturales es la siguiente:*

Si un conjunto de números naturales A *tiene las propiedades:*

a) 0 *pertenece a* A $(0 \in A)$*;*

b) si n *pertenece a* A *entonces el siguiente* $S(n)$ *también pertenece al conjunto* A $(n \in A \implies S(n) \in A)$*,*

entonces el conjunto A *es necesariamente igual a* $\mathbb{N}$*.*

Esta propiedad de los números naturales recibe el nombre de Principio de inducción y tiene esta otra forma equivalente:

> *Supongamos que para cada número natural* n *mayor o igual que* n_0 *nos es dada una proposición* $P(n)$*, susceptible de ser verdadera o falsa. Si resulta que* $P(n_0)$ *es cierta y la verdad de* $P(n)$ *implica la de* $P(n+1)$*, cualquiera que sea el natural* n*, entonces las proposiciones* $P(k)$*,* $k \geq n_0$*, son todas verdaderas.*

Imaginemos una cantidad de fichas de dominó colocadas en fila, de manera que la caída de una de ellas derribe siempre a la siguiente. Entonces, abatiendo la primera ficha podemos estar seguros de la caída de todas las demás. En el enunciado del principio de inducción las fichas de dominó son las proposiciones (enunciados), susceptibles de ser verdaderas o falsas, una por cada número natural.

Ejemplo 1: *La proposición P_n afirma que la suma de los n primeros cuadrados $1^2 + 2^2 + \cdots + n^2$ es igual a*

$$\frac{n(n+1)(2n+1)}{6}.$$

Veamos cómo se aplica el principio de inducción a este ejemplo:

i) Suponiendo que sea cierta la igualdad

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

es decir, que la proposición P_n es cierta, tenemos que demostrar que P_{n+1} también lo es.

Ahora bien:

$$\begin{aligned} 1^2 + 2^2 + \cdots + (n+1)^2 &= 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2, \end{aligned}$$

bajo la hipótesis de que P_n es cierta. Una sencilla manipulación nos produce:

$$\begin{aligned} 1^2 + 2^2 + \cdots + (n+1)^2 &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)[2n^2 + n + 6n + 6]}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} \end{aligned}$$

que es lo que afirma la proposición P_{n+1}. Luego si P_n es cierta, entonces P_{n+1} también lo es.

Obsérvese que, en esta etapa, no afirmamos que las proposiciones sean ciertas o falsas. Lo que hemos comprobado es que están dispuestas de manera que si P_n es cierta (si la enésima ficha cae) entonces P_{n+1} lo es (la siguiente ficha también cae).

ii) Comprobemos ahora que P_1 es cierta (la primera ficha es abatida):

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

Luego, según el principio de inducción, podemos afirmar que todas las proposiciones son ciertas y que, por lo tanto, tenemos la identidad:

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

cualquiera que sea el número natural k.

El principio de inducción es pues una ley fundamental del razonamiento lógico-matemático y un arma poderosa de demostración. No obstante, su uso es siempre a posteriori y para poder aplicarla con éxito es necesario que hayamos construido previamente la familia de proposiciones P_n. En otras palabras, tenemos que haber imaginado, por otros medios, dónde se encuentra la verdad. Entonces podremos, quizá, utilizar el método de inducción para establecerla de esa forma tan especial, clara, nítida y diamantina como exigen las matemáticas.

En el caso de nuestro ejemplo, $1^2 + 2^2 + \cdots + n^2 = \big(n(n+1)(2n+1)\big)/6$, existe la siguiente estrategia plausible:

> *Recordemos la fórmula que obtuvo Gauss cuando, siendo un niño de pocos años, su maestro le mandó sumar los cien primeros números.*
>
> *Gauss lo resolvió en un periquete hallando la fórmula para sumar los términos de una progresión aritmética. En particular:*
>
> $$1 + 2 + \cdots + n = \frac{n(n+1)}{2} = \frac{1}{2}\, n^2 + \frac{1}{2}\, n.$$
>
> *Fijémonos en el resultado: la suma de los n primeros naturales resulta ser un polinomio cuadrático (de segundo grado) en el número n.*
>
> *Quizá no resulte entonces del todo artificial, o excesivamente ingenioso, que, si nos vemos confrontados con el problema de calcular la suma $1^2 + 2^2 + \cdots + n^2$, apostemos, o hagamos la conjetura, de que esa suma venga dada por un polinomio de tercer grado: $an^3 + bn^2 + cn + d$, para ciertos valores de los coeficientes a, b, c y d.*
>
> *Ahora bien, si esto fuese cierto, no resultaría complicado calcular dichos coeficientes, ya que:*
>
> $$\begin{aligned} 1 &= 1^2 = a + b + c + d \\ 5 &= 1^2 + 2^2 = 8a + 4b + 2c + d \\ 14 &= 1^2 + 2^2 + 3^2 = 27a + 9b + 3c + d \\ 30 &= 1^2 + 2^2 + 3^2 + 4^2 = 64a + 16b + 4c + d \end{aligned}$$

Tenemos un sistema de cuatro ecuaciones con cuatro incógnitas del que podemos despejar los valores de a, b, c y d. En principio, parece complicado, pero en realidad no lo es tanto: Si restamos la primera ecuación de las otras tres obtenemos:

$$\left.\begin{array}{rcl} 7a+3b+c &=& 4 \\ 26a+8b+2c &=& 13 \\ 63a+15b+3c &=& 29 \end{array}\right\}$$

Eliminamos ahora la c y nos queda el sistema:

$$\left.\begin{array}{rcl} 12a+2b &=& 5 \\ 42a+6b &=& 17 \end{array}\right\}$$

Que nos lleva fácilmente a la solución:

$$a=\frac{1}{3},\quad b=\frac{1}{2},\quad c=\frac{1}{6},\quad d=0,$$

y por lo tanto a formular la conjetura o hipótesis precisa:

$$P_n:\ 1^2+2^2+\cdots+n^2 \;=\; \frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n \;=\; \frac{n(n+1)(2n+1)}{6}.$$

Pero cuidado, la relación anterior es solo una hipótesis que hemos elaborado de manera natural a partir de los deberes de Gauss, pero no será un teorema hasta que no logremos dar con una demostración. Ahí, precisamente, es donde el principio de inducción viene en nuestra ayuda.

Ejemplo 2: *La fórmula del binomio de Newton*

$$(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k$$

puede ser demostrada usando el principio de inducción.

En esta fórmula se usa que:

$$\binom{n}{k}=\frac{n!}{k!\,(n-k)!}$$

es el número combinatorio n sobre k, y $k!=1\cdot 2\cdots(k-1)\cdot k$ es la notación habitual para designar al llamado factorial de k, con el convenio añadido de que $0!=1$.

Tenemos que:

$$P_0:\quad 1=(1+x)^0=\sum_{k=0}^{0}\binom{0}{k}x^k=1$$

$$P_1:\quad (1+x)=\sum_{k=0}^{1}\binom{1}{k}x^k=\binom{1}{0}x^0+\binom{1}{1}x=1+x$$

$$P_2:\quad (1+x)^2=\sum_{k=0}^{2}\binom{2}{k}x^k=\binom{2}{0}x^0+\binom{2}{1}x+\binom{2}{2}x^2=1+2x+x^2.$$

Suponiendo P_n cierta, se obtiene que:

$$\begin{aligned} P_{n+1}: \quad (1+x)^{n+1} &= (1+x)^n(1+x) = \left(\sum_{k=0}^{n}\binom{n}{k}x^k\right)(1+x) \\ &= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=0}^{n}\binom{n}{k}x^{k+1} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=1}^{n}\binom{n}{k-1}x^k + x^{n+1} \\ &= 1 + \sum_{k=1}^{n}\left\{\binom{n}{k} + \binom{n}{k-1}\right\}x^k + x^{n+1} \end{aligned}$$

Para concluir observemos que:

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{(n+1-k)!n! + k\cdot n!}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}. \end{aligned}$$

Ejemplo 3: *Leonardo de Pisa, también llamado Fibonacci, vivió entre los siglos* XII *y* XIII*, y desempeñó un papel fundamental en la difusión europea del sistema decimal de numeración, creado por los matemáticos indios, aunque hubo antecedentes sumerios, y trasladado a Europa por los árabes a través de España, según se desprende de diversos documentos de la época del rey Sabio. Escribió un tratado, el Liber Abaci, que ejerció una notable influencia en su tiempo. Fibonacci construyó también una sucesión muy interesante. Se trata de la siguiente:*

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ \ldots$$

cuyo término general F_n se obtiene sumando los dos anteriores:

$$F_n = F_{n-1} + F_{n-2},\ n \geq 3\,, \qquad F_1 = 1, \quad F_2 = 1.$$

Proposición. $F_n \geq n-1$.

Demostración *(por inducción).*

a) $F_1 = 1 \geq 1-1 = 0$; $F_2 = 1 \geq 2-1 = 1$; $F_3 = 2 \geq 3-1 = 2$.

b) Dado $n \geq 3$, si $F_k \geq k-1$, para $k = 1, \ldots, n$, entonces $F_{n+1} \geq n$.

Veamos: dado $n \geq 3$ tenemos, por la definición, que $F_{n+1} = F_n + F_{n-1}$, y por la hipótesis de inducción:

$$F_{n+1} \geq n-1\ +\ n-2 = n\ +\ n\ -\ 3\ \geq\ n. \qquad \blacksquare$$

Luego la sucesión F_n va creciendo haciéndose tan grande como queramos desde un término en adelante.

Observemos que:

$$\begin{aligned} 1 \times 2 - 1^2 &= 1 \\ 1 \times 3 - 2^2 &= -1 \\ 2 \times 5 - 3^2 &= 1 \\ 3 \times 8 - 5^2 &= -1 \\ 5 \times 13 - 8^2 &= 1 \\ 8 \times 21 - 13^2 &= -1 \\ 13 \times 34 - 21^2 &= 1 \\ &\dots \end{aligned}$$

Parece razonable hacer la conjetura:

$$F_n F_{n+2} - F_{n+1}^2 = (-1)^{n+1}$$

cuya demostración es, de nuevo, un sencillo ejercicio del método de inducción:

a) *Cuando $n = 1$ resulta ser verdadera:*

$$1 \times 2 - 1^2 = 1.$$

b) *Supongamos cierto que*

$$F_n F_{n+2} - F_{n+1}^2 = (-1)^{n+1}.$$

Se trata de ver que también se cumple la siguiente igualdad:

$$F_{n+1} F_{n+3} - F_{n+2}^2 = (-1)^{n+2}.$$

Veamos:

$$\begin{aligned} F_{n+1} F_{n+3} - F_{n+2}^2 &= F_{n+1}(F_{n+2} + F_{n+1}) - F_{n+2}^2 \\ &= F_{n+1}^2 - F_{n+2}(F_{n+2} - F_{n+1}) \\ &= F_{n+1}^2 - F_{n+2} F_n \\ &= -(F_n F_{n+2} - F_{n+1}^2) \\ &= -(-1)^{n+1} = (-1)^{n+2} \end{aligned}$$

donde la hipótesis de inducción ha sido usada en la penúltima igualdad, completando rigurosamente la demostración de la fórmula:

$$F_n F_{n+2} - F_{n+1}^2 = (-1)^{n+1}$$

para cualquier valor de n.

Dividiendo ambos miembros por el producto $F_n \cdot F_{n+1}$ *obtenemos que:*

$$\frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n} = \frac{(-1)^{n+1}}{F_n F_{n+1}}.$$

Y teniendo en cuenta que $F_n \geq n-1$, *resulta que para todo* $n \geq 2$ *ha de verificarse la estimación:*

$$\Big|\frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n}\Big| \leq \frac{1}{n(n-1)}.$$

Consideremos ahora la diferencia:

$$\begin{aligned}
\Big|\frac{F_{n+m+1}}{F_{n+m}} - \frac{F_{n+1}}{F_n}\Big| &= \Big|\frac{F_{n+m+1}}{F_{n+m}} - \frac{F_{n+m}}{F_{n+m-1}} + \frac{F_{n+m}}{F_{n+m-1}} - \frac{F_{n+m-1}}{F_{n+m-2}} \\
&\quad + \cdots + \frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n}\Big| \\
&\leq \Big|\frac{F_{n+m+1}}{F_{n+m}} - \frac{F_{n+m}}{F_{n+m-1}}\Big| + \Big|\frac{F_{n+m}}{F_{n+m-1}} - \frac{F_{n+m-1}}{F_{n+m-2}}\Big| \\
&\quad + \cdots + \Big|\frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n}\Big| \\
&\leq \frac{1}{(n+m-1)(n+m-2)} + \frac{1}{(n+m-2)(n+m-3)} \\
&\quad + \cdots + \frac{1}{n(n-1)} \\
&= \frac{1}{n-1} - \frac{1}{n+m-1} \leq \frac{1}{n-1}
\end{aligned}$$

ya que $\dfrac{1}{k(k+1)} = \dfrac{1}{k} - \dfrac{1}{k+1}$.

La estimación anterior demuestra que la sucesión de los cocientes de términos consecutivos de la sucesión de Fibonacci, $\{\frac{F_{n+1}}{F_n}\}$, *es una sucesión de Cauchy de números racionales. Tiene por lo tanto un límite, que será un número real*[*], *al que llamaremos* Φ.

Como $F_{n+2} = F_n + F_{n+1}$ *resulta que:*

$$\frac{F_{n+2}}{F_n} = 1 + \frac{F_{n+1}}{F_n}\,; \qquad \textit{pero:} \quad \frac{F_{n+2}}{F_n} = \frac{F_{n+2}}{F_{n+1}} \cdot \frac{F_{n+1}}{F_n}.$$

Tomando límites obtenemos la identidad:

$$\Phi^2 = 1 + \Phi$$

y, como $\Phi \geq 1$, *la solución buscada es:*

$$\Phi = \frac{1+\sqrt{5}}{2} = 1{,}6180339\ldots, \quad \textit{¡el número de oro!, ¡la divina proporción!}$$

[*] Ver el capítulo 5 sobre los números reales.

A ti, maravillosa disciplina,
media, extrema razón de la hermosura
que claramente acata la clausura
viva en la malla de tu ley divina.

A ti, cárcel feliz de la retina
áurea sección, celeste cuadratura,
misteriosa fontana de mesura
que el universo armónico origina.

A ti, mar de los sueños angulares,
flor de las cinco formas regulares,
dodecaedro azul, arco sonoro.

Luces por alas un compás ardiente.
Tu canto es una esfera transparente.
A ti, divina proporción de oro.

Rafael Alberti

Ejercicios

1) *Hallar una fórmula para la suma* $1^3+2^3+\cdots+n^3$ *y demostrar su validez usando la inducción completa.*

2) *Demostrar la fórmula:*

$$\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^3}+\cdots+\frac{n}{2^n} = 2-\frac{n+2}{2^n}.$$

3) *Demostrar la fórmula:*

$$(1+q)(1+q^2)(1+q^4)\cdots(1+q^{2^n}) = \frac{1-q^{2^{n+1}}}{1-q}.$$

4) *La sucesión de Fibonacci,* $\{F_n\}$*, está definida por medio de la ley de recurrencia:*

$$F_1=1, \quad F_2=1, \quad F_{n+2}=F_n+F_{n+1}.$$

Calcular los diez primeros términos de la sucesión y demostrar la siguiente identidad:

$$F_n = \frac{\left[\frac{1+\sqrt{5}}{2}\right]^n - \left[\frac{1-\sqrt{5}}{2}\right]^n}{\sqrt{5}}.$$

5) *Demostrar por inducción:*

a) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$ *para cualquier* $n \in \mathbb{N}$, $n \geq 1$.

b) *La suma de los primeros* k *números naturales impares es* k^2.

c) *La suma de los primeros* k *números naturales pares es* $k^2 + k$.

d) *Dado* $a \in \mathbb{R}$, $a \neq 1$, *se tiene* $\sum_{j=0}^{n} a^j = \frac{a^{n+1}-1}{a-1}$ *para cualquier* $n \in \mathbb{N}$.

e) $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$ *para cualquier* $n \in \mathbb{N}$, $n \geq 1$.

6) k) *Demostrar que si* $n \in \mathbb{N}$, $n > 2$, *entonces* $2^n > 1 + 2n$.

b) *Demostrar que si* $n \in \mathbb{N}$, $n > 4$, *entonces* $2^n > n^2 + 1$.

c) *Demostrar que si* $n \in \mathbb{N}$, *entonces el número* $a_n = 4^n + 6n - 1$ *es divisible por* 9.

d) *Demostrar que si* $n \in \mathbb{N}$, *entonces el número* $b_n = 7^n - 4^n$ *es divisible por* 3.

7) *Vamos a demostrar que, dado un conjunto* C *de* n *caballos, todos los caballos de* C *son del mismo color. Lo haremos por inducción sobre* n.

a) *Si* $n = 1$ *solo hay un caballo, luego todos son del mismo color. (Podíamos incluso haber empezado con* $n = 0$, *ningún caballo, de modo que también son todos del mismo color, pero no es el caso más interesante.)*

b) *Supongámoslo cierto para conjuntos de* n *caballos, y sea* $C = \{c_1, c_2, \ldots, c_n, c_{n+1}\}$ *un conjunto con* $n+1$ *caballos. Por la hipótesis de inducción, los* n *caballos del conjunto* $C' = \{c_1, \ldots, c_n\}$ *tienen el mismo color, y lo mismo sucede con los* n *caballos del conjunto* $C'' = \{c_2, \ldots, c_{n+1}\}$. *Como* c_n *está en* C' *y en* C'', *todos los caballos de* C *tienen el mismo color que* c_n, *y por tanto son todos del mismo color.*

Como todos hemos visto caballos de al menos dos colores, ¿dónde está el fallo de esta "demostración"?

1.2. Conjuntos

La noción intuitiva de conjunto constituye un elemento básico de nuestro lenguaje. Una biblioteca es un conjunto de libros; los jugadores de un equipo de fútbol forman un conjunto; también lo son los andaluces de Jaén o los buscadores de setas.

Lo que quizá no es tan conocido es que las matemáticas (y por tanto toda la ciencia) se basa, finalmente, en la Teoría de Conjuntos. Al menos ese

es el sueño reduccionista que ha ocupado, y sigue ocupando, a una cantidad importante de matemáticos. He aquí algunos nombres especialmente significativos: Frege, Russell, Cantor, Zermelo, Boole, Hilbert, Gödel, Turing...

La historia de la Teoría de Conjuntos se inició con las investigaciones de Cantor sobre la unicidad de los desarrollos trigonométricos, y pronto deparó sorpresas y paradojas que obligaron a los matemáticos a precisar los conceptos y las relaciones existentes entre ellos. El resultado es el edificio magnífico de la Lógica Matemática del siglo XX*, con sus implicaciones filosóficas y sus aplicaciones a la teoría de la computación.*

La notación $a \in X$ es la usual en matemáticas para designar que a es un elemento del conjunto X. La letra griega épsilon, escrita de esta manera especial, $\in$, se reserva exclusivamente para indicar la relación de pertenencia, de manera que cuando hay que usar épsilon en otro contexto, suele escribirse de forma ligeramente distinta:

$$\text{“para todo } \varepsilon > 0 \text{ existe } \delta > 0, \ldots \text{”}$$

Un conjunto puede describirse dando la lista de sus elementos. Otro procedimiento consiste en presentar una propiedad que los caracterice. Por ejemplo:

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

es el conjunto de los diez dígitos del sistema de numeración decimal; mientras que el conjunto de los andaluces de Jaén está formado por todas las personas censadas en dicha provincia.

La igualdad de conjuntos, $X = Y$, significa que ambos tienen los mismos elementos. Es una relación reflexiva ($X = X$ siempre), y simétrica, (si $X = Y$, entonces $Y = X$). Es también transitiva por cuanto si X e Y son iguales, e Y coincide con Z, entonces X y Z son iguales.

La inclusión, $X \subset Y$, se da cuando todos los elementos de X lo son también de Y. Es una relación reflexiva, por cuanto $X \subset X$ siempre, y antisimétrica, ya que si tenemos que $X \subset Y$ y que $Y \subset X$, entonces necesariamente ha de darse la igualdad $X = Y$. Es también transitiva por cuanto si X es un subconjunto de Y ($X \subset Y$), e Y es un subconjunto de Z ($Y \subset Z$), entonces X es un subconjunto de Z ($X \subset Z$).

Un postulado importante es la existencia del conjunto vacío, $\emptyset$, que no tiene elementos. Otro es que todo conjunto X da lugar al conjunto $\mathcal{P}(X)$ (partes de X) cuyos elementos son precisamente los subconjuntos de X. Por ejemplo, si $X = \{1, 2, 3, 4\}$ entonces

$$\begin{aligned}\mathcal{P}(X) \;=\; \Big\{ &\emptyset,\, \{1\},\, \{2\},\, \{3\},\, \{4\},\, \{1,2\},\, \{1,3\},\, \{1,4\},\, \{2,3\},\, \{2,4\},\, \{3,4\},\\ &\{1,2,3\},\, \{1,2,4\},\, \{1,3,4\},\, \{2,3,4\},\, \{1,2,3,4\}\Big\}\end{aligned}$$

De manera que la situación se complica, por cuanto hay muchos conjuntos interesantes cuyos elementos son asimismo otros conjuntos. La Geometría nos provee muchos ejemplos: una recta es un conjunto de puntos; un haz de rectas es un conjunto de rectas; etc.

A veces es preciso considerar situaciones en las que los elementos de un conjunto son conjuntos, cuyos elementos son también conjuntos, y estos, a su vez, son conjuntos, etc., formándose torres de longitudes arbitrarias. Pero entonces hay que tener un cuidado exquisito con las reglas lógicas y con el lenguaje. De otra forma se originan paradojas por el uso indiscriminado e intuitivo de la noción de conjunto. Esa fue la lección que los matemáticos que se preocuparon de los fundamentos aprendieron a principios del siglo pasado. El resultado, como ya apuntamos antes, fue la creación del magnífico edificio de la Lógica Matemática.

A veces, y para no repetir en demasía la palabra conjunto, conviene usar algunos sinónimos, tales como colección o familia. También está la palabra clase, aunque esta presenta el inconveniente de que, en algunas teorías más sofisticadas que las que vamos a considerar en este libro, tiene un significado muy preciso y distinto al de conjunto. Por eso es recomendable no hacer uso de ella.

Dos operaciones importantes entre conjuntos son la unión y la intersección.

En el caso de dos conjuntos X, Y, la unión, que se designa mediante el símbolo $X \cup Y$, es el conjunto de los elementos que pertenecen a alguno de los conjuntos X o Y:

$$X \cup Y = \{\, x \mid x \in X \text{ o } x \in Y \,\}.$$

La intersección, $X \cap Y$, consta de los elementos que están en ambos X e Y:

$$X \cap Y = \{\, x \mid x \in X \text{ y } x \in Y \,\}.$$

Puede darse el caso de que X e Y no tengan ningún elemento común, entonces su intersección es el conjunto vacío ($X \cap Y = \emptyset$) y diremos que son dos conjuntos disjuntos.

Dado un conjunto, o universo, X, en el conjunto de sus partes, $\mathcal{P}(X)$, podemos definir el importante concepto de complementario: a todo subconjunto Y de X le asociamos $Y^c = X - Y$ (su complementario) que es el conjunto de los elementos de X que no pertenecen a Y. Usando la notación $x \notin Y$ para designar que x no es elemento de Y, podemos escribir:

$$Y^c = \{\, x \in X \mid x \notin Y \,\}.$$

Estas tres operaciones (unión, intersección y complementario) nos permiten dotar al conjunto $\mathcal{P}(X)$ de una estructura interesante, llamada álgebra de Boole de los subconjuntos de un conjunto.

En varios capítulos de este libro se profundizará en el estudio del álgebra de Boole, y en las nociones de relación de equivalencia y conjunto cociente. También se estudiarán: tipos de funciones (inyectiva, sobreyectiva, biyectiva); el concepto de equipotencia de conjuntos (Teorema de Schröeder-Bernstein); la noción de número cardinal (numerabilidad e hipótesis del continuo); las paradojas y la necesidad de una axiomática (el sistema de Zermelo-Fraenkel).

Otra operación importante es el producto cartesiano, que pasamos a describir.

Producto cartesiano. *Dados dos conjuntos no vacíos, W y Z, su producto cartesiano, $W \times Z$, es el conjunto de todos los pares ordenados, (w, z), formados por un primer elemento w de W, y un segundo elemento z perteneciente al conjunto Z:*

$$W \times Z = \big\{(w, z) \mid w \in W,\, z \in Z\big\}.$$

El par ordenado (w, z) tiene dos elementos, pero es distinto del conjunto $\{w, z\}$ que ambos constituyen. La razón estriba en que los conjuntos $\{w, z\}$ y $\{z, w\}$ son idénticos por tener los mismos elementos, pero (w, z) y (z, w) son pares ordenados diferentes (salvo, claro está, en el caso $w = z$). Una definición plausible de par ordenado como conjunto es la siguiente:

$$(a, b) \stackrel{\text{def}}{\equiv} \big\{\{a\}, \{a, b\}\big\}.$$

Es decir, el par ordenado (a, b) es un conjunto con dos elementos: el primero es el conjunto $\{a\}$, cuyo único elemento es el primero del par; mientras que el segundo, $\{a, b\}$, es el conjunto cuyos miembros son las dos componentes del par. De esta sencilla manera conseguimos asimetría entre los dos elementos ya que

$$(b, a) = \big\{\{b\}, \{a, b\}\big\} \text{ es distinto de:}$$
$$(a, b) = \big\{\{a\}, \{a, b\}\big\} \text{ excepto cuando } a = b.$$

Si ambos conjuntos, W y Z, tienen un número finito de elementos, entonces el número de elementos de $W \times Z$, su cardinal, es igual al producto de los cardinales de W y Z:

$$Z = \{z_1, \ldots, z_n\}$$
$$W = \{w_1, \ldots, w_m\}$$
$$W \times Z = \big\{(w_j, z_k) \mid j = 1, \ldots, m;\, k = 1, \ldots, n\big\}$$
$$\text{card}(W \times Z) = m \times n = \text{card}(W) \times \text{card}(Z).$$

Empero en muchas ocasiones interesantes los conjuntos W y Z pueden ser infinitos y, en este caso, la cuenta anterior nos llevará a manejar la aritmética de los cardinales infinitos.

Si en vez de dos conjuntos dispusiéramos ahora de un número finito de ellos, $W_1, \ldots, W_n$, el producto cartesiano

$$W_1 \times \cdots \times W_n = \big\{(w_1, \ldots, w_n) \mid w_1 \in W_1, \ldots, w_n \in W_n\big\}$$

es el conjunto formado por todas las n–uplas ordenadas, $(w_1, \ldots, w_n)$, tales que $w_j \in W_j$, $j = 1, \ldots, n$.

La definición precisa puede hacerse por inducción:

$$W_1 \times \cdots \times W_n = (W_1 \times \cdots \times W_{n-1}) \times W_n\,.$$

Cabría también la posibilidad simétrica de definir

$$W_1 \times \cdots \times W_n = W_1 \times (W_2 \times \cdots \times W_n)\,,$$

en cuyo caso obtendríamos un conjunto equivalente (biyectable) con el anterior:

$$(w_1,\, (w_2, \ldots, w_n)\,) \iff (\,(w_1, \ldots, w_{n-1}), w_n\,)\,.$$

La demostración la dejamos como ejercicio al lector.

Otra posibilidad interesante es definir directamente una n–upla ordenada como un conjunto:

$$\begin{aligned}(w_1, \ldots, w_n) = \big\{\{w_1\}, \{\{w_1, w_2\}\}, \{\{\{w_1, w_2, w_3\}\}\}, \ldots \\ \ldots, \{\{\cdots\{\{w_1, w_2, \ldots, w_n\}\}\cdots\}\}\big\}\end{aligned}$$

siendo entonces $W_1 \times \ldots \times W_n$ el conjunto de todas las n–uplas ordenadas $(w_1, \ldots, w_n)$ tales que $w_j \in W_j$, $\forall j$.

El lector puede entretenerse en analizar la equivalencia de estas distintas definiciones en el sentido de generar conjuntos con el mismo número de elementos.

Análogamente al caso de los pares ordenados, también una n–upla ordenada es un conjunto:

$$(w_1, \ldots, w_n) = (w_1,\, (w_2, \ldots, w_n)\,) = \big\{\{w_1\}, \{w_1, (w_2, \ldots, w_n)\}\big\}.$$

Si cada componente, W_j, es un conjunto finito, entonces también lo será el producto, $W_1 \times \cdots \times W_n$, de forma que:

$$card\big(W_1 \times \cdots \times W_n\big) = \prod_{k=1}^{n} card(W_k).$$

Si alguno de los conjuntos, W_j, fuese vacío, entonces no cabe la construcción anterior, pero podríamos convenir que, en ese caso, el producto cartesiano es también vacío. Resulta una extensión un poco pedante, pero tiene la virtud de que podemos considerar el producto cartesiano de n conjuntos, $W_1 \times \cdots \times W_n$, sean vacíos o no. Basta con que uno de los factores sea el vacío para que también lo sea su producto. En caso contrario los elementos del producto cartesiano son las n–uplas ordenadas $(w_1, \ldots, w_n)$, con $w_j \in W_j$ para $j = 1, \ldots, n$.

No obstante, en las matemáticas, hay muchas situaciones interesantes que nos llevan a considerar el producto cartesiano de una infinidad de conjuntos:

$$\prod_{i \in I} W_i.$$

Es decir, un producto sobre un conjunto infinito de índices, I. Un ejemplo es cuando I son los números naturales, $\mathbb{N}$; otro cuando I son los números reales.

Un elemento del producto $\prod_{i \in I} W_i$ podríamos designarlo con la misma notación de las n–uplas ordenadas como: $(w_i)_{i \in I}$ y consiste en una función (ver §1.5) $w : I \to \bigcup W_i$ con la propiedad de que $\forall i$, $w_i = w(i) \in W_i$.

Pero cuando tratamos con el infinito el panorama se complica algo:

> *¿Puede ser vacío el producto cartesiano de infinitos conjuntos distintos del vacío?*

A primera vista parece una pregunta de perogrullo, cuya respuesta es obviamente "negativa". Pero no es tan fácil: Señalar a un elemento del producto cartesiano equivale a escoger un elemento en cada conjunto W_i. Es decir, hacer infinitas elecciones, una para cada conjunto; y eso, piénsese en el caso $I = \mathbb{R}$ = conjunto de los números reales, no es una consecuencia de los postulados que hemos ido detectando. En realidad se trata de uno nuevo, llamado axioma de elección, que tiene consecuencias nada inocentes, como iremos descubriendo más adelante. Elegir en el caso de infinitos conjuntos resulta a veces muy complicado.

Bertrand Russell, quien dedicó mucho tiempo a dilucidar estas cuestiones de Lógica Matemática, gustaba describir esta situación con un ejemplo:

> *Si tenemos una colección de pares de zapatos es muy fácil elegir uno de cada par (el del pie derecho, por ejemplo), pero la situación se complica en el caso de parejas de calcetines.*

Ejercicios

1) *Demostrar que para todo conjunto X se tiene que $\emptyset \subset X$ y que $X \subset X$.*

2) *Demostrar que si $X \subset Y$ entonces $\mathcal{P}(X) \subset \mathcal{P}(Y)$.*

3) *Elabora la lista de todos los subconjuntos de $X = \{0, 1, 2, 3, 4\}$.*

4) *Demostrar por inducción que si un conjunto tiene exactamente n elementos, entonces tiene 2^n subconjuntos.*

5) *Demostrar que $\mathcal{P}(X \cap Y) = \mathcal{P}(X) \cap \mathcal{P}(Y)$.*

6) *Demostrar que $\mathcal{P}(X) \cup \mathcal{P}(Y) \subset \mathcal{P}(X \cup Y)$, y dar un ejemplo que muestre que, en general, ambos conjuntos son distintos.*

7) *Demostrar que $(Y \cap Z)^c = Y^c \cup Z^c$, y que $(Y \cup Z)^c = Y^c \cap Z^c$.*

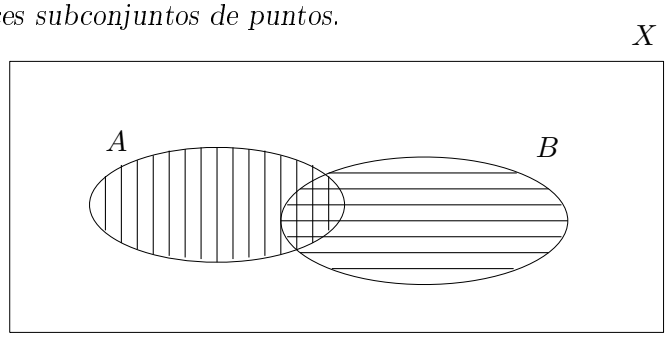
8) *Demostrar la identidad:*

$$(X \cup Y) \cap (Z \cup W) = (X \cap Z) \cup (X \cap W) \cup (Y \cap Z) \cup (Y \cap W)$$

9) *¿Cuántos elementos tiene el conjunto $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))))$?*

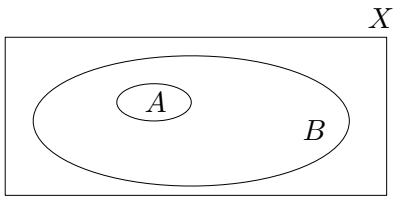
Fijado el conjunto X (nuestro universo) podemos representar gráficamente el álgebra $\mathcal{P}(X)$ por medio de los llamados diagramas de Venn.

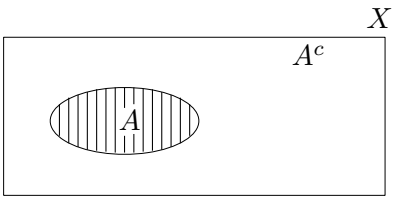
La idea consiste en asignar al conjunto universal X un conjunto de puntos del plano, por ejemplo un rectángulo, de manera que los puntos de X se corresponden con los puntos de dicho rectángulo. Los subconjuntos de X son entonces subconjuntos de puntos.



Esta figura representa al conjunto A (rayado verticalmente) y al B (rayado horizontalmente). La intersección, $A \cap B$, se corresponde con la región doblemente rayada, mientras que la unión, $A \cup B$, es la región rayada de alguna manera (horizontalmente, verticalmente o ambas).

Los diagramas siguientes ilustran, respectivamente, las nociones de inclusión ($A \subset B$) y complementario, $A \cup A^c = X$, $A \cap A^c = \emptyset$:





Ejercicios

1) *Dibujar diagramas de Venn para ilustrar las relaciones siguientes:*

1. $A \cup (B \cup C) = (A \cup B) \cup C$
2. $A \cap (B \cap C) = (A \cap B) \cap C$
3. $A \cup B = B \cup A$
4. $A \cap B = B \cap A$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
7. $(A \cup B)^c = A^c \cap B^c$
8. $(A \cap B)^c = A^c \cup B^c$
9. $A \cup A^c = X$
10. $A \cap A^c = \emptyset$
11. $(A^c)^c = A$

2) *Sean* $S = \{1, 2, 3, 4, 5\}$, $T = \{3, 4, 5, 7, 8, 9\}$, $U = \{1, 2, 3, 4, 9\}$, $V = \{2, 4, 6, 8\}$ *subconjuntos del conjunto* $\mathbb{N}$ *(de números naturales). Calcular:*

a) $S \cap U$ c) $(S \cup U) \cap V$ e) $(U \cup V \cup T) \setminus S$

b) $(S \cap T) \cup U$ d) $(S \cup V) \setminus U$ f) $(S \cup V) \setminus (T \cap U)$

3) *Dados los subconjuntos* S *y* T *en el ejercicio 2, indica cuáles son los elementos del conjunto* $S \times T$ *y observa que es un subconjunto de* $\mathbb{N} \times \mathbb{N}$.

4) *Siguiendo la notación del ejercicio 2, calcula los siguientes subconjuntos de* $\mathbb{N} \times \mathbb{N}$*:*

$$(a)\ (S \times V) \setminus (T \times U) \qquad (b)\ (S \setminus T) \times (V \setminus U)$$

5) *Probar las siguientes fórmulas para subconjuntos* S, T, U *y* V *de un conjunto* X. *(Indicación: Los diagramas de Venn pueden ser muy útiles para aclarar las ideas, pero no sirven para dar una demostración).*

a) $(S \setminus T) \cup (T \setminus S) = (S \cup T) \setminus (S \cap T)$

b) $S \setminus (T \cup U) = (S \setminus T) \cap (S \setminus U)$

c) $S \setminus (T \cap U) = (S \setminus T) \cup (S \setminus U)$

d) $(S \setminus T) \times (U \setminus V) = (S \times U) \setminus [(S \times V) \cup (T \times U)]$

e) $(S \cup T) \times V = (S \times V) \cup (T \times V)$

6) *Calcula el conjunto de partes del conjunto vacío.*

7) *Demuestra que si T es un conjunto finito con n elementos, entonces $\mathcal{P}(T)$ (conjunto de partes de T) es un conjunto con 2^n elementos.*

8) *Calcular el conjunto de partes del conjunto de partes de $T = \{1, 2\}$ (i.e. $\mathcal{P}(\mathcal{P}(T))$).*

9) *Escribir los conjuntos de partes de los siguientes conjuntos:*

$$(a)\ \{1, \emptyset, \{a, b\}\} \qquad (b)\ \{\bullet, \triangle, \partial\} \qquad (c)\ \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$$

10) *Sea $S = \{a, b, c, d\}$. $T = \{1, 2, 3\}$, y $U = \{b, 2\}$. ¿Cúales de las siguientes afirmaciones son verdaderas?:*

(1) $\{a\} \in S$	(2) $a \in S$	(3) $\{a, c\} \subset S$
(4) $\emptyset \in S$	(5) $\{a\} \in \mathcal{P}(S)$	(6) $\{\{a\}, \{a, b\}\} \subset \mathcal{P}(S)$
(7) $\{a, c, 2, 3\} \subset S \cup T$	(8) $U \subset S \cup T$	(9) $b \in S \cap U$
(10) $\{b\} \subset S \cap U$	(11) $\{1, 3\} \in T$	(12) $\{1, 3\} \subset T$
(13) $\{1, 3\} \in \mathcal{P}(T)$	(14) $\emptyset \in \mathcal{P}(S)$	(15) $\{\emptyset\} \in \mathcal{P}(S)$
(16) $\emptyset \subset \mathcal{P}(S)$	(17) $\{\emptyset\} \subset \mathcal{P}(S)$	

11) *Probar o demostrar que son falsas las siguientes afirmaciones:*

$$(a)\ \mathcal{P}(A \cup B) = \mathcal{P}(A) \cup P(B) \quad (b)\ \mathcal{P}(A \cap B) = \mathcal{P}(A) \cap P(B)$$
$$(c)\ \mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$$

12) *Verdadero o falso: Si S_1, S_2, ... son conjuntos de enteros y si $\bigcup_{j=1}^{\infty} S_j = \mathbb{Z}$, entonces uno de los conjuntos S_j debe tener infinitos elementos.*

13) *Verdadero o falso: Si S_1, S_2, ... son conjuntos de números reales, y si $\bigcup_{j=1}^{\infty} S_j = \mathbb{R}$, entonces uno de los S_j debe tener infinitos elementos.*

En los cuatro ejercicios siguientes: A es un conjunto arbitrario de índices y para cada $\alpha \in A$, S_α es un conjunto; T es un conjunto cualquiera.

14) *Probar las siguientes igualdades (donde ^{c} denota el complementario en un universo $\mathcal{U}$):*

(1) $(\bigcap_{\alpha\in A} S_\alpha)^c = \bigcup_{\alpha\in A} S_\alpha^c$ (2) $(\bigcup_{\alpha\in A} S_\alpha)^c = \bigcap_{\alpha\in A} {S_\alpha}^c$

(3) $T \cap (\bigcup_{\alpha\in A} S_\alpha) = \bigcup_{\alpha\in A} (T \cap S_\alpha)$ (4) $T \cup (\bigcap_{\alpha\in A} S_\alpha) = \bigcap_{\alpha\in A} (T \cup S_\alpha)$

15) *Si $T \subset S_\alpha$ para todo $\alpha \in A$, entonces $T \subset \cap_{\alpha\in A} S_\alpha$*

16) *Si $T \supset S_\alpha$ para todo $\alpha \in A$, entonces $T \supset \cup_{\alpha\in A} S_\alpha$*

17) *Decimos que los conjuntos S_α son disjuntos si $\cap_\alpha S_\alpha = \emptyset$; y que son disjuntos dos a dos si $S_\alpha \cap S_\beta = \emptyset$ cuando $\alpha \neq \beta$. Explicar la diferencia entre los dos conceptos y dar ejemplos.*

Una relación binaria $\mathcal{R}$ en un conjunto no vacío X determina una familia A de pares ordenados, o elementos del producto cartesiano $X \times X$, que satisfacen precisamente esa relación:

$A\,\mathcal{R}\,b$ (a está relacionado con b) si y solo si $(a, b) \in A \subset X \times X$.

Ejemplos:

i) $X = \{$ *españoles* $\}$. *La relación $a\,\mathcal{R}\,b$ significa que ambos, a y b, nacieron el mismo día del año, aunque quizás en años distintos.*

ii) $X = \{$ *andaluces* $\}$; *$a\,\mathcal{R}\,b$ si y solo si ambos, a y b, habitan en la misma provincia.*

iii) $X = \{$ *triángulos planos* $\}$; *$\sigma\,\mathcal{R}\,\tau$ si y solo si son triángulos semejantes.*

iv) $X = \{$ *líneas rectas del plano* $\}$; *$r\,\mathcal{R}\,s$ si y solo si son perpendiculares.*

Siguiendo el punto de vista según el cual todo es un conjunto ("conjunto es todo lo que es, pero el de todos no es"), definir una relación $\mathcal{R}$ en X equivale pues a identificar un subconjunto A del producto cartesiano $X \times X$. Habrá pues tantas relaciones como elementos de $\mathcal{P}(X \times X)$.

No obstante, entre todas las relaciones que pueden establecerse en un conjunto X las hay que tienen un interés especial:

Definición. *La relación $\mathcal{R}$ dada por el conjunto de pares ordenados $A \subset X \times X$ es de equivalencia si posee las propiedades siguientes:*

i) Reflexiva: *Para todo elemento $a \in X$ se verifica que $(a, a) \in A$. En otras palabras, todo elemento está relacionado consigo mismo.*

ii) Simétrica: *Si $(a, b) \in A$, entonces $(b, a) \in A$. Es decir, si a está relacionado con b, entonces b lo está con a.*

iii) Transitiva: *Si $(a, b) \in A$ y $(b, c) \in A$, entonces, necesariamente, también $(a, c) \in A$.*

Ejercicio 1. *Discernir cuales de los ejemplos anteriores son relaciones de equivalencia.*

Una relación de equivalencia definida en el conjunto X origina una partición de X en una familia, $\{X_i\}$, de subconjuntos disjuntos, $X_i \cap X_j = \emptyset$ si $i \neq j$, $\bigcup X_i = X$. De manera que en cada X_i se encuentran todos los elementos que están relacionados entre sí. En el lenguaje de las matemáticas se dice que la relación de equivalencia da lugar al conjunto cociente $X/\mathcal{R}$ formado, precisamente, por todas esas clases de equivalencia, disjuntas dos a dos.

Se trata de un poderoso mecanismo de construcción de objetos más complejos, clases de equivalencia, a partir de un conjunto dado, que será ampliamente utilizado a lo largo de este libro en la construcción de las diversas clases de números: enteros, racionales, reales y complejos.

En cierta medida, podríamos decir que los capítulos sucesivos representan un homenaje a este procedimiento. No obstante, aún a riesgo de adelantarnos un tanto a la muy básica construcción *de los números, podemos entrenarnos en los ejercicios siguientes.*

Ejercicios

1) *Hemos definido una relación $\mathcal{R}$ en un conjunto A a partir de un subconjunto $S_{\mathcal{R}} \subset A \times A$.*

i) Definir en $A = \{a, b, c\}$ una relación $\mathcal{R}$ que sea de equivalencia y que no sea la identidad.

ii) Hallar la partición en A definida por la relación en i).

2) *Definir una partición en $A = \{a, b, c\}$ y describir el subconjunto $S_{\mathcal{R}} \subset A \times A$ correspondiente a la relación de equivalencia asociada a dicha partición.*

3) *Sea $\mathcal{R}$ una relación definida en un conjunto X. Demostrar que $\mathcal{R}$ es una relación de equivalencia $\Longleftrightarrow$ $\mathcal{R}$ satisface las dos propiedades siguientes:*

i) Para todo $x \in X$ existe un $a \in X$ tal que $a\,\mathcal{R}\,x$.

ii) $a\,\mathcal{R}\,b$ y $a\,\mathcal{R}\,c \Rightarrow b\,\mathcal{R}\,c$.

4) *Considerar la relación sobre $\mathbb{Z}$ definida por: $(m, n) \in \mathcal{R} \Leftrightarrow m + n$ es par. Demostrar que es una relación de equivalencia. Describir las clases de equivalencia y el conjunto cociente.*

5) *(Véase la sección 3.1.) (a) Sea $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$. Considerar la relación sobre $\mathbb{Z}$ definida por: $(m, n) \in \mathcal{R} \Leftrightarrow m - n \in 3\mathbb{Z}$. Demostrar que es una relación de equivalencia. Describir las clases de equivalencia y el conjunto cociente. Al conjunto cociente de esta relación lo denotamos por $\mathbb{Z}/3\mathbb{Z}$ (se lee "$\mathbb{Z}$ módulo 3").*

(b) En general, fijado un entero positivo b, definimos $b\mathbb{Z} = \{bk \mid k \in \mathbb{Z}\}$ y consideramos la relación sobre $\mathbb{Z}$ dada por $(m,n) \in \mathcal{R} \Leftrightarrow m - n \in b\mathbb{Z}$. Demostrar que es una relación de equivalencia. Describir las clases de equivalencia y el conjunto cociente. Al conjunto cociente de esta relación lo denotamos por $\mathbb{Z}/b\mathbb{Z}$ (se lee "$\mathbb{Z}$ módulo b").

6) *Considerar la relación sobre $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ definida por: $(m,n)\,\mathcal{R}\,(m',n') \Leftrightarrow mn' = m'n$. Probar que es una relación de equivalencia. ¿Puedes describir las clases de equivalencia y el conjunto cociente?.*

7) *Consideramos ahora la relación sobre $\mathbb{Z}\times\mathbb{Z}$ definida por: $(m,n)\,\mathcal{R}\,(m',n') \Leftrightarrow mn' = m'n$. ¿Es esta relación una relación de equivalencia?*

8) *Considerar la relación en $\mathbb{Z}\times\mathbb{Z}$ definida por $(m,n)\,\mathcal{R}\,(m',n') \Leftrightarrow m+n' = m'+n$. Probar que es una relación de equivalencia. ¿Puedes decribir las clases de equivalencia? ¿Puedes identificar cada clase de equivalencia con los elementos de algún conjunto de forma que te ayude a describir el conjunto cociente?*

9) *Definimos en $\mathbb{Q}$ la siguiente relación: $x\,\mathcal{R}\,y \iff$ existe $h \in \mathbb{Z}$ tal que $x - y = h$. Estudiar si es una relación de equivalencia y, en caso afirmativo, describir las clases del 0 y de $1/2$, el conjunto cociente y decidir si $2/3$ y $1/3$ pertenecen a la misma clase.*

10) *Definimos en $\mathbb{Q}$ la siguiente relación: $x\,\mathcal{R}\,y \iff$ existe $h \in \mathbb{Z}$ tal que $x = \frac{3y+h}{3}$. Estudiar si es una relación de equivalencia y, en caso afirmativo, describir el conjunto cociente y decidir si $2/3$ y $4/5$ pertenecen a la misma clase.*

11) *Considerar la relación definida sobre el plano $\mathbb{R}^2$ por $(x,y)\,\mathcal{R}\,(x',y') \iff y = y'$. Probar que es una relación de equivalencia. ¿Puedes identificar cada clase de equivalencia con los elementos de algún conjunto de forma que te ayude a describir el conjunto cociente?*

12) *Considerar la relación definida sobre el plano $\mathbb{R}^2$ por $(x,y)\,\mathcal{R}\,(x',y')$ si $x - x'$ es un entero e $y - y'$ es un entero. Probar que es una relación de equivalencia. ¿Puedes identificar cada clase de equivalencia con los elementos de algún conjunto de forma que te ayude a describir el conjunto cociente?*

13) *Considerar la relación definida sobre el plano $\mathbb{R}^2$ por $(x,y)\,\mathcal{R}\,(x',y') \iff d((x,y),(x',y')) < 1$, donde d indica la distancia usual entre dos puntos del plano. Estudiar si es una relación de equivalencia y en caso afirmativo describir las clases de equivalencia.*

14) *Considerar la relación definida sobre el plano $\mathbb{R}^2$ por $(x,y)\,\mathcal{R}\,(x',y') \iff xy = x'y'$. Estudiar si es una relación de equivalencia y, en caso afirmativo, describir las clases de equivalencia.*

15) *Sea A un conjunto y B un subconjunto de A. En $\mathcal{P}(A)$ se considera la siguiente relación: Dados $X, Y \in \mathcal{P}(A)$, $X\,\mathcal{R}\,Y \iff X \cap B = Y \cap B$. Estudia*

si es una relación de equivalencia, en caso afirmativo describe el conjunto cociente.

16) *Sea S el conjunto de todos los seres humanos. Sean $x, y \in S$. Decimos que x está relacionado con y si x e y son hermanos (o sea, tienen la misma madre y el mismo padre). Probar que es una relación de equivalencia. ¿Qué son las clases de equivalencia?*

17) *Sea S el conjunto de todos los seres humanos. Sean $x, y \in S$. Decimos que x está relacionado con y si x e y tienen al menos un progenitor en común. ¿Es una relación de equivalencia? Justificar la respuesta.*

Si sustituimos la propiedad simétrica por la

Antisimétrica: $a \mathcal{R} b$ *y* $b \mathcal{R} a$ *implica que* $a = b$

diremos que tenemos una relación de orden en el conjunto X, que es una generalización, o trasunto, del conocido orden $\leq$ entre los números.

En el capítulo séptimo se estudian con detalle las relaciones de orden en un conjunto: orden total; orden parcial; cotas; extremo superior e inferior; elementos maximales; el axioma de elección, el lema de Zorn y el principio de buena ordenación; la existencia de conjuntos no medibles (Lebesgue) y la paradoja de Banach-Tarski. El tratamiento de estos últimos temas no incluirá las demostraciones, pero sí la descripción de estos interesantes hechos matemáticos y el papel que desempeñan.

1.3. Proposiciones

Este barbero afeita a todos los individuos del pueblo que no se afeitan ellos mismos: ¿se afeita el barbero a sí mismo?

B. Russell

Suele decirse que la cortesía de un matemático reside en la claridad y en la precisión. Comparado con los modos de expresión de otras disciplinas, más barrocos y caóticos, el lenguaje de las matemáticas resulta sobrio y, desde luego, preciso. No obstante, puede llegar a convertirse en una barrera difícil de franquear si se carece de la destreza adecuada para el manejo de los modos de razonamiento y de los conceptos involucrados.

Empero, el lenguaje es un asunto que permite enfoques muy distintos, uno de esos temas a los que se ha puesto de moda llamar poliédricos. Podemos

invocar, por ejemplo, la conocida frase de Galileo: "El gran libro de la naturaleza puede ser leído solo por aquellos que conocen el idioma en que está escrito, que es la Matemática". Pero también podríamos analizar su influencia en el habla cotidiana. En español tenemos expresiones tales como: salirse por la tangente; llevar vidas paralelas; tener intereses ortogonales; pasar de la alegría a la tristeza sin solución de continuidad; incurrir en círculo vicioso; desempeñar cargos homólogos; sostener que algo está tan claro como que dos y dos son cuatro; o ese multiplícate por cero, que han puesto de moda los dibujos animados de la televisión.

La etimología de los términos matemáticos es, a menudo, también muy interesante. He aquí algunos ejemplos: álgebra, del término árabe Al-jbr, que significa restauración; azar, del árabe Zahar, que significa flor, y también dado; hipotenusa, del griego hypotéinusa, participio pasado femenino de hypoteino (yo tiendo una cuerda); elipse, del griego élleipsis (insuficiencia); capicúa, del catalán cap-i-cua (cabeza y cola); logaritmo, del griego logos, razón, y de Arithmos, número; martingala, del francés Martingale, cincha del caballo; seno, del sánscrito Jya-ardha, que los indios simplificaron como Jya o Jiva, pero que escribieron en la forma jb. Posteriormente se le dio la interpretación Jaib, que significa seno, ubre, y que fue traducido al latín por sinus.

La lengua y las matemáticas son los pilares de la ilustración. El estudio de las matemáticas conlleva la adquisición, y el uso, de un lenguaje extremadamente preciso, donde no cabe la ambigüedad.

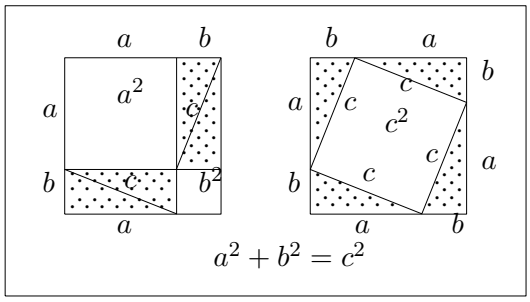
En las matemáticas se formulan proposiciones acerca de objetos tales como: números reales, funciones continuas o triángulos del plano. Son fórmulas bien hechas, para las que hay un sentido inequívoco de decir si son verdaderas o falsas. Ejemplos de proposiciones son las siguientes:

1) $\sqrt{2}$ *es un número irracional.*
2) *En un triángulo rectángulo la suma de los cuadrados de los catetos es igual al cuadrado de la hipotenusa.*
3) *Toda función continua es diferenciable en algún punto.*
4) *Todo par mayor que dos es la suma de dos números primos.*
5) $\sqrt{2}$ *es mayor o igual que* 3 *o* 3 *es mayor que* $\sqrt{2}$.
6) $\sqrt{2}$ *es mayor o igual que* 3 *y* 3 *es mayor que* $\sqrt{2}$.
7) *Existen dos números irracionales,* r *y* s*, tales que* r^s *es racional.*
8) *Existen números reales que no son computables.*
9) *Todo mapa del plano puede ser coloreado con* 4 *colores.*

Naturalmente de lo que se trata es de saber cuáles son verdaderas y cuáles son falsas.

La primera es verdadera y su demostración, como ya mencionamos en el prólogo, se encuentra en los Elementos de Euclides y se atribuye a Hipaso de Metaponto, un miembro de la escuela pitagórica, quien, según la leyenda, pagó con su vida haber hecho tan sorprendente observación que ponía en tela de juicio el principio pitagórico de que los números enteros y sus cocientes eran la esencia del Universo. El descubrimiento de la irracionalidad del número $\sqrt{2}$ (diabolus en música) fue, quizá, la primera revolución científica de la que se tiene noticia.

La segunda es el famoso Teorema de Pitágoras. He aquí una demostración (¡sin palabras!) de Chou Ching (200 años a. de C.).



La proposición 3 es falsa, pero hubo que esperar a mediados del siglo XIX *para que Weierstrass obtuviera el primer ejemplo de una función continua que carece de derivada en todos sus puntos.*

La proposición 4 es un problema abierto todavía. Fue formulado por Goldbach, y existe un premio de un millón de dólares para quien consiga su solución, es decir, decidir si es verdadera o falsa.

Las proposiciones 5 (verdadera) y 6 (falsa) son de una naturaleza distinta y mantendrían el mismo carácter aunque sustituyésemos los números $\sqrt{2}$ y 3 por cualquier otro par de números reales.

La proposición 7 es verdadera por la siguiente demostración:

Consideremos el número $(\sqrt{2})^{\sqrt{2}} = t$ y observemos que $t^{\sqrt{2}} = (\sqrt{2})^2 = 2$. Luego:

(a) *Si t es irracional, entonces la proposición 7 sería cierta tomando $r = t$, $s = \sqrt{2}$.*

(b) *Si t es racional, entonces demostraríamos la proposición 7 con $r = \sqrt{2}$ y $s = \sqrt{2}$.*

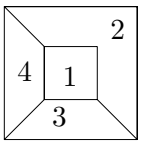
Como una de las dos alternativas, (a) o su negación, (b), tiene que ser cierta (principio del tercero excluido), podemos concluir la verdad de la proposición 7.

Observemos que la demostración se basa en el hecho de que tanto (a) como su negación (b) implican la verdad de la proposición 7 (¡sin que tengamos necesidad de saber cuál de ellas es la verdadera!).

La proposición 8 es cierta y su demostración la analizaremos más adelante, cuando estudiemos la equipotencia de conjuntos y la no numerabilidad del continuo en el capítulo 5. Por el momento digamos que un número es computable si podemos escribir un programa de ordenador que nos dé cualquier cifra que queramos de su desarrollo decimal. Comoquiera que los programas de ordenador son textos finitos con número finito de símbolos (por ejemplo las letras del alfabeto), pueden ponerse en fila por orden lexicográfico: a, b, ..., z, aa, ab, ..., zz, aaa, aab, ..., zzy, zzz, ... Por lo tanto los números computables también pueden ponerse en fila (son numerables).

Ahora bien, desde los trabajos de G. Cantor (ver capítulo 5), sabemos que los números reales, los puntos de la recta real, no son numerables, no pueden ponerse en fila y, por lo tanto, hay números reales (la mayoría) que no son computables. Luego la proposición 8 es cierta.

La proposición 9 fue, desde su formulación en el siglo XVIII *hasta que se encontró la demostración en* 1974*, una conjetura famosa, objeto del deseo de las matemáticas durante todo ese periodo. Dado un mapa del plano, formado por regiones poligonales, se trata de colorearlo de manera que dos regiones que tengan frontera común (es decir un trozo de poligonal) reciban colores distintos. El mapa siguiente demuestra que al menos cuatro colores son necesarios:*



En la otra dirección, el trabajo ingenioso de muchos matemáticos logró demostrar que 5 *colores son siempre suficientes. Pero, ¿dónde está la verdad? ¿Cuál es el número mínimo de colores que es suficiente para colorear cualquier mapa del plano?*

La respuesta es 4 *pero la demostración lograda por K. Appel y W. Haken en* 1976 *necesitó la ayuda de* 3 *ordenadores para decidir un conjunto residual, finito pero enorme, de casos. Se trata de un salto cualitativo importante en la evolución del concepto de "demostración matemática" que todavía es objeto de polémica y discusión.*

En algunas áreas especiales de las matemáticas es necesario desarrollar un lenguaje extremadamente preciso para poder discernir las sutilezas lógicas involucradas. Afortunadamente, en el resto, que incluye la actividad de la mayoría de los matemáticos, basta con unas pocas precauciones de uso del idioma común (el español en nuestro caso).

Las proposiciones, que en adelante designaremos con las letras mayúsculas en cursiva $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, ..., pueden encadenarse unas con otras, a través de las conjunciones "o", "y", de la negación "no $\mathcal{A}$" y de las frases condicionadas (implicación: $\Longrightarrow$) para dar lugar a nuevas proposiciones.

Dadas dos proposiciones $\mathcal{A}$, $\mathcal{B}$, la conjunción, o producto lógico, "$\mathcal{A}$ y $\mathcal{B}$", que designaremos también por medio del símbolo $\mathcal{A} \wedge \mathcal{B}$, es la proposición cuya verdad equivale a la de ambas, $\mathcal{A}$ y $\mathcal{B}$: $\mathcal{A} \wedge \mathcal{B}$ es verdadera si y solo si $\mathcal{A}$ es verdadera y $\mathcal{B}$ es verdadera.

Ejemplo 4: *Supongamos que $\mathcal{A}$ es la proposición "$\sqrt{2}$ es irracional" y que $\mathcal{B}$ reza "$\sqrt{2} < 3$". Entonces, $\mathcal{A} \wedge \mathcal{B}$ sería la proposición: "$\sqrt{2}$ es irracional y menor que 3".*

En este caso $\mathcal{A} \wedge \mathcal{B}$ es verdadera, porque lo son las dos proposiciones $\mathcal{A}$ y $\mathcal{B}$. Pero hubiese bastado que una de ellas fuera falsa para que también lo fuese $\mathcal{A} \wedge \mathcal{B}$. Tal es el caso de $\mathcal{A} \wedge \mathcal{C}$ siendo $\mathcal{C}$: "$\sqrt{2} < 1$". A pesar de seguir siendo $\mathcal{A}$ verdadera, $\mathcal{A} \wedge \mathcal{C}$ es falsa por serlo $\mathcal{C}$.

La suma lógica, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A}$ o $\mathcal{B}$, y, también, ora $\mathcal{A}$ ya $\mathcal{B}$. La verdad de $\mathcal{A} \vee \mathcal{B}$ conlleva que al menos una de las dos proposiciones, $\mathcal{A}$, $\mathcal{B}$, sea verdadera. Pero, ¡ojo!, puede ocurrir que ambas, $\mathcal{A}$ y $\mathcal{B}$, sean verdaderas (y, por lo tanto, también $\mathcal{A} \vee \mathcal{B}$).

Esta situación discrepa a veces del uso que la disyunción tiene en el lenguaje común. Así la expresión "lloverá o jugaremos al fútbol", suele interpretarse, normalmente, como que ocurrirá una de las dos situaciones, excluyendo la otra. Sin embargo, "bailaré con una rubia o con una chica vestida de rojo", no excluye el caso de que se den ambas circunstancias. La expresión "mañana lloverá o estará nublado", no impide tampoco que ocurran ambos fenómenos.

En el español coexisten ambos usos, excluyente y no excluyente, de la conjunción disyuntiva "o". El lenguaje matemático no puede permitirse esa ambigüedad y se opta por la versión no excluyente en todos los casos. De manera que la verdad de la proposición $\mathcal{A} \vee \mathcal{B}$ ($\mathcal{A}$ o $\mathcal{B}$), significa que una de ellas (o ambas) es verdadera.

La negación de $\mathcal{A}$ (que se designa $\neg\mathcal{A}$ o "no $\mathcal{A}$") es la proposición cuya verdad o falsedad equivale, respectivamente, a la falsedad o verdad de $\mathcal{A}$. En este caso el uso del lenguaje habitual coincide con el del matemático.

Ejemplo 5: *La negación de "$\sqrt{2}$ es irracional" sería "$\sqrt{2}$ no es irracional".*

Finalmente tenemos las proposiciones condicionadas o implicaciones, que son fundamentales en las cadenas de razonamientos que componen las demostraciones. Responden a expresiones del tipo: si $\mathcal{A}$ entonces $\mathcal{B}$ ($\mathcal{A} \Longrightarrow \mathcal{B}$, $\mathcal{A}$ implica $\mathcal{B}$). Si la proposición $\mathcal{A}$ es verdadera, entonces también lo es $\mathcal{B}$: La proposición $\mathcal{A} \Longrightarrow \mathcal{B}$ se define como $(\neg\mathcal{A}) \vee \mathcal{B}$.

Ejemplo 6: *Si todo número par mayor que 4 es la suma de dos primos, entonces todo impar mayor que 7 es la suma de tres primos.*

En este caso tenemos las proposiciones:

> $\mathcal{A}$: *"Todo par mayor que 4 es la suma de dos primos".*
> $\mathcal{B}$: *"Todo impar mayor que 7 es la suma de tres primos".*

La demostración de $\mathcal{A} \Longrightarrow \mathcal{B}$ se puede hacer de la manera siguiente:

> *Sea n un impar mayor que 7. Entonces $n-3$ es un par mayor que 4. Suponiendo que $\mathcal{A}$ es verdadera, podemos escribir $n-3=p+q$, donde p y q son números primos. Por lo tanto, $n=3+p+q$ es la suma de tres números primos.*

Obsérvese que el argumento anterior es una demostración rigurosa de $\mathcal{A} \Longrightarrow \mathcal{B}$. Sin embargo no nos dice nada acerca de si $\mathcal{A}$ o $\mathcal{B}$ son verdaderas o falsas. De hecho todavía no sabemos si $\mathcal{A}$ lo es pues se trata de la famosa conjetura de Goldbach, que sigue siendo un problema abierto. En cuanto a $\mathcal{B}$, usando métodos analíticos muy potentes, se ha demostrado que todo número impar suficientemente grande (mayor que un cierto n_0) puede escribirse como suma de tres primos. Pero las cotas obtenidas para n_0 no permiten, por ahora, abordar uno a uno los casos residuales, incluso con la ayuda del computador.

En el caso de que tengamos la doble implicación, $(\mathcal{A} \Longrightarrow \mathcal{B})$ y $(\mathcal{B} \Longrightarrow \mathcal{A})$, diremos que las dos proposiciones son equivalentes: $\mathcal{A} \Longleftrightarrow \mathcal{B}$. En esta situación la verdad o falsedad de $\mathcal{A}$ equivale, respectivamente, a la verdad o falsedad de $\mathcal{B}$.

Tablas de verdad. *Un instrumento para analizar las proposiciones compuestas de otras a través de los conectivos consiste en estudiar su tabla de verdad, es decir, la tabla de los valores $V=$ verdadero y $F=$ falso que toma cuando consideramos todas las posibilidades, V, F, de las proposiciones que la constituyen.*

Ejemplos:

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$
V	V	V
V	F	V
F	V	V
F	F	F

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$
V	V	V
V	F	F
F	V	F
F	F	F

$\mathcal{A}$	$\mathcal{B}$	$\{\mathcal{A} \Longrightarrow \mathcal{B}\} \stackrel{\text{def}}{\equiv} \{\neg\mathcal{A} \vee \mathcal{B}\}$
V	V	V
V	F	F
F	V	V
F	F	V

$\mathcal{A}$	$\neg\mathcal{A}$	$\mathcal{A} \vee (\neg\mathcal{A})$
V	F	V
F	V	V

$\mathcal{A}$	$\neg\mathcal{A}$	$\mathcal{A} \wedge (\neg\mathcal{A})$
V	F	F
F	V	F

Las dos últimas tablas resultan notables por cuanto el valor de esas proposiciones compuestas es siempre el mismo, independientemente del valor que tomen las proposiciones constituyentes: $\mathcal{A} \vee (\neg\mathcal{A})$ *es siempre verdadera (principio del tercero excluido), mientras que* $\mathcal{A} \wedge (\neg\mathcal{A})$ *es siempre falsa (principio de contradicción). Una proposición compuesta que es siempre verdadera, cualquiera que sean los valores, verdadero o falso, que tomen sus componentes, recibe el nombre de tautología.*

Dos proposiciones $\mathcal{B}$ *y* $\mathcal{C}$ *formadas a partir de las proposiciones* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *son equivalentes si ambas tienen la misma tabla de verdad. Obsérvese que en este caso tanto* $(\neg\mathcal{B}) \vee \mathcal{C}$ *como* $(\neg\,\mathcal{C}) \vee \mathcal{B}$ *son siempre ciertas. Es decir, al tener la misma tabla de verdad se verifica la doble implicación:* $\mathcal{B} \Longrightarrow \mathcal{C}$ *y* $\mathcal{C} \Longrightarrow \mathcal{B}$.

Ejemplo 7: *Las proposiciones* $\neg(\mathcal{A} \vee \mathcal{B})$ *y* $(\neg\mathcal{A}) \wedge (\neg\mathcal{B})$ *son equivalentes. Su tabla de verdad es:*

$\mathcal{A}$	$\mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\neg(\mathcal{A} \vee \mathcal{B})$	$(\neg\mathcal{A}) \wedge (\neg\mathcal{B}$
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

Ejercicios

Demostrar las siguientes equivalencias.

1) $\mathcal{A} \wedge \mathcal{B} \iff \mathcal{B} \wedge \mathcal{A}$.

2) $\mathcal{A} \vee \mathcal{B} \iff \mathcal{B} \vee \mathcal{A}$.

3) $\neg\neg\mathcal{A} \iff \mathcal{A}$.

4) $\mathcal{A} \wedge (\mathcal{B} \wedge \mathcal{C}) \iff (\mathcal{A} \wedge \mathcal{B}) \wedge \mathcal{C}$.

5) $\mathcal{A} \vee (\mathcal{B} \vee \mathcal{C}) \iff (\mathcal{A} \vee \mathcal{B}) \vee \mathcal{C}$.

6) $\mathcal{A} \wedge (\mathcal{B} \vee \mathcal{C}) \iff (\mathcal{A} \wedge \mathcal{B}) \vee (\mathcal{A} \wedge \mathcal{C})$.

7) $\mathcal{A} \vee (\mathcal{B} \wedge \mathcal{C}) \iff (\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{A} \vee \mathcal{C})$.

8) $\neg(\mathcal{A} \vee \mathcal{B}) \iff \neg\mathcal{A} \wedge \neg\mathcal{B}$.

9) $\neg(\mathcal{A} \wedge \mathcal{B}) \iff \neg\mathcal{A} \vee \neg\mathcal{B}$.

Dada $\mathcal{A} \Longrightarrow \mathcal{B}$, *la implicación* $\mathcal{B} \Longrightarrow \mathcal{A}$ *se llama su recíproca; mientras que* $\neg\mathcal{A} \Longrightarrow \neg\mathcal{B}$ *es la contraria. La implicación* $\neg\mathcal{B} \Longrightarrow \neg\mathcal{A}$ *es la contrarrecíproca.*

10) *Demostrar que toda implicación es equivalente a su contrarrecíproca.*

11) *(Modus ponens) Escribir la tabla de verdad de* $\big(\mathcal{A} \wedge (\mathcal{A} \Longrightarrow \mathcal{B})\big) \Longrightarrow \mathcal{B}$.

Si puedes mantener serena la cabeza
cuando todos la pierden y te culpen a ti.

Si aunque nadie en ti crea, te basta tu certeza,
pero dejando un margen para la duda en sí.

Si puedes esperar y no desesperarte,
y, por más que te mientan, no mentir a tu vez.

Si puedes ser odiado y no odiar por tu parte,
y no mostrar, con todo, ni orgullo ni altivez.

Si sueñas, y los sueños no te marcan el paso.
Si piensas, y la idea no es tu meta final.

Si puedes aceptar el triunfo y el fracaso,
y a esos dos impostores tratarlos por igual.

Si puedes soportar que aquello que afirmaste,
sirva, manipulado, a una oscura ambición.

O ver roto el proyecto al que tu alma entregaste,
y volver a erigirlo con el mismo tesón.

Si puedes, cuanto fuiste cosechando en la vida,
jugártelo a esa carta que te asignó el azar.

Y perder, y volver al punto de partida,
sin que nadie te escuche siquiera protestar.

Y si es tu corazón tan valiente, que puede,
cuando sin fuerzas yaces, hacerte resistir.

E impedir que claudiques cuando nada te quede,
salvo la voluntad firme que te empuja a seguir.

Si para hablarle al pueblo no bajas un peldaño,
ni al hacerlo con reyes, pierdes la sensatez.

Si ni el amor ni el odio pueden hacerte daño,
y ni a pocos complaces, ni a todos a la vez.

Si puedes rellenar el minuto vacío
con sesenta segundos que no olvides jamás,
tuyos serán los frutos de la tierra, hijo mío,
y tú serás un hombre: no se puede ser más.

Rudyard Kipling
(If)

Demostrar la verdad de la proposición $\mathcal{A}$ es equivalente a probar la falsedad de su negación, $\neg\mathcal{A}$. Esta estrategia recibe el nombre de reducción al absurdo y es un método poderoso que ya utilizaron los griegos hace veintiséis siglos en la demostración de la irracionalidad de $\sqrt{2}$.

Ejemplo 8: *$\mathcal{A}$: $\sqrt{2}$ es irracional.*

Supongamos la verdad de $\neg\mathcal{A}$: $\sqrt{2}$ es racional. Entonces existen dos enteros a, b (que podemos suponer sin factores comunes, o primos entre sí) de manera que :

$$\sqrt{2} = \frac{a}{b}.$$

Elevando al cuadrado obtenemos que $a^2 = 2b^2$, por lo que el número a tiene que ser par: $a = 2c$. Sustituyendo en la ecuación anterior obtenemos ahora la identidad: $b^2 = 2c^2$ y, por tanto, b es también un número par. Ahora bien, esto contradice la hipótesis de partida de que a y b eran primos entre sí. Luego la hipótesis de que $\neg\mathcal{A}$ es verdadera resulta ser falsa. Y la falsedad de $\neg\mathcal{A}$ es equivalente a la verdad de $\mathcal{A}$.

Analizando esta demostración encontramos dos proposiciones

$\mathcal{A}$: *$\sqrt{2}$ es irracional*

$\mathcal{B}$: *$\sqrt{2} = \dfrac{a}{b}$, donde a y b son enteros positivos primos entre sí.*

Resulta que $\mathcal{B} = \neg\mathcal{A}$ por las propiedades de la divisibilidad de los enteros. Entonces:

$$\Big(\Big\{\{(\neg\mathcal{A}) \vee \mathcal{B}\} \Longrightarrow \neg\mathcal{B}\Big\} \Longrightarrow \mathcal{A}\Big) \iff \Big(\neg\Big\{\neg\{(\neg\mathcal{A}) \vee \mathcal{B}\} \vee \neg\mathcal{B}\Big\} \vee \mathcal{A}\Big)$$
$$\iff \Big(\Big\{\{(\neg\mathcal{A}) \vee \mathcal{B}\} \wedge \mathcal{B}\Big\} \vee \mathcal{A}\Big) \iff (\mathcal{B} \vee \mathcal{A}) \iff (\neg\mathcal{A} \vee \mathcal{A})$$

que es el principio del tercero excluido, y por tanto siempre cierta.

Una ampliación importante del cálculo de proposiciones lo constituye el de predicados o funciones proposicionales. Veamos un ejemplo: dada la proposición "Carlos es madrileño", si sustituimos "Carlos" por la letra "X", obtenemos "X es madrileño", que no es una proposición en el sentido dado anteriormente al vocablo, puesto que no es verdadera ni falsa. Empero, es susceptible de convertirse en proposición cuando en vez de X pongamos un individuo concreto. Expresiones que contienen variables reciben el nombre de funciones. Funciones como la del ejemplo, tales que al sustituir la variable por un individuo se convierten en proposiciones, se llaman funciones proposicionales o predicados.

En las matemáticas tenemos abundantes ejemplos de esta situación. Por ejemplo la ecuación

$$x^2 - 3x + 2 = 0 \text{ tiene las raíces } x = 1 \text{ y } x = 2.$$

Luego si nuestro universo es el conjunto de los números reales, el predicado "$x^2 - 3x + 2 = 0$" se convierte en una proposición verdadera si sustituimos x por los números 1 o 2, y en falsa para los demás casos.

Dado un conjunto $\mathcal{U}$ (universo) y un predicado $\mathcal{A}(x)$ podemos definir el conjunto de verdad:

$$V(\mathcal{A}(x)) = \{u \in \mathcal{U} \,:\, \mathcal{A}(u) \text{ es verdadera}\}.$$

De esta manera establecemos un diccionario para trasladar problemas del cálculo de predicados al álgebra de los subconjuntos de $\mathcal{U}$, y viceversa.

De particular importancia son los cuantificadores:

El cuantificador existencial ($\exists$) postula la existencia de un elemento x del universo $\mathcal{U}$ tal que $\mathcal{A}(x)$ es cierta:

$$\exists x \in \mathcal{U}\ \mathcal{A}(x) \text{ es cierta.}$$

Dicho de otro modo: el cuantificador existencial predica que

$$V(\mathcal{A}(x)) \neq \emptyset.$$

El cuantificador universal ($\forall$) nos dice que para todo elemento $x \in \mathcal{U}$, $\mathcal{A}(x)$ es cierta:

$$\forall x \in \mathcal{U}\ \mathcal{A}(x) \text{ es cierta} \iff V(\mathcal{A}(x)) = \mathcal{U}.$$

<u>Notación:</u> Cuando en el cuantificador existencial se quiere precisar que existe un único elemento, se usa el símbolo $\exists\,!\,x$ que se lee "existe un único x"

$$\exists\,!\,x\,\mathcal{A}(x) \ :\equiv:\ \big(\exists x\,\mathcal{A}(x)\big) \wedge \Big(\big(\forall x\,\forall y\,(\mathcal{A}(x) \wedge \mathcal{A}(y))\big) \implies x = y\Big)$$

Ejercicios

Estudiar la verdad o falsedad de las proposiciones siguientes:

1) $\forall x \in \mathbb{R}$, $2x \geq x$, *($\mathbb{R}$ = números reales).*

2) $\forall x \in \mathbb{N}$, $3x \geq x$, *($\mathbb{N}$ = números naturales).*

3) $\exists x \in \mathbb{R}$, $x^2 = 2$.

4) $\exists x \in \mathbb{Q}$, $x^2 = 2$, *($\mathbb{Q}$ = números racionales).*

5) $\forall x$, $\exists\,!\,y$, $y = x^4$, $x, y \in \mathbb{R}$.

6) $\forall x \in \mathbb{R}$, $x^3 + 7x^2 + 1 \geq 0$.

7) *Escribir, usando los símbolos* $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\exists$, $\forall$, $\in$, $\subset$, $\cap$, $\cup$, *los silogismos aristotélicos:*

i) Barbara: Para todos $\mathcal{A}$, $\mathcal{B}$ *y* $\mathcal{C}$*: si cada* $\mathcal{B}$ *es* $\mathcal{C}$ *y cada* $\mathcal{A}$ *es* $\mathcal{B}$*, entonces todo* $\mathcal{A}$ *es* $\mathcal{C}$*.*

ii) Celarent: Para todos $\mathcal{A}$, $\mathcal{B}$ *y* $\mathcal{C}$*: si ningún* $\mathcal{B}$ *es* $\mathcal{C}$ *y cada* $\mathcal{A}$ *es* $\mathcal{B}$*, entonces ningún* $\mathcal{A}$ *es* $\mathcal{C}$*.*

iii) Darii: Para todos $\mathcal{A}$, $\mathcal{B}$ *y* $\mathcal{C}$*: si cada* $\mathcal{B}$ *es* $\mathcal{C}$ *y algún* $\mathcal{A}$ *es* $\mathcal{B}$*, entonces algún* $\mathcal{A}$ *es* $\mathcal{C}$*.*

iv) Ferio: Para todos $\mathcal{A}$, $\mathcal{B}$ *y* $\mathcal{C}$*: si ningún* $\mathcal{B}$ *es* $\mathcal{C}$ *y algún* $\mathcal{A}$ *es* $\mathcal{B}$*, entonces algún* $\mathcal{A}$ *no es* $\mathcal{C}$*.*

8) *Lo mismo que en el ejercicio anterior pero con los restantes silogismos: Cesare, Camestres, Festino, Baroco, Darapti, Disamis, Datisi, Felapton, Bocardo, Ferison.*

9) *Construye las tablas de verdad de las proposiciones:*
a) $\neg S$; *b)* $\neg(\neg S)$; *c)* $S \wedge T$; *d)* $S \vee T$; *e)* $S \implies T$;
f) $S \iff T$; *g)* $(S \vee T) \wedge V$.

10) *Construye las tablas de verdad de las siguientes proposiciones:*
a) $(S \wedge T) \vee \neg(S \vee T)$; *b)* $(S \vee T) \implies (S \wedge T)$;
c) $(\neg S \vee T) \iff \neg(S \wedge \neg T)$; *d)* $(S \wedge \neg T) \implies (T \wedge \neg S)$.

11) *Observa que las cuatro proposiciones del ejercicio anterior se expresan en función de variables proposicionales* S, T*. Por otro lado el valor de verdad de cada proposición depende de los valores de sus variables. Decimos que una proposición en variables* S, T, V, $\ldots$ *es una* tautología *cuando es verdadera cualesquiera sean los valores de verdad de las variables; y decidimos que es una* contradicción *cuando es falsa cualesquiera sean los valores de verdad de las variables.*

¿Es alguna de las proposiciones anteriores una tautología?

12) *Comprueba que la proposición*

$$\big((P \implies Q) \wedge \neg Q\big) \wedge \big(Q \vee \neg(\neg R \implies \neg P)\big)$$

es una contradicción.

13) *Decir cuáles de las siguientes condiciones son* necesarias *y cuáles* suficientes *para que un número natural* n *sea divisible por* 6.

a) n *es divisible por* 3;
b) n *es divisibles por* 12;
c) $n = 24$;
d) n^2 *es divisible por* 6;
e) n *es par y divisible por* 3;
f) n *es par o divisible por* 3.

14) *¿Cuáles de las siguientes afirmaciones son verdaderas? ¿Cuáles son falsas? Justifica las respuestas:*

a) *Si* $3 \cdot 2 = 6$ *y* $4 + 4 = 8$, *entonces* $5 \cdot 5 = 20$.

b) *Si no ocurre que* $3^2 = 8$, *entonces* $4^2 = 16$.

c) *Si no ocurre que* $3^2 = 9$, *entonces* $4^2 = 16$.

d) *Si* $3 \cdot 2 = 6$ *y* $4 + 4 = 7$, *entonces* $5 \cdot 5 = 20$.

15) *Demuestra la equivalencia (lógica) de los siguientes pares de proposiciones:*

a) $S \wedge T$ *es equivalente a* $T \wedge S$.

b) $S \vee T$ *es equivalente a* $T \vee S$.

c) $\neg(\neg S)$ *es equivalente a* S.

d) $(S \wedge T) \wedge V$ *es equivalente a* $S \wedge (T \wedge V)$.

e) $(S \vee T) \vee V$ *es equivalente a* $S \vee (T \vee V)$.

f) $\neg(S \wedge T)$ *es equivalente a* $\neg S \vee \neg T$.

g) $\neg(S \vee T)$ *es equivalente a* $\neg S \wedge \neg T$.

h) $S \wedge (T \vee V)$ *es equivalente a* $(S \wedge T) \vee (S \wedge V)$.

i) $S \vee (T \wedge V)$ *es equivalente a* $(S \vee T) \wedge (S \vee V)$.

16) *Demuestra que* $S \implies T$ *es equivalente a* $\neg S \vee T$ *y que* $S \implies T$ *es equivalente a* $\neg T \implies \neg S$.

17) *Para cada una de las siguientes proposiciones, formula una lógicamente equivalente usando solo* S, T, $\neg$ *y* $\vee$. *(Se pueden usar tantos paréntesis como sean necesarios.)*

a) $S \implies \neg T$, b) $S \wedge (T \vee \neg S)$,

c) $(S \Rightarrow T) \vee (T \Rightarrow S)$, d) $[\neg(S \vee T)] \Rightarrow S$.

18) *Sean* A, B, C *tres proposiciones para las que podemos probar que* $A \Rightarrow B$ *y* $B \Rightarrow C$ *son verdaderas. Demuestra que también es verdadera* $A \Rightarrow C$. *¿Podemos deducir algo sobre la verdad o falsedad de* A, B *o* C*?*

19) *Sabiendo que* $P \implies Q$ *es verdadero y que también es verdadero* $P \vee Q$, *¿se puede concluir que* P *es verdadero?*

20) *En las siguientes proposiciones x, y son variables en $\mathbb{R}$ (el universo consiste en el conjunto de los números reales). Traduce cada una de ellas a frases. Las respuestas no deben contener ningún símbolo, solo palabras. (Las fórmulas de este ejercicio son todas verdaderas, pero no se pide su verificación.)*

a) $\forall x\,((x > 0) \Rightarrow \exists y\,(y > 0 \wedge y^2 = x))$
b) $\exists x \forall y\,((y > x) \Rightarrow (y > 5))$
c) $\neg\exists x\,(1 < x^2 < x)$
d) $\forall y \exists x\,(x \in \mathbb{R} \wedge x^3 = y + 1)$.

21) *Escribe la negación de las proposiciones del ejercicio anterior.*

22) *Traduce cada una de las siguientes afirmaciones a símbolos y cuantificadores. Las respuestas no deben contener palabras.*

a) El número 5 tiene una raíz cuadrada positiva.

b) Todo número real positivo tiene dos raíces cuartas reales y distintas.

23) *Explica por qué son verdaderas cada una de las siguientes proposiciones para cada número natural* $x \leq 6$.

a) $x > 2 \implies 2x > 4$

b) $x^2 + 1 = 0 \implies x^2 + 2 < 0$

c) $x^2 + 1 < 0 \implies x = 3$

d) $x^2 - 4x + 4 = 0 \implies x > 1$.

24) *Razona con palabras por qué los siguientes pares de afirmaciones no son equivalentes en los números naturales.*

a) $\forall x \exists y\,(x = 2y \vee x = 2y + 1)$ *y* $\exists x \forall y\,(x = 2y \vee x = 2y + 1)$

b) $\forall x \exists y$, $x < y < x + 2$ *y* $\exists x \forall y$, $x < y < x + 2$.

25) *¿Cuáles de las siguientes afirmaciones son verdaderas? (El universo asociado a las variables se da entre corchetes.)*

a) $\forall x\,(x + 1 \geq x)$, *[*$\mathbb{R}$*]*

b) $\exists x\,(2x + 3 = 5x + 1)$, *[*$\mathbb{N}$*]*

c) $\exists x\,(x^2 + 1 = 2^x)$, *[*$\mathbb{R}$*]*

d) $\exists x\,(x^2 = 2)$, *[*$\mathbb{R}$*]*

e) $\exists x\,(x^2 = 2)$, *[*$\mathbb{Q}$*]*

f) $\forall x\,(x^3 + 17x^2 + 6x + 100 \geq 0)$, *[*$\mathbb{R}$*]*

g) $\exists x\,(x^3 + x^2 + x + 1 \geq 0)$, *[*$\mathbb{R}$*]*

h) $\forall x \exists y\,(x + y = 0)$, *[*$\mathbb{R}$*]*

i) $\exists x \forall y\,(x + y = 0)$, *[*$\mathbb{R}$*]*

j) $\forall x \exists y \forall z\,(xy = xz)$, *[*$\mathbb{R}$*]*

k) $\forall x \exists y\,(x \geq 0 \Rightarrow y^2 = x)$, *[*$\mathbb{R}$*]*

l) $\forall x \exists y\,(x \geq 0 \Rightarrow y^2 = x)$, *[*$\mathbb{N}$*]*

En el capítulo 8 volveremos a estos asuntos de la lógica matemática. Las paradojas que aparecieron en la teoría "ingenua" de conjuntos llevaron a la construcción de "teorías axiomáticas formales" y a la búsqueda de sistemas de axiomas consistentes, independientes y completos. En matemáticas no puede haber ignorabimus, según frase famosa de Hilbert. Pero K. Gödel, con su famoso teorema de incompletitud, puso final al gran sueño reduccionista. De ahí surgió la "Teoría de la computación" de A. Turing, y en eso andamos.

1.4. Falacias

> *... el no haber caído, cuando me interesé por la filosofía, en manos de ningún sofista, ni haberme entregado a los autores, ni resolver silogismos, ni ocuparme de la mecánica celeste. Pues todo eso requiere de los dioses y de la fortuna.*
>
> Marco Aurelio
> *(Meditaciones)*

Toda demostración matemática involucra cadenas de razonamientos engarzados de forma precisa, siendo cada nueva proposición deducida de las anteriores. Pero el discurso cotidiano está lleno de falacias, algunas son de naturaleza lógica o sintáctica, otras son materiales o semánticas. He aquí algunos ejemplos.

- *Argumento "ad hominem", muy común entre ciertos políticos, que consiste en hablar en contra del oponente en vez de refutar lo que este haya dicho: "Váyase Sr. González"; "Ud. Sr. presidente del gobierno es un tahúr del Mississippi"; "Y tú, enano, habla castellano".*
- *"Secundum quid": "A dicto simpliciter ad dictum secundum quid". De un dicho tomado muy a la ligera, con demasiada simplicidad: de que en España haya corridas de toros no puede deducirse que todos los españoles seamos toreros.*
- *"Ad verecundiam": Querer probar una proposición basándose en la autoridad de las personas que la sustentan. Muy utilizado entre los padres de las diversas iglesias.*

- *"Ad ignorantiam": Cuando se intenta probar que algo es de una forma porque nadie haya podido probar que no lo sea. Como la prueba del presidente Bush de la existencia de las famosas armas de destrucción masiva en Irak.*
- *"Ad populum": Poner la atención en los gustos y opiniones de la gente en vez de en la lógica de los argumentos.*

  Incluso entre los científicos se ha puesto de moda enjuiciar el valor de un obra a través de índices de impacto o número de citas, y existen agencias especializadas en su confección:

Original jamás tuvo una idea,
mas presume de mil publicaciones
repitiendo unas pocas opiniones
que aburren a cualquiera que las lea.

Conviene publicar un disparate,
tan obsceno que ofenda de ipso facto.
Te darán un gran índice de impacto
los ingenuos que miren tu dislate.

Resolver los problemas no desea,
sino seguir alzando sus opciones,
con citas de un hatajo de bufones
de pillar las prebendas de la aldea.

No importa si es con cuerdo o botarate,
de citas mutuas sellarás un pacto.
Aunque sean banales y sin tacto
juntas harán lucir tu escaparate.

Trivialidad de tal naturaleza,
hipótesis que mudan cada rato,
teoremas de estúpida simpleza.

No intentes un problema complicado
si el ritmo frena en tus publicaciones:
pues debes mantenerlo acelerado.

Si, viendo tanto plagio sin recato,
el gran Gauss levantara la cabeza,
en su sitio pondría al insensato.

En alza tengas siempre tus opciones
de rozar el poder en el poblado,
con índices y citas a montones.

- *"Ad baculum": Por intimidación, por la fuerza. Muy usado por la Inquisición en sus juicios y autos de fe. Y por los terroristas para convencernos de sus razones.*
- *"Círculo vicioso": Ocurre cuando la premisa presupone, de forma abierta o encubierta, la conclusión que se quería demostrar. Una variante consiste en probar que:*

$$p_1 \Longrightarrow p_2 \Longrightarrow p_3 \Longrightarrow \ldots \Longrightarrow p_n \Longrightarrow p_1,$$

  y concluir que todas las proposiciones son ciertas en vez de que todas son equivalentes, que es lo correcto: Nosotros somos más listos que ellos, por lo que nos damos más cuenta que ellos de lo que pasa y, en consecuencia, cometemos muchos menos errores, es decir, somos más listos que ellos.
- *"Equiparar" significados distintos de los términos involucrados. Falacia que es muy común en el discurso de los políticos, especialmente en todo ese embrollo de naciones, regiones, nacionalidad, razas, etnias, pueblos,*

tribus y demás. Como en un trabalenguas que pregunta por qué son iguales, o en qué se parecen, dos cosas muy distintas. Por ejemplo: ¿Por qué son iguales un gato y un triángulo rectángulo?

El gato persigue al ratón. El ratón se come el queso. El queso se hace de la leche. La leche la da la vaca. La vaca es una res. Res en catalán significa nada. El que nada no se ahoga. El que no se ahoga flota. La flota es una escuadra. Y la escuadra es un triángulo rectángulo.

- *"Post hoc, ergo propter hoc": Consiste en proponer que algo que ha ocurrido después de una acción sea consecuencia suya: "Puesto que ha llovido después de la procesión, es que esta ha provocado la luvia".*
- *"Confundir el consecuente con el antecedente": De $\mathcal{A} \Longrightarrow \mathcal{B}$ no puede deducirse que $\mathcal{B} \Longrightarrow \mathcal{A}$. Es el error de confundir los síntomas con las causas: La meningitis produce fiebre pero un enfermo febril no tiene, necesariamente, que padecer meningitis.*

1.5. Funciones

He quemado mis largas horas
en la lumbre de símbolos y fórmulas.
Junto a crisoles de arcilla al rojo vivo
hasta encontrar la plata.

María Cegarra
(Cristales míos)

El concepto de función es fundamental en todas las ciencias. En cada teoría matemática hay que determinar cuáles son los conjuntos y funciones relevantes. El Álgebra Lineal considera espacios vectoriales y las funciones lineales; en la Teoría de grupos los conjuntos son los grupos y las funciones, los homomorfismos (que conservan las operaciones); en Topología tenemos los conjuntos abiertos y las funciones continuas; etc.

Un ejemplo notable son los polinomios y las fracciones algebraicas, tales como:

$$y = \frac{x^2 - 3x + 7}{x + 1}. \tag{1.1}$$

Si sustituimos la letra x por el número 2, obtenemos el valor $y = 5/3$. Mientras que si hacemos $x = 3$, resulta que $y = 7/4$. Diremos que $5/3$ (resp. $7/4$) es el valor que toma la función en $x = 2$ (resp. $x = 3$).

La fracción algebraica nos proporciona un truco o maquinaria capaz de asignar a cualquier número x un valor de y. ¿A cualquier x? Bueno, no a todos, ya que si tomamos $x = -1$ nos encontramos con que el denominador se anula y nosotros no sabemos dividir por el número cero.

Pero si exceptuamos ese caso patológico de $x = -1$, la fracción algebraica funciona maravillosamente y para cada elemento de su dominio de definición, es decir a cada número real distinto de -1, la fórmula (1.1) nos da un único valor de y.

Consideremos los números primos:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,$$
$$59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, \ldots$$

Sea $\pi(x)$ el número de primos menores o iguales que x: $\pi(1) = 0$, $\pi(7{,}5) = 4$, $\pi(20) = 8$, ...

Ejercicio 2. *Calcular los valores de $\pi(40)$, $\pi(65)$ y $\pi(200)$. Elabora una tabla de primos hasta 1000 y comprueba en ella la propiedad:*

$$\pi(2x) - \pi(x) \geq 1 \quad si\ x \geq 1.$$

Sin embargo, el concepto de función es más amplio que el de una mera relación numérica: el color del cielo depende de la nubosidad; la subida de los precios del petróleo es función de la estabilidad política del Oriente Medio; la cotización de las bolsas españolas en el año 1994 reflejó los descubrimientos de casos de corrupción política; las posibilidades de Miguel Indurain aumentaban con el número de etapas "contra el reloj"... Expresiones como estas aparecen con frecuencia en los medios de comunicación de masas. La palabra función, que proviene del latín "functio", que deriva del verbo "fungere" (que significa "cumplir"), impregna nuestro lenguaje: dio las órdenes en el ejercicio de sus funciones; la función de los estudiantes es aprender; las funciones de la nutrición; una función de circo o de iglesia; la función crea el órgano, etc., son frases corrientes de nuestro idioma.

A cada entero positivo n le asignamos $d(n)$ el número de sus divisores positivos: $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(10) = 4$, $d(30) = 8$, ... ¿Cómo se llaman los números cuya imagen por esta función es 2? ¿Podrías describir a los números n tales que $d(n) = 4$?

La mayor parte de las fórmulas matemáticas involucran a funciones: a cada círculo del plano le podemos asignar su área, o la longitud de su circunferencia; a cada polígono, su número de lados; podemos considerar el número de primos que son menores que una cantidad x dada, $\pi(x)$; a cada natural n le podemos asociar el número de sus divisores, $d(n)$; etcétera.

Las leyes de la Física son también ejemplos de funciones: el volumen de un gas encerrado en un cilindro es una función de su temperatura y de la presión que ejerzamos sobre él. La música de un violín puede ser analizada y expresada con unas funciones especiales; la propagación del calor, de la luz

y los movimientos de los cuerpos celestes se entienden y explican por medio de funciones adecuadas.

La función $\sigma(n)$ asigna a cada entero positivo la suma de sus divisores positivos: $\sigma(1) = 1$, $\sigma(2) = 1+2 = 3$, $\sigma(4) = 1+2+4 = 7$, $\sigma(7) = 1+7 = 8$, $\sigma(28) = 56$, ...

Obsérvese que p es un número primo si y solo si $\sigma(p) = p+1$. Los números n tales que $\sigma(n) = 2n$ se llaman perfectos: 6, 28, 496, 8.128 y 33.550.336, son números perfectos. ¡Nadie sabe si hay algún número perfecto impar!

La noción de función. *Los términos función, aplicación y transformación, son sinónimos y significan lo siguiente: A cada elemento x de un conjunto D, llamado conjunto de partida o dominio de la función, le asignamos un único elemento y de un conjunto E de llegada de la transformación.*

Es costumbre escribir $y = f(x)$ para designar a una función. Esta consta, pues, de un conjunto de salida D (o dominio), de un conjunto de llegada E, y de un "truco o maquinaria", f, que asigna a cada elemento de D un único elemento de E.

Ejemplo 9: *Sean D = conjunto de los españoles; E = conjunto de pueblos del mundo; y consideremos la función:*

$$y = f(x) = \text{ lugar de nacimiento.}$$

Algunas evaluaciones serían:

$$\begin{aligned} f(\text{Sta. Teresa de Jesús}) &= \text{Ávila} \\ f(\text{S. Juan de la Cruz}) &= \text{Fontiveros} \\ f(\text{Pablo Picasso}) &= \text{Málaga} \\ f(\text{Severo Ochoa}) &= \text{Luarca} \\ f(\text{Cristóbal Colón}) &= \text{Génova} \\ f(\text{Juan Ramón Jiménez}) &= \text{Moguer} \\ f(\text{Francisco de Goya}) &= \text{Fuendetodos} \\ f(\text{Diego Velázquez}) &= \text{Sevilla} \\ f(\text{Santiago Ramón y Cajal}) &= \text{Petilla de Aragón} \\ \dots &\quad \dots \end{aligned}$$

El conjunto imagen, $f(D)$, está constituido por todos los elementos de E que son imágenes de algún elemento de D. El conjunto imagen $f(D)$, que a veces también se designa con la notación $\mathrm{Im}(f)$, no tiene por qué coincidir con el conjunto E, en general, y será solo una parte suya. Siguiendo con ese afán de reducir todas las definiciones a la noción primaria de conjunto, podemos también decir que una función definida en D con valores en E es un subconjunto A del producto cartesiano $D \times E$ con la propiedad de unicidad siguiente: si $(x, z) \in A$ y $(x, w) \in A$ entonces $z = w$.

Ejemplos: *a) Consideremos la función* $y = x^2$, *definida en* $D = \mathbb{R}$ *(los números reales), y que toma valores en* $E = \mathbb{R}$.

$$\mathrm{Im}(f) = f(\mathbb{R}) = \text{ números reales no-negativos.}$$

b) Por el contrario, la función $y = f(x) = x^3$ *sí verifica que*

$$\mathrm{Im}(f) = f(\mathbb{R}) = \mathbb{R}$$

pues todo número real tiene una raíz cúbica real.

c) Definimos $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *mediante la regla* $f(n) =$ *resto obtenido al dividir* n *por* 7: $f(8) = 1$, $f(10) = 3$, $f(28) = 0$, $f(-4) = 3$, $f(123) = 4$, ... *¿Quién es el conjunto* $\mathrm{Im}(f) = f(\mathbb{Z})$? *Obsérvese que* $f(m) = f(n)$ *si y solo si* $m - n$ *es un múltiplo de* 7.

Cuando el conjunto imagen coincide con el conjunto de llegada, es decir, cuando todo elemento de E *es la imagen de, por lo menos, un elemento de* D, *diremos que la función es suprayectiva, sobreyectiva o simplemente "sobre".*

La notación $f : D \longrightarrow E$ *es también usada a menudo para designar la maquinaria funcional. Asimismo, es costumbre escribir* $x \overset{f}{\longmapsto} y$ *en vez de* $y = f(x)$, *para indicar que* y *es la imagen de* x *por medio de la función* f.

Hay funciones que siempre asignan imágenes distintas a elementos distintos. Se denominan inyectivas o simplemente "in".

Ejemplo 10: *La aplicación* $x \longmapsto x^3$ *de los números reales en sí mismos es inyectiva, puesto que si* $a^3 = b^3$, *entonces, necesariamente, los números reales* a *y* b *deben coincidir:* $a = b$.

También son inyectivas las funciones $x \longmapsto 7x$; $x \longmapsto 13\,x^5$; *y si la Administración no tuviese errores*

$$\begin{array}{rcl} f : \{\text{españoles mayores de 14 años}\} & \longrightarrow & \mathbb{N} \\ x & \longmapsto & f(x) = \text{ número del D.N.I.} \end{array}$$

Por el contrario la función $x \longmapsto x^2$ *no es inyectiva, considerada como función de los números reales en sí mismos, porque tanto* x *como* $-x$ *tienen la misma imagen,* x^2: $(-5)^2 = 25 = 5^2$, ...

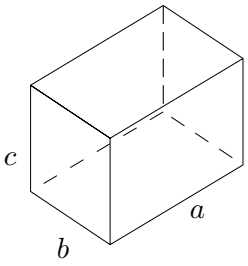
Pregunta: *¿Es inyectiva la función* $f(x) =$ *lugar de nacimiento de* x?, *¿es sobreyectiva?*

Consideremos la función número de divisores de un número, $d(n)$, *cuyo dominio son los enteros positivos*

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\},$$

y cuyo conjunto de llegada es también $\mathbb{Z}^+$. ¿Es d inyectiva? La respuesta es que no: $d(2) = d(3) = d(5) = \cdots = 2$, esto es, existen elementos distintos con la misma imagen. ¿Es d sobreyectiva? Sí lo es, puesto que $d(2^{n-1}) = n$.

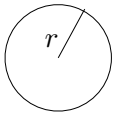
Consideremos la fórmula $V = a \cdot b \cdot c$, que a cada terna de números reales positivos, (a, b, c), le hace corresponder su producto, V. Si a, b, c son, respectivamente, el largo, ancho y alto de un prisma recto rectangular, entonces V es el volumen.



¿Es inyectiva? ¿Es sobreyectiva? (como conjunto de llegada se considera el de los reales positivos).

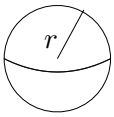
Las fórmulas que siguen son ejemplos de funciones importantes de la Geometría.

Área del círculo de radio r: $S = \pi r^2$
Longitud de la circunferencia de radio r: $L = 2\pi r$



Volumen de la esfera de radio r:

$$V = \frac{4}{3}\pi r^3$$

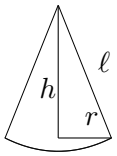


Superficie de la esfera de radio r:

$$S = 4\pi r^2$$

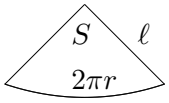
Volumen del cono de radio x y altura h:

$$\begin{aligned} V(r,h) &= \frac{1}{3}\pi r^2 h \\ \ell &= \sqrt{h^2 + r^2}. \end{aligned}$$



Área lateral del cono de radio x y altura h:

$$S = \pi r \ell = \pi r \sqrt{r^2 + h^2}.$$



Hay funciones que son a la vez inyectivas y suprayectivas: cada elemento del conjunto de llegada E es la imagen de un único elemento del dominio. Un ejemplo es la función $x \longmapsto x^3$, que ya hemos considerado antes, en la que $D = E =$ conjunto de los números reales.

Estas aplicaciones que son inyectivas y suprayectivas se llaman biyectivas; también se dice que son una biyección entre los conjuntos de partida y de llegada, y que estos conjuntos, D y E, están en correspondencia biyectiva.

En el caso de que ambos conjuntos, D y E, tengan un número finito de elementos, entonces, la existencia de una biyección entre ellos implica, necesariamente, que sus cardinales coinciden. Esto es válido también para conjuntos infinitos, pero esa discusión nos llevaría a un terreno muy delicado, que es la teoría de los cardinales, y que dejaremos para exploraciones futuras.

Sin embargo, conviene notar que si un conjunto tiene infinitos elementos puede entonces ponerse en correspondencia biyectiva con una de sus partes propias.

Ejemplo 11: *Sean los conjuntos:*

$$\begin{aligned} \mathbb{N} = \{0,1,2,3,4,\dots\} &= \textit{naturales} \\ P = \{0,2,4,6,8,\dots\} &= \textit{números pares} \end{aligned}$$

$$\begin{aligned} \textit{y tomemos la función} \qquad f : \mathbb{N} &\longrightarrow P \\ x &\longmapsto 2x. \end{aligned}$$

Resulta que f es una biyección[**] entre $\mathbb{N}$ y P, a pesar de que P sea un subconjunto propio de $\mathbb{N}$ (le faltan los impares).

Por el contrario, si A tiene solo un número finito de elementos, entonces A no está en biyección con ningún subconjunto propio.

En el caso de una aplicación biyectiva $f : D \longrightarrow E$ podemos definir la función inversa, $f^{-1} : E \longrightarrow D$, por medio de la fórmula:

$$f^{-1}(y) = x \textit{ si y solo si } y = f(x).$$

Ejemplos: *1) $D = E = \mathbb{Q}$ (números racionales). Sea $f(x) = 7x$. Se tiene que f es biyectiva y su función inversa es*

$$f^{-1}(y) = \frac{1}{7}\, y.$$

2) Sea $D = E = \mathbb{R}$ y $f(x) = x^3$, entonces

$$f^{-1}(y) = \sqrt[3]{y}$$

es la única raíz cúbica real del número y.

3) Sea $D = \mathbb{R}$ y $E = \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, entonces $y = e^x$ es una aplicación biyectiva de D en E cuya inversa es $x = \log y$, logaritmo natural o neperiano.

[**] En la teoría de los cardinales, dos conjuntos tienen el mismo cardinal, $\text{card}(A) = \text{card}(B)$, si existe una biyección entre ambos. En este sentido, $\text{card}(\mathbb{N}) = \text{card}(P)$. Sin embargo, resulta que $\mathbb{N}$ (los naturales) y $\mathbb{R}$ (los reales) tienen "cardinales infinitos" distintos.

Dadas dos funciones $f_1 : D_1 \longrightarrow E_1$, $f_2 : D_2 \longrightarrow E_2$, *si resulta que*

$$\mathrm{Im}(f_1) \subset D_2$$

podemos componer ambas funciones, $(f_2 \circ f_1)$ *de la manera siguiente:*

$$f_2 \circ f_1(x) = f_2(f_1(x)).$$

Es decir, dado un elemento $x \in D_1$, *primero aplicamos* f_1, *para obtener un elemento* $f_1(x) \in \mathrm{Im}(f_1) \subset D_2$ *(por la hipótesis de partida). Es entonces legítimo aplicar* f_2 *a* $f_1(x)$ *para obtener el valor de la función compuesta,* $f_2 \circ f_1 : D_1 \longrightarrow E_2$*:*

$$f_2 \circ f_1(x) = f_2(f_1(x)).$$

La composición de funciones es un mecanismo muy importante de generación de funciones complicadas a partir de elementos simples. Las matemáticas están llenas de expresiones tales como:

$$y = \log\left(\sqrt{1 + (\cos^2 x)\, e^{x^2}}\right)$$

que son funciones compuestas. El procedimiento de la composición se puede iterar muchas veces, de manera que, en lo sucesivo, nos encontraremos con composiciones múltiples:

$$f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1.$$

Una cuestión importante, en cada teoría, es discernir qué propiedades de las funciones f_i *hereda su composición. Por ejemplo: la composición de funciones lineales es lineal; la composición de funciones continuas es continua; la composición de funciones diferenciables es diferenciable y además tenemos la fórmula (regla de la cadena):*

$$\big(f_2 \circ f_1\big)'(x) = f_2'(f_1(x)) \cdot f_1'(x).$$

Estas afirmaciones, que son teoremas en cada una de sus respectivas teorías, son muy útiles, por cuanto nos permiten estudiar funciones complicadas, tales como:

$$y = \log\sqrt{1 + e^x \cosh\left(x^2\right)} \,+\, \mathrm{senh}(x),$$

reduciéndolas al estudio de sus componentes más sencillas.

Según nuestra definición de función necesitamos tres ingredientes: un conjunto de partida o dominio, D; un conjunto de llegada, E; y un "truco" o procedimiento, f, para asignar a cada elemento de D una imagen en E. Por lo tanto, en sentido estricto, la fórmula

$$y = \frac{x}{x^2 - 7}$$

no es una función hasta que expliquemos cuál es su dominio (y su rango o conjunto imagen). No obstante, la tradición, que es buena mientras no produzca demasiada confusión, impone cuestiones del tipo: "¿Cuál es el dominio, en $\mathbb{R}$, de la función $y = \frac{x}{x^2-7}$?" En realidad, de lo que se trata es de encontrar el mayor subconjunto de los reales donde la fórmula tenga sentido y nos dé un valor de y para cada uno de x. En este ejemplo particular el dominio resulta ser: $D = \mathbb{R} - \{+\sqrt{7}, -\sqrt{7}\}$.

Aparte del dominio, y de la imagen, de una función, $f : D \longrightarrow E$, existe otro conjunto importante asociado y que es muy útil en el estudio de las funciones.

Definición. *El grafo o la gráfica de f es el conjunto de las parejas $(a, f(a))$, donde a recorre el dominio D:*

$$Graf(f) = \Big\{(a, f(a)) \mid a \in D\Big\}.$$

Así, el grafo de f, $Graf(f)$, es un subconjunto del producto cartesiano $D \times E$, que es el conjunto de todos los pares ordenados (a, b), $a \in D$ y $b \in E$.

Dada una función, $f : D \longrightarrow E$, tenemos pues los conjuntos:

$$\begin{aligned} \mathrm{Im}(f) &= \big\{y \in E \mid y = f(x) \text{ para algún } x \in D\big\} \\ Graf(f) &= \big\{(x, f(x)) \in D \times E \mid x \in D\big\}. \end{aligned}$$

También son interesantes los llamados conjuntos de nivel:

$$f^{-1}(y) = \big\{x \in D \mid f(x) = y\big\}.$$

El nombre de conjunto de nivel proviene del caso: $f : D \longrightarrow \mathbb{R}$, donde el dominio $D \subset \mathbb{R}^2$ es una región, y $z = f(x, y)$ es, por ejemplo, la altura sobre el nivel cero (nivel del mar) del punto de la superficie terrestre de coordenadas (x, y) (longitud, latitud). Entonces, $f^{-1}(z)$ es la "curva" de nivel z: los puntos que están a altura z. Esta función es muy importante en los mapas topográficos. En otros ámbitos tenemos las líneas isobaras, isotermas, etcétera.

Ejemplo 12: *Sea* $f(x,y) = x^2 + y^2$, *entonces* $f^{-1}(1) =$ *circunferencia de radio* 1 *centrada en el origen de coordenadas.*

Un conjunto puede ser descrito en alguna de estas tres formas, o en varias de ellas. Un ejemplo es C, *la circunferencia unidad del plano:*

(1) $C = f^{-1}(1) = \{(x,y) = \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ *donde* $f(x,y) = x^2 + y^2$.

Cuando un conjunto está descrito de esta forma, como un conjunto de nivel, se dice que viene dado de forma implícita.

(2) $C = \{(\cos t, \operatorname{sen} t) \mid 0 \leq t < 2\pi\}$.

En este caso, C *es una imagen. Si consideramos la función, cuyo dominio es el intervalo* $[0, 2\pi)$, *dada por:*

$$f(t) = (\cos t, \operatorname{sen} t),$$

resulta que $f([0,2\pi)) = \operatorname{Im}(f) = C$.

Si un conjunto está descrito como la imagen de una función, se dice que lo hemos dado de forma paramétrica.

(3) Finalmente, un conjunto puede ser la gráfica de una función:

La semicircunferencia $C^+ = \{(x,y) \mid x^2 + y^2 = 1, y \geq 0\}$ *es la gráfica de la función:*

$$f : [-1,1] \longrightarrow \mathbb{R}$$
$$y = f(x) = \sqrt{1 - x^2}.$$

Cuando un conjunto viene dado como la gráfica de una función, diremos que tenemos una representación explícita.

Ejercicios

1) *Sea* $f : \{$*cuadros del Museo del Prado*$\} \longrightarrow \{$*pintores*$\}$, *de manera que* $f(x) =$ *autor del cuadro* x. *Calcular las imágenes de: Las Meninas, El Jardín de las Delicias, Las tres Gracias, El Lavatorio. ¿Es* f *una aplicación inyectiva? ¿Es* f *sobreyectiva? Dar ejemplos fehacientes.*

2) *Estudiar si son inyectivas, sobreyectivas o biyectivas las funciones:*

a) $f : \mathbb{R}^+ \longrightarrow \mathbb{R}, \quad f(x) = \sqrt{x}$.
b) $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = x - \sqrt{2}$.
c) $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = 1 - x^2$.
d) $f : \mathbb{Q} \longrightarrow \mathbb{R}, \quad f(x) = 7x$.
e) $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x,y) = 7y$.

3) *Calcular el dominio de definición y el conjunto imagen, como subconjuntos de $\mathbb{R}$, de las funciones siguientes:*

$$\text{i) } f(x) = (x-1)^2\,; \qquad \text{ii) } g(x) = 2x - 1\,;$$
$$\text{iii) } h(x) = \frac{1}{x^2-1}\,; \qquad \text{iv) } j(x) = \sqrt{1 + 1/x}.$$

4) *Encontrar una función polinómica sencilla que tome los valores siguientes*

a)

x	...	-2	-1	0	1	2	3	...
$f(x)$	...	-5	-3	-1	1	3	5	...

b)

x	...	-2	-1	0	1	2	3	...
$f(x)$	...	-8	-1	0	1	8	27	...

5) *Sea $f : \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(x) =$ suma de las cifras de x en base 10. Ejemplos: $f(12) = 3$, $f(347) = 14, \ldots$ ¿Es f inyectiva? ¿Es sobreyectiva? ¿Cuáles son los x tales que $f(x) = x$?*

6) *Representar gráficamente las funciones:*

i) Identidad: $y = x$.
ii) Función cuadrática: $y = x^2$.
iii) Función cúbica: $y = x^3$.
iv) Valor absoluto: $y = |x| = \max\{x, -x\}$.
v) Parte entera: $y = [x] =$ mayor entero menor o igual que x.
vi) Parte fraccionaria: $y = \{x\} = x - [x]$.
vii) Proporcionalidad inversa: $y = \dfrac{1}{x}$.

7) *Dada una función $f : D \longrightarrow E$, definamos para cada subconjunto $A \subset E$ la imagen inversa:*

$$f^{-1}(A) \;=\; \{\, x \in D \;\mid\; f(x) \in A\}.$$

¿Qué relaciones existen entre $f^{-1}(A)$, $f^{-1}(B)$, $f^{-1}(A \cup B)$ y $f^{-1}(A \cap B)$?

8) *¿Cuáles de las siguientes funciones son inyectivas? ¿Cuáles suprayectivas? ¿Es alguna de ellas biyectiva? (Empieza por asegurarte de que todas ellas son, efectivamente, funciones.)*

a) $f : \mathbb{N} \to \mathbb{N}, \quad f(m) = m + 2$
b) $g : \mathbb{Z} \to \mathbb{Z}, \quad g(m) = 2m - 7$
c) $f : \mathbb{Q} \to \mathbb{Q}, \quad f(x) = x^2 + 4x$
d) $g : \mathbb{N} \to \mathbb{N}, \quad g(n) = n(n+1)$
e) $f : \mathbb{Z} \to \mathbb{N}, \quad f(n) = n^2 + n + 1$
f) $g : \mathbb{N} \to \mathbb{Q}, \quad g(t) = \frac{t}{t+1}$

9) *Exhibe ejemplos de aplicaciones $f : \mathbb{N} \to \mathbb{N}$ de cada uno de los siguientes tipos:*

i) Inyectivas pero no suprayectivas; ii) Suprayectivas pero no inyectivas; iii) Biyectivas y iv) Ni inyectivas ni suprayectivas.

10) *Sea A un conjunto* finito.

a) *Demuestra que toda aplicacion inyectiva $A \to A$ es suprayectiva, y toda aplicacion suprayectiva $A \to A$ es inyectiva. Compara con el ejercicio 9.*

b) *¿si A tiene n elementos, cuántos elementos tiene el conjunto*

$$\{f : A \to A \mid f \text{ es una aplicación biyectiva }\}?$$

11) *Sean $f, g : \mathbb{Q} \to \mathbb{Q}$ las aplicaciones definidas por $f(x) = x^2$, $g(x) = x+2$. Estudia la posible suprayectividad o inyectividad de f, g, $f \circ g$, $g \circ f$.*

12) *Se considera la aplicación $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por $f(\alpha, \beta) = 3\alpha + 2\beta$. Averigua si f es inyectiva y/o suprayectiva.*

En los ejercicios 13, 14 y 15 siguientes los conjuntos X e Y son no vacíos.

13) *a) Demuestra que $f : X \to Y$ es inyectiva $\iff$ existe $g : Y \to X$ tal que $g \circ f = id_X$.*

b) *Dar un ejemplo donde X e Y sean conjuntos finitos.*

c) *Dar un ejemplo donde X e Y sean conjuntos infinitos.*

14) *a) Demuestra que $f : X \to Y$ es sobreyectiva $\iff$ existe $g : Y \to X$ tal que $f \circ g = id_Y$.*

b) *Dar un ejemplo donde X e Y sean conjuntos finitos.*

c) *Dar un ejemplo donde X e Y sean conjuntos infinitos.*

15) *a) Demuestra que $f : X \to Y$ es biyectiva $\iff$ existe $g : Y \to X$ tal que $g \circ f = id_X$ y $f \circ g = id_Y$.*

a) *Dar un ejemplo donde X e Y sean conjuntos finitos.*

b) *Dar un ejemplo donde X e Y sean conjuntos infinitos.*

16) *Sea $f : X \to Y$ una aplicación. Recuerda que si $Z \subset Y$, se define*

$$f^{-1}(Z) = \{x \in X \mid f(x) \in Z\}.$$

Define una aplicación $f : \mathbb{R} \to \mathbb{R}$ tal que $f^{-1}(\{3\}) = \mathbb{R}$. Describe $f^{-1}(\{\pi\})$ para la función f que hayas definido.

17) *Sea $f : X \to Y$ una aplicación, y sean Z_1 y Z_2 subconjuntos de X.*

i) *Analiza la relación entre $f(Z_1 \cap Z_2)$ y $f(Z_1) \cap f(Z_2)$.*

ii) *Analiza la relación entre $f(Z_1 \cup Z_2)$ y $f(Z_1) \cup f(Z_2)$.*

18) *Dada una aplicación $f : X \to Y$ y subconjuntos $Z, W \subset Y$, demuestra que*

a) $f^{-1}(Z \cup W) = f^{-1}(Z) \cup f^{-1}(W)$

b) $f^{-1}(Z \cap W) = f^{-1}(Z) \cap f^{-1}(W)$

c) $f(f^{-1}(Z)) = f(X) \cap Z$

d) $X \setminus f^{-1}(Z) = f^{-1}(Y \setminus Z)$.

19) *Sea $f : \mathbb{R} \to \mathbb{R}$ la función definida por*

$$f(x) = \begin{cases} x^2 + 4x & si\ x \leq -1 \\ 3x & si\ x > -1 \end{cases}$$

y sea $A = [-2, 1] \subset \mathbb{R}$.

a) *Dibuja el gráfico de f y calcula $f(A)$.*

b) *Demuestra que f no es ni inyectiva ni suprayectiva, pero que si la restringimos a $f : A \to f(A)$ la función restringida es una biyección. Encuentra la función inversa de esta biyección.*

20) *Sea $g : \mathbb{R} \to \mathbb{R}$ la función definida por*

$$g(x) = \begin{cases} x^3 & si\ x < -1 \\ -x & si\ -1 \leq x < 1 \\ x^2 & si\ x \geq 1\,. \end{cases}$$

a) *Dibuja el gráfico de g.*

b) *Demuestrar que g no es ni inyectiva ni suprayectiva, pero que basta con cambiar la definición de $g(x)$ para un único valor de x para obtener una función biyectiva. (La manera de hacer esto no es única.)*

c) *Describe explícitamente la función inversa de la que has obtenido en el apartado b).*

21) *Sean $f, g : \mathbb{R} \to \mathbb{R}$ las funciónes definidas por:*

$$f(x) = \begin{cases} x^2 & si\ x \leq 1 \\ 1 - x^2 & si\ x > 1 \end{cases} \qquad g(x) = \begin{cases} x^2 & si\ x < 0 \\ (x-1)^2 & si\ x \geq 0\,. \end{cases}$$

a) *Dibuja los gráficos de las funciones f, g, $g \circ f$ y $f \circ g$.*

b) *Encuentra las imágenes de cada una de las cuatro funciones anteriores y decide si son inyectivas y/o suprayectivas.*

— 2 —

Los números naturales

Yo no soy nadie.
¿Quién eres tú?
¿Tampoco eres nadie?
¡Ya somos dos!
Emily Dickinson

2.1. La esencia de los números

Como ya señalamos en el capítulo anterior, los números naturales, uno, dos, tres, etc., junto con el cero, están en la base de cualquier idioma, siendo la operación de contar los elementos de un conjunto una de las primeras destrezas que adquiere el cerebro humano. De manera que las Matemáticas de la infancia consisten, en gran medida, en el aprendizaje de las reglas de uso de sus operaciones: suma, resta, multiplicación y división.

No obstante, su naturaleza es mucho más esquiva de lo que cabría esperar. Hagamos la prueba preguntándonos seriamente: ¿Qué es el número 1*? Hacia finales del siglo* XIX *el lógico G. Frege y el matemático G. Cantor, entre otros, trataron de dar una respuesta reduciendo la noción de número a la "más primitiva" de conjunto, siguiendo el modo de funcionamiento de nuestro cerebro, que llega a los números "contando" los elementos de los conjuntos.*

Consideremos pues el conjunto fundamental de cualquier egoísta: $\{yo\}$ *o* $\{yo\ mismo\}$*. Enseguida encontramos otros conjuntos que se pueden poner en correspondencia biyectiva con él:* $\{mi\ mamá\}$, $\{mi\ ombligo\}$, *etc. Querríamos que nuestra noción de número* 1 *esté asociada a esta familia de conjuntos, mientras que el número* 2 *lo fuese, por ejemplo, al conjunto* $\{él,\ ella\}$ *y al de todos los que le son biyectables. En algunas teorías filosóficas cabría decir*

que 1 *es la propiedad que comparten todos los conjuntos biyectables con* $\{yo\}$ *y que* 2 *es la de los equipotentes con* $\{$*él, ella*$\}$*, y así sucesivamente. Pero en Matemáticas no es válido este tipo de definiciones, porque antes habría que tener una lista de todas las propiedades donde escoger precisamente la única que comparten todos esos conjuntos, lo que, pensémoslo un momento, resultaría bastante complicado de conseguir.*

La solución que Frege y Cantor creyeron haber encontrado era: consideremos la relación entre conjuntos dada por la biyectabilidad. Es decir, diremos que los conjuntos A *y* B *están relacionados,* $A\mathcal{R}B$*, si existe una aplicación biyectiva* f *entre ellos. Es fácil ver que esta relación verifica las propiedades:*

1. *Reflexiva:* $\forall A$, $A\mathcal{R}A$.

2. *Simétrica:* $\forall A$, B, *si* $A\mathcal{R}B$ *entonces* $B\mathcal{R}A$.

3. *Transitiva:* $\forall A$, B, C, *si* $A\mathcal{R}B$ *y* $B\mathcal{R}C$ *entonces* $A\mathcal{R}C$.

Es decir, se trata de un ejemplo de lo que llamamos relación de equivalencia. Esta relación divide al "conjunto de todos los conjuntos" en clases disjuntas, estando formada cada clase de equivalencia por conjuntos biyectables entre sí. Entonces 1 *es la clase de todos los conjuntos biyectables (equipotentes) con* $\{yo\}$ *y* 2 *es la de los biyectables con* $\{$*él, ella*$\}$*, y así sucesivamente.*

¡Fantástico! Quizá al principio nos parezca un tanto rebuscado pensar que 1 *es el conjunto de todos los conjuntos biyectables con* $\{yo\}$*, pero, si lo miramos con más detenimiento, resulta una definición de lo más natural. A partir de ella podemos reducir la Aritmética (y el resto de las matemáticas) a la noción fundamental de conjunto y a los postulados básicos de la Lógica.*

Pero hay una pega muy seria que radica en el uso de la expresión "el conjunto de todos los conjuntos", que da lugar a diversas antinomias. Uno de los primeros en darse cuenta fue Bertrand Russell quien formuló la siguiente paradoja:

> *Definamos un conjunto ordinario como aquel que no se contiene a sí mismo como miembro. Así un conjunto extraordinario es aquel que es elemento de sí mismo.*
>
> *Formemos ahora "el conjunto de todos los conjuntos ordinarios" y preguntémonos de qué tipo es: ¿ordinario o extraordinario? Veamos: no puede ser ordinario, porque de serlo, habría de ser extraordinario. Pero tampoco puede ser extraordinario pues, entonces, al ser miembro de sí mismo sería también ordinario.*

¡Qué horror! tanto exquisito cuidado en la definición de número natural llevándonos a una contradicción. En la historia de las matemáticas ocupa un lugar preeminente este episodio, que originó la llamada crisis de los fundamentos y cuya solución (o soluciones) dio lugar al desarrollo de la Lógica Matemática. En el capítulo 8 volveremos a tratar estos temas con más detenimiento.

Feliz surge la idea que nos lleva
por la senda ingeniosa,
que parece certera,
a la vera, muy cerca,
de ese ansiado teorema.

Pero la esquiva verdad no nos deja,
escondida en su templo,
ni desnuda probarla,
ni tampoco falsarla
con sutil contraejemplo.

Y aunque la mente mil tretas produce,
ofreciendo al diablo el clásico pacto.
Pasa el tiempo, la ambición se reduce,
y otra derrota cedemos de facto:

Poseerla en cualquier traje típico
de una hipótesis clara y razonable,
que permita un saludo al respetable
en forma de artículo científico.

En las crisis suelen aparecer esos caracteres pragmáticos sugiriendo que olvidemos las cuestiones de principios y proponen que nos centremos en la tarea de establecer reglas de juego que sean claras y nos permitan, manteniendo cierta dignidad, continuar de alguna forma. Esa fue la propuesta formulada por el gran D. Hilbert, siendo la axiomática de G. Peano una de sus más notables concreciones.

Sostiene Peano que postulemos la existencia de un conjunto $\mathbb{N}$ *llamado de los números naturales de acuerdo con los siguientes axiomas:*

i) $\exists\, 0 \in \mathbb{N}$ *(existencia del cero).*

ii) $\forall n \in \mathbb{N}$, $\exists S(n)$ *(el siguiente de* n*) que pertenece a* $\mathbb{N}$.

iii) 0 *no es el siguiente de nadie.*

iv) $\forall n, m \in \mathbb{N}$, $S(n) = S(m) \implies n = m$.

v) Si $A \subset \mathbb{N}$ *es tal que* $0 \in A$ *y* $(n \in A) \implies (S(n) \in A)$*, entonces* $A = \mathbb{N}$ *(principio de inducción).*

Con Peano llamemos $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, $\ldots$ *A partir de los axiomas podemos fácilmente obtener muchas propiedades y operaciones de los números naturales.*

Ejemplo 1:

1º La SUMA *queda definida por las siguientes reglas:*

i) $m + 0 = 0 + m = m$, $\forall\, m \in \mathbb{N}$

ii) $m + S(n) = S(m + n)$, $\forall\, m,\, n \in \mathbb{N}$.

Veamos:

$$\begin{aligned} 1 + 1 &= 1 + S(0) = S(1 + 0) = S(1) = 2 \\ 1 + 2 &= 1 + S(1) = S(1 + 1) = S(2) = 3 \\ 2 + 1 &= 2 + S(0) = S(2 + 0) = S(2) = 3 \\ 2 + 2 &= 2 + S(1) = S(2 + 1) = S(3) = 4 \\ &\cdots \quad \cdots \quad \cdots \end{aligned}$$

Ejercicio 1. *Demostrar las propiedades asociativa y conmutativa de la suma a partir de la definición.*

2º La MULTIPLICACIÓN*:*

i) $0 \times m = m \times 0 = 0$, $\forall\, m \in \mathbb{N}$

ii) $m \times S(n) = m \times n + m$, $\forall\, m,\, n \in \mathbb{N}$.

Veamos:

$$\begin{aligned} m \times 1 &= m \times S(0) = m \times 0 + m = 0 + m = m \\ 1 \times 1 &= 1 \times S(0) = 1 \times 0 + 1 = 0 + 1 = 1 \\ 1 \times 2 &= 1 \times S(1) = 1 \times 1 + 1 = 1 + 1 = 2 \\ 2 \times 2 &= 2 \times S(1) = 2 \times 1 + 2 = 2 + 2 = 4 \\ &\cdots \quad \cdots \quad \cdots \end{aligned}$$

Ejercicio 2. *Demostrar las propiedades asociativa y conmutativa del producto, así como la distributiva del producto respecto de la suma, a partir de la definición anterior.*

Ejercicio 3. *Dar una definición de la relación $\leq$ entre números naturales y demostrar sus propiedades: i) reflexiva: $a \leq a$, $\forall\, a \in \mathbb{N}$; ii) transitiva: $a \leq b$ y $b \leq c \implies a \leq c$, $\forall a,\, b,\, c \in \mathbb{N}$; iii) antisimétrica: $a \leq b$ y $b \leq a \implies a = b$.*

Habiendo introducido el conjunto $\mathbb{N}$ a través de los axiomas de Peano, conviene mostrar un modelo que los satisfaga. Por ejemplo: partamos de la existencia del conjunto vacío $\emptyset$ y del axioma que nos asegura, a partir de un conjunto X, la existencia de otro conjunto $S(X)$ de manera que: $a \in S(X)$ si y solo si ora $a \in X$ ya $a = X$.

Tenemos entonces la sucesión:

$$\emptyset,\ S(\emptyset) = \{\emptyset\},\ S(\{\emptyset\}) = \big\{\emptyset, \{\emptyset\}\big\},\ S\Big(\big\{\emptyset, \{\emptyset\}\big\}\Big) = \Big\{\emptyset, \{\emptyset\}, \big\{\emptyset, \{\emptyset\}\big\}\Big\}, \ldots$$

Designando $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \big\{\emptyset, \{\emptyset\}\big\}$, ..., obtendremos un modelo del conjunto $\mathbb{N}$ de los números naturales, en el que $n = \{0, 1, 2, \ldots, n - 1\}$.

Y todas las cosas para llegar a ser se miran
en el vacío espejo de su nada.

José Ángel Valente

Cabrían algunas preguntas interesantes, tales como si el sistema de axiomas que hemos ido presentando es consistente o no lo es, es decir, si da lugar a contradicciones o si está libre de ellas. También querríamos saber si es completo, es decir si toda pregunta "bien formulada" ha de tener necesariamente una respuesta, positiva o negativa. ¿Existen otros "modelos" que satisfagan los axiomas de Peano y no se parezcan a $\mathbb{N}$*? Son estas algunas cuestiones que han dado lugar a magníficas teorías que enseguida sobrepasan los límites de este libro.*

Pero volviendo a plantear la pregunta original (¿qué son los números naturales?) resulta que a muchos matemáticos no les pareció que la axiomática de Peano fuese una buena respuesta, por lo que contribuyeron a perfeccionar la estrategia de Frege y Cantor hasta convertirla en una teoría satisfactoria. Pero a eso volveremos en el capítulo 8.

2.2. Divisibilidad: números primos y números compuestos

Consideremos la multiplicación que junto con la suma constituyen las dos operaciones fundamentales que podemos realizar con los números naturales:

Definición. *Diremos que el número* a *es divisible por el* b*, o bien que* b *es un divisor de* a*, si podemos encontrar otro número natural* c *de manera que* $a = b \times c$*: escribimos entonces* $b \mid a$ *(y leeremos: "*b *divide a* a*").*

Ejemplos: 6 *es divisible por* 2 *y por* 3*, ya que* $6 = 2 \times 3$*; también es divisible por* 1 *y por* 6*, puesto que* $6 = 1 \times 6$*. Resulta fácil ver que* $\{1, 2, 3, 6\}$ *es el conjunto de todos los divisores del número* 6*.*

Otras factorizaciones son: $7 = 1 \times 7$*;* $11 = 1 \times 11$*;* $12 = 1 \times 12 = 2 \times 6 = 3 \times 4$*;* $20 = 1 \times 20 = 2 \times 10 = 4 \times 5$*;* $120 = 1 \times 120 = 2 \times 60 = 3 \times 40 = 4 \times 30 = 5 \times 24 = 6 \times 20 = 8 \times 15 = 10 \times 12$*. Resumiendo:*

$$\begin{aligned}
&\textit{Divisores de } 6 && = \{1, 2, 3, 6\} \\
&\textit{Divisores de } 7 && = \{1, 7\} \\
&\textit{Divisores de } 11 && = \{1, 11\} \\
&\textit{Divisores de } 20 && = \{1, 2, 4, 5, 10, 20\} \\
&\textit{Divisores de } 120 && = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, \\
& && \quad 24, 30, 40, 60, 120\}.
\end{aligned}$$

El número 1 *es un divisor universal puesto que cualquier otro número,* a*, es igual al producto* $1 \times a$*. Es decir, cualquier número distinto de la unidad, tiene, por lo menos, dos divisores. A saber: él mismo y la unidad.*

Desde esta perspectiva tenemos, además de la unidad, dos clases de números: aquellos que solo son divisibles por sí mismos y por la unidad, como es el caso de 7 *y* 11*, o bien aquellos otros que tienen más divisores, como son los ejemplos:* 6, 12, 20 *y* 120.

En otras palabras: el número 6 *puede ser generado como un producto a partir de los números* 2 *y* 3*. Este no es el caso del número* 7*, puesto que el único producto que da* 7 *es precisamente* 1×7*, que ya involucra al número* 7.

Desde el punto de vista de la multiplicación el 6 *es un número del que podríamos prescindir, ya que se obtiene a partir del* 2 *y del* 3*; pero ese no es el caso del* 7*, que resulta del todo imprescindible.*

Esta diferencia era ya conocida por los griegos del periodo clásico, siendo motivo de consideración y estudio en los Elementos de Euclides, que es el compendio del saber matemático de su tiempo.

Definición. *Un número natural distinto de* 1 *es primo si y solo si es divisible solo por sí mismo y por la unidad. Los números que no son primos se llaman compuestos.*

Ejemplo 2: 2, 3, 5, 7, 11, 13, 19, 23 *son números primos;* 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22 *son números compuestos.*

Ejercicio 4. *Detectar los números primos entre los siguientes:*

45, 47, 49, 53, 57, 58, 59, 60, 61,
709, 1.067, 1.069, 1.071, 3.137, 4.409.

Escribir los conjuntos de divisores para los que sean compuestos.

Ejercicio 5. *Encontrar cuatro números consecutivos que sean compuestos. Si ha resultado fácil, tratar ahora de hacerlo con* 5, 10, 15, ... *números consecutivos. ¿Es cierto que para todo* n *existen* n *naturales consecutivos que son todos compuestos?*

Primos gemelos o primos hermanos. *Los primos* 3 *y* 5, 5 *y* 7, 11 *y* 13, 17 *y* 19, 29 *y* 31*, forman parejas de números primos que son impares consecutivos. Los denominaremos primos hermanos o primos gemelos. ¡Todavía no se sabe cuántas parejas de primos gemelos existen!*

Primos de Fermat. *Pierre de Fermat observó que la fórmula* $F_n = 2^{2^n} + 1$ *produce números primos cuando se sustituyen los valores:*

$$
\begin{aligned}
&n = 0, \quad F_0 = 2^{2^0} + 1 = 2 + 1 = 3 \\
&n = 1, \quad F_1 = 2^{2^1} + 1 = 4 + 1 = 5 \\
&n = 2, \quad F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17 \\
&n = 3, \quad F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257 \\
&n = 4, \quad F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65.536 + 1 = 65.537.
\end{aligned}
$$

Sin embargo, Euler demostró que F_5 es compuesto y divisible por 641. Nadie, hasta ahora, ha logrado encontrar otro número primo en la sucesión de Fermat.

Recientemente, con la ayuda de los supercomputadores, se ha logrado factorizar el número F_9, que resulta ser el producto de tres primos que poseen 7, 49 y 99 cifras, respectivamente.

En el sistema decimal de numeración el número edcba (donde las letras a, b, c, d, e son dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 o 9) tiene el valor:

$$\boxed{edcba = a + 10b + 100c + 1.000d + 10.000e.}$$

Ejemplo 3: $24.739 = 9 + 10 \times 3 + 100 \times 7 + 1.000 \times 4 + 10.000 \times 2$.

Tenemos que $edcba = a + 5(2 \times b + 20 \times c + 200 \times d + 2.000 \times e)$, luego edcba es un múltiplo de 5 si y solo si lo es a, es decir si $a = 0$ o $a = 5$.

Los números que son múltiplos de 5 acaban en 0 o en 5.

Ejercicio 6. *Usar las identidades*

$$a+10b+100c+1.000d+10.000e = a+b+c+d+e+9(b+11c+111d+1.111e)$$
$$a+10b+100c+1.000d+10.000e = a-b+c-d+e+11(b+9c+91d+909e)$$

para obtener criterios de divisibilidad por 3, 9 y 11.

La divisibilidad de números naturales goza de las tres propiedades siguientes:

1ª) Reflexiva: Todo número es divisor de sí mismo: $a \mid a$.

2ª) Antisimétrica: Si $a \mid b$ y $b \mid a$, entonces, $a = b$.

3ª) Transitiva: Si $a \mid b$ y $b \mid c$, entonces, $a \mid c$.

Cuando una relación entre los elementos de un conjunto tenga estas tres propiedades, diremos que se trata de un orden o una relación de orden.

El arquetipo de relaciones de orden entre los números naturales es la relación menor o igual ($a \leq b :=: \exists c \in \mathbb{N}, a + c = b$), que claramente satisface:

1º) $a \leq a$ cualquiera que sea $a \in \mathbb{N}$ (reflexiva);

2º) si $a \leq b$ y $b \leq a$, entonces, $a = b$ (antisimétrica);

3º) si $a \leq b$ y $b \leq c$, entonces, $a \leq c$ (transitiva).

Estas dos relaciones "$\leq$" y "$\mid$" comparten pues el carácter de ser "órdenes" en el conjunto $\mathbb{N}$ de los números naturales. Sin embargo, tienen otras características distintas:

a) $\mathbb{N}$ *con el orden "$\leq$" tiene un primer elemento, que es el* 0*, pero no tiene un elemento máximo: "no existe un natural* n *que sea posterior (mayor) que todos los demás".*

b) *Con el orden de la divisibilidad "$|$", el conjunto* $\mathbb{N}$ *tiene un primer elemento, o mínimo, que es* 1*; pero también tiene un último elemento, o máximo, que es el* 0*: "Para todo natural* a *se verifica que* $1|a$ *y* $a|0$*".*

c) *Otra diferencia entre "$\leq$" y "$|$" es la siguiente: dados dos naturales* a *y* b*, necesariamente ha de verificarse una de las dos desigualdades:* $a \leq b$ *o* $b \leq a$*. Es decir, dos números naturales siempre están relacionados por "$\leq$". Sin embargo, ese no tiene por qué ser el caso respecto a la relación de divisibilidad, pudiendo ocurrir que ni* a *sea divisible por* b*, ni* b *por* a *(ejemplo:* $a = 2$ *y* $b = 21$*).*

   En la terminología de las relaciones de orden, se distingue esta propiedad con el nombre de "orden total", para las relaciones similares a "$\leq$" y "orden parcial" para las otras, como "$|$".

2.3. El algoritmo de Euclides

En los ejemplos anteriores, hemos visto que
divisores de $12 = \{1, 2, 3, 4, 5, 6, 12\}$ *y divisores de* $20 = \{1, 2, 4, 5, 10, 20\}$*. Luego* $\{1, 2, 4\}$*, que es la intersección de los dos conjuntos, consta de los divisores comunes a ambos números,* 12 *y* 20*. El mayor de ellos, que resulta ser* 4*, tiene un status especial: "es el máximo común divisor de* 12 *y* 20*", propiedad que escribiremos abreviadamente con la notación*

$$m.c.d.(12, 20) = 4.$$

En general, dados dos números naturales, a *y* b*, designaremos por* $m.c.d.(a, b)$ *al mayor de sus divisores comunes.*

Observemos que cualesquiera que sean a *y* b*, siempre tienen, por lo menos, al* 1 *como divisor común. Puede ocurrir que sea el único, en cuyo caso* $m.c.d.(a, b) = 1$ *y se dice que* a *y* b *son primos relativos o primos entre sí (por ejemplo:* $m.c.d.(6, 7) = 1$*,* $m.c.d.(120, 77) = 1$*).*

Problemas. *Calcular el m.c.d de* 105 *y* 38*.*

SOLUCIÓN:
$$\begin{array}{r|l} 105 & 38 \\ 29 & 2 \end{array} \qquad \begin{array}{r|l} 38 & 29 \\ 9 & 1 \end{array} \qquad \begin{array}{r|l} 29 & 9 \\ 2 & 3 \end{array} \qquad \begin{array}{r|l} 9 & 2 \\ 1 & 4 \end{array} \qquad \begin{array}{r|l} 2 & 1 \\ 0 & 2 \end{array}$$

Luego $m.c.d.(105, 38) = 1$*.*

Calcular $m.c.d.(700, 182)$*.*

SOLUCIÓN:
$$\begin{array}{r|l} 700 & 182 \\ 154 & 3 \end{array} \qquad \begin{array}{r|l} 182 & 154 \\ 28 & 1 \end{array} \qquad \begin{array}{r|l} 154 & 28 \\ 14 & 5 \end{array} \qquad \begin{array}{r|l} 28 & 14 \\ 0 & 2 \end{array}$$

Luego $m.c.d.(700, 182) = 14$*.*

Ejercicio 7. *Calcular el máximo común divisor de los números siguientes:* $m.c.d.(36, 84)$*,* $m.c.d.(231, 99)$*,* $m.c.d.(360, 150)$*.*

La noción de máximo común divisor es muy interesante. Por fortuna, en los mismos Elementos de Euclides se encuentra una estrategia, o algoritmo, para calcularlo:

> *Sean a y b dos números naturales de los que proponemos investigar sus divisores comunes. Supongamos que a es mayor que $b \neq 0$. Si tenemos tanta suerte de que a sea divisible por b, entonces los divisores comunes de a y b consisten simplemente en los divisores de b, y no hay nada más que decir. En caso contrario, de mala suerte, siempre podemos expresar a como un múltiplo de b más un resto:*
>
> $$a = b \times c + r, \quad 0 \leq r < b$$
>
> $a =$ *dividendo*, $b =$ *divisor*,
> $c =$ *cociente*, $r =$ *resto*.
>
> *dividendo* $=$ *divisor* $\times$ *cociente* $+$ *resto*,
> *el resto es menor que el divisor.*
>
> *que es el algoritmo de la división que aprendimos en las matemáticas de la infancia: dados dos números naturales a y $b \neq 0$, podemos encontrar otros dos números c, cociente, y r, resto, tales que: $a = b \times c + r$, $0 \leq r < b$. Además c y r están unívocamente determinados por la propiedad anterior.*

El algoritmo. *Es claro que todo número que sea divisor común de a y de b, tiene también que serlo de b y de $r = a - b \times c$. Recíprocamente, todo divisor común de b y de r lo es también de $a = b \times c + r$ y de b.*

El problema de calcular los divisores comunes de a y de b queda reducido así al de calcular los divisores comunes de b y de r. La gran ventaja es que b y r son, respectivamente, más pequeños que a y b.

El algoritmo de Euclides consiste en la repetición de esta estrategia: si tenemos la suerte de que b es divisible por r, entonces los divisores comunes de b y r son todos los divisores de r. En caso contrario, podemos dividir otra vez: $b = d \times r + s$, $0 \leq s < r$. De nuevo resulta que los divisores comunes de b y r son los mismos que los divisores comunes de r y s.

El proceso continúa hasta que se acaba, y esto solo puede ocurrir cuando lleguemos a un resto igual a cero. Es decir, cuando lleguemos a un número en la sucesión $a, b, r, s, \ldots$ que sea un divisor del término que le precede. Ahora bien, es obvio que el proceso ha de tener un final puesto que una sucesión decreciente de números naturales $a > b > r > s > \ldots$ no puede continuarse de manera indefinida.

Dados dos números naturales a y b y su máximo común divisor, d, el algoritmo de Euclides nos permite calcular dos números naturales x e y tales que: o bien $d = ax - by$ o bien $d = by - ax$.

Ejemplos: *1)* $m.c.d.(12, 20) = 4$. *Tenemos que:*

$$\begin{aligned} 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \\ 4 = 12 - 8 &= 12 - (20 - 12) = 2 \times 12 - 1 \times 4. \end{aligned}$$

2) $m.c.d.(36.000, 34.452) = 36$.

$$\begin{aligned} 36.000 &= 1 \cdot 34.452 + 1.548 \\ 34.452 &= 22 \cdot 1.548 + 396 \\ 1.548 &= 3 \cdot 396 + 360 \\ 396 &= 1 \cdot 360 + 36 \\ 360 &= 10 \cdot 36 + 0 \end{aligned}$$

$$\begin{aligned} 36 = 396 - 360 &= 396 - (1.548 - 3 \times 396) \\ &= 4 \times 396 - 1.548 = 4 \times (34.452 - 22 \times 1.548) - 1.548 \\ &= 4 \times 34.452 - 89 \times 1.548 \\ &= 4 \times 34.452 - 89 \times (36.000 - 34.452) \\ &= 93 \times 34.452 - 89 \times 36.000. \end{aligned}$$

La demostración se puede hacer por inducción:

Sea P_n *la proposición que dice que todos los restos del algoritmo de Euclides, hasta el enésimo, pueden ser escritos de esa forma:* $\forall\, k{=}1, \ldots, n$, $\exists\, x_k, y_k$ *naturales tales que:*

$$\begin{aligned} &o\ bien \qquad r_k = ax_k - by_k \\ &o\ bien \qquad r_k = by_k - ax_k. \end{aligned}$$

Claramente P_1 *es cierta, por cuanto* $a = bc_1 + r_1$ *da lugar a*

$$r_1 = a - bc_1.$$

Supongamos P_n *cierta. Al dividir* r_{n-1} *entre* r_n *se obtiene:*

$$r_{n-1} = r_n c_n + r_{n+1}.$$

Luego $r_{n+1} = r_{n-1} - r_n c_n$. *Si sustituimos ahora* r_{n-1} *y* r_n *por sus respectivas expresiones como combinaciones de* a *y* b *con coeficientes naturales (recordad que hemos supuesto* P_n *cierta), y agrupamos los coeficientes de* a *y de* b, *obtendremos la expresión correspondiente a* r_{n+1}. ■

Ejercicio 8. *Con el algoritmo de Euclides calcular el máximo común divisor de:* 124 *y* 36*;* 2112 *y* 363*;* 93 *y* 341*. Expresarlo en cada caso en la forma* $d = ax - by$ *o* $d = by - ax$*.*

Una consecuencia sencilla es la siguiente observación, que resulta ser muy útil en el empeño de calcular el m.c.d. de dos números.

> *Sean* a*,* b *y* n *tres números naturales y formemos los productos* na *y* nb*. Entonces tenemos que*
> $$m.c.d.(na, nb) = n \times m.c.d.(a, b).$$

Esta identidad se deduce inmediatamente del algoritmo de Euclides. Si dividimos na *por* nb*, el cociente es el mismo que el obtenido al dividir* a *por* b*, pero el nuevo resto es igual a* n *veces el resto de dividir* a *por* b*:*

$$\begin{aligned} a &= b \times c + r, \qquad 0 \leq r < b \\ na &= nb \times c + nr, \qquad 0 \leq nr < nb. \end{aligned}$$

Luego la sucesión de los restos que vamos obteniendo al aplicar el algoritmo de Euclides a los números na *y* nb*, se obtiene sin más que multiplicar por* n *la sucesión de los restos correspondientes a los números* a *y* b*. En particular:*

$$m.c.d.(na, nb) = n \times m.c.d.(a, b).$$

Ejemplos: *1)* $m.c.d.(20.000, 12.000) = 1.000 \times m.c.d.(20, 12) = 4.000$*.*
2) $m.c.d.(7.000, 1.820) = 10 \times m.c.d.(700, 182) = 10 \times 14 = 140$*.*

Otra consecuencia importante es que los divisores comunes de a *y* b *son, precisamente, los divisores de su máximo común divisor. Es claro que si un número divide al máximo común divisor,* $d = m.c.d.(a, b)$*, entonces debe dividir a ambos,* a *y* b*. Recíprocamente, como* $d = ax - by$ *o* $d = by - ax$ *para unos ciertos naturales* x *e* y*, todo divisor común de* a *y de* b *lo debe ser también de* d*.*

Ejemplo 4: *Los divisores de* 12 *forman el conjunto* $\{1, 2, 3, 4, 6, 12\}$*. Los divisores de* 20 *son* $\{1, 2, 4, 5, 10, 20\}$*. Los divisores comunes son pues:* $\{1, 2, 4\}$*. Tenemos que* $m.c.d.(12, 20) = 4$ *y los divisores de* 4 *son:* $\{1, 2, 4\}$*.*

Ejercicio 9. *Dados los números* 120 *y* 300*, calcular los conjuntos de sus divisores. Utilizar el algoritmo de Euclides para hallar* $m.c.d.(120, 300)$ *y comprobar que los divisores de* $m.c.d.(120, 300)$ *son los comunes de* 120 *y* 300*. Escribir* $m.c.d.(120, 300) = 120x - 300y$ *o* $m.c.d.(120, 300) = 300y - 120x$*.*

Si los números a *y* b *son primos entre sí, entonces su máximo común divisor es igual a* 1*. El algoritmo de Euclides nos dice que podemos encontrar dos naturales,* x *e* y*, de manera que: o bien* $1 = ax - by$*, o bien* $1 = -ax + by$*.*

Ejemplo 5: $m.c.d.(105, 38) = 1$.

$$\begin{aligned} 1 &= 9 - 4 \times 2 = 9 - 4 \times (29 - 3 \times 9) = 13 \times 9 - 4 \times 29 \\ &= 13 \times (38 - 29) - 4 \times 29 = 13 \times 38 - 17 \times 29 \\ &= 13 \times 38 - 17 \times (105 - 2 \times 38) = 47 \times 38 - 17 \times 105; \end{aligned}$$

$$\boxed{x = 17,\ y = 47}$$

En realidad las cuestiones anteriores consisten en volver del revés las divisiones del algoritmo de Euclides:

$$\begin{aligned} 105 &= 2 \cdot 38 + 29 \\ 38 &= 1 \cdot 29 + 9 \\ 29 &= 3 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 1 = 9 - 4 \times 2 &= 9 - 4 \times (29 - 3 \times 9) \\ &= 13 \times 9 - 4 \times 29 \\ &= 13 \times (38 - 29) - 4 \times 29 \\ &\quad \textit{etcétera.} \end{aligned}$$

Supongamos que p sea primo y divisor del producto de dos números $n \times a$, pero que no sea un divisor de a.

Por ser primo, sus únicos divisores son 1 y p, y dado que p no es divisor de a, resulta que el único divisor común de p y de a es la unidad.

Por lo tanto $m.c.d.(np, na) = n \times m.c.d.(p, a) = n$. Sabemos que p es un divisor de np y de na, luego ha de serlo también de su m.c.d., n.

Este razonamiento constituye una prueba de un importante resultado que está descrito en el libro VII de los Elementos de Euclides:

> *Si p es un primo que resulta ser divisor del producto de dos números, entonces, necesariamente, divide a uno de los factores.*

Observación: La hipótesis de que p sea primo es crucial puesto que el enunciado análogo para números compuestos es falso. Por ejemplo: 6 es un divisor del producto 4×9, pero no es divisor de 4, ni tampoco de 9.

Ejercicios

1) *Usar el algoritmo de Euclides para calcular:*

$m.c.d.(89, 74)$	$m.c.d.(6120, 378)$	$m.c.d.(450, 360)$
$m.c.d.(1260, 75)$	$m.c.d.(345, 180)$	$m.c.d.(315, 140)$
$m.c.d.(4300, 720)$	$m.c.d.(980, 616)$	$m.c.d.(2080, 930)$

2) *Averiguar si son primos o compuestos los números siguientes:*

$$547,\ 793,\ 729,\ 989,\ 1073,\ 1103,\ 951,\ 1167,\ 2339,\ 843.$$

3) *El m.c.d. de los números* 729 *y* 125 *es igual a* 1. *Encontrar dos naturales* x, y *de manera que se tenga la igualdad:* $1 = 729x - 125y$ *o* $1 = -729x + 125y$.

4) *Si un primo* p *divide a un producto de números,* $a \cdot b \cdot c \cdot d \cdots$, *entonces es divisor de uno de los factores.*

El resultado anterior admite la siguiente extensión que podemos encontrar en los Elementos de Euclides.

Proposición. *Si* $a \mid b \cdot c$ *y m.c.d.*$(a, b) = 1$, *entonces* $a \mid c$.

Demostración. *Por ser m.c.d.*$(a, b) = 1$, *sabemos que existen dos naturales,* x, y, *tales que*

$$o\ bien \qquad 1 = ax - by$$
$$o\ bien \qquad 1 = by - ax.$$

Multiplicando por c *ambos miembros, obtenemos que:*

$$o\ bien \qquad c = axc - byc$$
$$o\ bien \qquad c = byc - axc\,,$$

como a *es un divisor de ambos,* axc *y* bcy, *necesariamente ha de serlo de su diferencia, es decir:* $a \mid c$. ■

2.4. El Teorema Fundamental de la Aritmética

Los Elementos de Euclides, que contienen muchas observaciones fundamentales acerca de los números primos, ha sido una de las obras más influyentes en el desarrollo científico de todos los tiempos. Es una de las maravillas de las matemáticas, que las distingue del resto de las ciencias, el que esas propiedades, halladas por los griegos hace veintitantos siglos, sigan tan vigentes ahora como cuando se descubrieron.

Consideremos un número n *y el conjunto de sus divisores que, necesariamente, contiene al* 1 *y al* n *entre sus elementos.*

En el caso en que n *sea primo, eso es todo; pero si* n *es compuesto, habrá de tener más divisores, a los que llamaremos propios, o sea, distintos de* 1 *y de* n.

Consideremos al más pequeño de entre ellos y llamémosle p. *Entonces,* p *tiene que ser un número primo.*

¡Es obvio!, ya que si p *fuera compuesto tendría que ser divisible por otro número* q *menor que él y distinto de la unidad. Pero* q *al ser divisor de* p *lo sería también de* n, *por lo que* p *no puede ser el divisor propio menor, en contra de la hipótesis de partida. ¡Luego* p *es un número primo!*

Podemos así afirmar que todo número natural mayor que uno es siempre divisible por un número primo. El divisor propio más pequeño de un número compuesto es siempre primo.

Es decir, dado un número natural a, ora es primo, ora podemos encontrarle un divisor primo: $a = p \cdot b$, p primo. Pero, en este último caso, podemos seguir con b y, o bien es primo, o bien tiene un divisor primo q, $b = q \cdot c$, $a = p \cdot q \cdot c$, ...

Si continuamos con este proceso, que necesariamente se acaba después de unos cuantos pasos, obtendremos que $a = p \cdot q \cdot r \cdots$ es un producto de números primos.

Todo número natural mayor que 1 es un producto de números primos.

Ejemplos: *Los divisores de 30 son $\{1, 2, 3, 5, 6, 10, 15, 30\}$, y el menor de sus divisores propios es 2, que es primo: $30 = 2 \times 15$.*

Los divisores de 15 son $\{1, 3, 5, 15\}$, siendo el menor de los propios, 3, un número primo: $15 = 3 \times 5$.

El último factor, 5, es ya primo, y así tenemos que $30 = 2 \times 3 \times 5$, es un producto de números primos.

Si tomamos ahora 420, la cadena de factorizaciones:

$$420 = 2 \times 210,\ 210 = 2 \times 105,\ 105 = 3 \times 35,\ 35 = 5 \times 7,$$

nos da la factorización de 420 en primos: $420 = 2^2 \times 3 \times 5 \times 7$.

Esta representación es única, porque si el número tuviera dos factorizaciones

$$a = p \cdot q \cdot r \cdots = p' \cdot q' \cdot r' \cdots$$

donde todos los factores son primos, entonces p sería divisor del producto $p' \cdot q' \cdot r' \cdots$ y, por tanto, debe ser divisor de uno de los factores. Ahora bien, la única posibilidad de que un primo divida a otro es que sean iguales.

Supongamos que $p = p'$, podemos entonces cancelarlos de la igualdad $p \cdot q \cdot r \cdots = p' \cdot q' \cdot r' \cdots$ para obtener $q \cdot r \cdots = q' \cdot r' \cdots$, y procederíamos ahora con el primo q. Eventualmente obtendríamos que los primos de la izquierda son los de la derecha y que las dos representaciones son iguales.

Teorema. *(*Teorema Fundamental de la Aritmética*) Todo número natural mayor que 1 se descompone de manera única como producto de números primos.*

Ejemplos: $6 = 2 \times 3$

$600 = 2 \times 2 \times 2 \times 3 \times 5 \times 5 = 2^3 \times 3 \times 5^2$

$242550 = 2 \times 3 \times 3 \times 5 \times 5 \times 7 \times 7 \times 11 = 2 \times 3^2 \times 5^2 \times 7^2 \times 11.$

Una de las cualidades que se asocian con las matemáticas es la precisión, que ha trascendido incluso al lenguaje coloquial: "esto es tan claro como que dos y dos son cuatro", o, "el equipo de tu pueblo está matemáticamente ascendido", que dicen los locutores de radio y televisión. La precisión no debe confundirse con la pedantería. A propósito del Teorema Fundamental, alguien nos podría decir que, por ejemplo, el número 6 *admite dos descomposiciones:*

$$6 = 2 \times 3 = 3 \times 2$$

que difieren en el orden de los factores. Bueno, podemos ponernos a cubierto de los pedantes añadiendo que la descomposición es única salvo el orden de los factores que, como todos sabemos, no cambia el producto y que también se conoce como propiedad conmutativa de la multiplicación.

Fijémonos en el número 600, *el factor primo* 2 *aparece tres veces, mientras que el* 3 *lo hace solo una, y el* 5, *dos. La notación exponencial de la derecha* $2^3 \times 3 \times 5^2$ *es más compacta y, a la larga, mucho más cómoda que* $2 \times 2 \times 2 \times 3 \times 5 \times 5$. *Claro está que son totalmente equivalentes, dicen exactamente lo mismo. Sin embargo, si tenemos que escribirlas muchas veces nos resultará más cómoda y económica la notación exponencial* $600 = 2^3 \times 3 \times 5^2$. *El caso de* 242.550 *resulta mucho más dramático.*

Según el Teorema Fundamental, todo número natural $n > 1$ *se escribe de manera única de la forma, llamada normal:*

$$n = p^a q^b r^c \dots$$

donde $p < q < r < \dots$ *son números primos, y los exponentes,* a, b, c *son enteros positivos.*

Ejercicio 10. *Escribir la descomposición normal de los números siguientes:*

$$90,\ 270,\ 1.221,\ 140,\ 8.712.$$

El Teorema Fundamental de la Aritmética confirma el carácter multiplicativo básico de los números primos que señalamos antes. Los números compuestos se generan como producto de primos. Si quisiéramos, podríamos prescindir de la palabra seis y sustituirla por la combinación dos por tres; ocho es dos por dos por dos; catorce es dos por siete, etc., quizás parezca este empeño otra pedantería, pero no lo es tanto ya que, como iremos descubriendo más adelante, sabremos mucho más de las propiedades de un número entero si conocemos su descomposición en factores primos.

Ejemplo 6: *De la descomposición en factores primos del número* 600, $600 = 2^3 \times 3 \times 5^2$, *vemos que sus divisores han de ser de la forma:*

$$d = 2^a \times 3^b \times 5^c,$$

donde $0 \leq a \leq 3$, $0 \leq b \leq 1$ *y* $0 \leq c \leq 2$. *Tenemos* 4 *posibilidades para* a, 2 *para* b *y* 3 *para* c. *Luego, en total tendremos* $4 \times 2 \times 3 = 24$ *posibles divisores, a saber:*

$$\begin{aligned} 1 &= 2^0 \times 3^0 \times 5^0 \\ 2 &= 2^1 \times 3^0 \times 5^0 \\ 4 &= 2^2 \times 3^0 \times 5^0 \\ &\vdots \quad \vdots \quad \vdots \\ 600 &= 2^3 \times 3 \times 5^2. \end{aligned}$$

A veces esta tarea no es fácil, incluso con la ayuda de las modernas computadoras. Por ejemplo, ha sido una verdadera epopeya el descomponer en factores primos el número de Fermat $F_9 = 2^{2^9} + 1$, *que tiene* 155 *cifras y que es el producto de tres números primos de* 7, 49 *y* 99 *cifras respectivamente.*

Resulta que saber descomponer eficientemente, o sea, con rapidez, es de interés para los espías que quieren leer los mensajes cifrados. No debe resultar extraño que los resultados de la investigación en esta área estén considerados de alto secreto.

¿Cuántos primos hay? ¿Conocemos un procedimiento sistemático para obtenerlos? La respuesta a estas dos preguntas se encuentran también en los Elementos.

Teorema. *Existen infinitos primos.*

La demostración de Euclides es una pequeña joya de orfebrería matemática basada en el principio de contradicción.

Demostración. *Supongamos que la tesis sea falsa y que hay solo un número finito de primos que podemos enumerar de menor a mayor:* $p < q < \ldots < r$; $p = 2$, $q = 3$, $\ldots$ *Formemos el número*

$$M = p \cdot q \cdots r + 1.$$

Entonces M *no puede ser primo ya que es mayor que* r *que, por hipótesis, es el primo mayor. Pero si* M *es compuesto nosotros sabemos que ha de ser divisible por un primo.*

Ahora bien, al dividir M *por cualquiera de los primos del universo* p, q, $\ldots$, r *siempre da resto igual a* 1; *luego* M *ni es primo ni es divisible por un primo.*

No hay escapatoria posible a las reglas del razonamiento, excepto proclamar que la hipótesis de partida era falsa. Es decir, no es cierto que solo haya un número finito de primos. Luego la sucesión de los primos nunca se acaba, es decir: "existen infinitos primos". ■

La criba de Eratóstenes. *Intentemos confeccionar una lista de números primos:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,$$
$$59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, \ldots$$

Resulta que cada vez es más difícil decidir si un número es primo o compuesto. Si queremos continuarla será fácil ver que 104, 105 *y* 106 *no son primos ya que el primero y el tercero son pares, mientras que el segundo es múltiplo de* 3 *y de* 5, *pero quizás nos llevaría un rato comprobar que* 107 *es primo.*

El primer algoritmo que se inventó para fabricar listas de números primos se denomina la criba de Eratóstenes, haciendo honor a su creador:

Criba de Eratóstenes

> *Para encontrar los primos menores que un número M dado, se escribe la sucesión* 2, 3, 4, 5, 6, $\ldots$, M, *y se tachan los múltiplos de* 2 *(salvo el* 2*). El primer superviviente es* 3 *que resulta ser primo.*
>
> *A continuación se tachan todos los múltiplos de* 3 *(salvo el* 3*):* 6, 9, 12, 15, $\ldots$ *El segundo superviviente es el* 5, *que resulta ser primo; el siguiente paso es tachar los múltiplos de* 5*:* 10, 15, 20, 25, $\ldots$
>
> *El siguiente superviviente es el* 7, *etcétera. Los números que sobreviven al proceso son los primos menores que M.*

En la práctica basta con "cribar" hasta el primer número superviviente p cuyo cuadrado, p^2, sobrepase a M. La razón es la siguiente: el divisor propio p más pequeño de un número compuesto N siempre es menor o igual que su raíz cuadrada: $p^2 \leq N$.

Ejemplo 7: *Para confeccionar la lista de los primos menores que* 200, *basta con eliminar o cribar, de los naturales menores que* 200, *todos aquellos que son múltiplos de primos menores que* 15, *puesto* $15^2 = 225 > 200$ *(ver Figura 2.1). Los supervivientes 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, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

Y estos son los primos menores que 200.

Ejercicio 11. *a) Usar la criba de Eratóstenes para confeccionar la lista de los primos menores que* 500.

b) Contar el número de parejas de primos hermanos que aparecen en la lista anterior.

[2]	[3]	4	[5]	6	[7]	8	9	10	[11]	12	[13]	14	15
16	[17]	18	[19]	20	21	22	[23]	24	25	26	27	28	[29]
30	[31]	32	33	34	35	36	[37]	38	39	40	[41]	42	[43]
44	45	46	[47]	48	49	50	51	52	[53]	54	55	56	57
58	[59]	60	[61]	62	63	64	65	66	[67]	68	69	70	[71]
72	[73]	74	75	76	77	78	[79]	80	81	82	[83]	84	85
86	87	88	[89]	90	91	92	93	94	95	96	[97]	98	99
100	[101]	102	[103]	104	105	106	[107]	108	[109]	110	111	112	[113]
114	115	116	117	118	119	120	121	122	123	124	125	126	[127]
128	129	130	[131]	132	133	134	135	136	[137]	138	[139]	140	141
142	143	144	145	146	147	148	[149]	150	[151]	152	153	154	155
156	[157]	158	159	160	161	162	[163]	164	165	166	[167]	168	169
170	171	172	[173]	174	175	176	177	178	[179]	180	[181]	182	183
184	185	186	187	188	189	190	[191]	192	[193]	194	195	196	[197]
198	[199]	200											

Figura 2.1: Criba de Eratóstenes en $\{2, 3, \ldots, 200\}$

Máximo común divisor m.c.d.(a,b)

Si conocemos la descomposición en factores primos de dos números, entonces resulta muy fácil hallar su m.c.d.:

Los primos que dividen al m.c.d. han de dividir a ambos números. El exponente de cada primo debe ser el más pequeño de los que tienen en a y en b.

Ejemplo 8:

$$a = 2^3 \times 3^2 \times 5 = 360$$
$$b = 2^2 \times 3 \times 5^2 = 300$$
$$m.c.d.(360, 300) = 2^2 \times 3 \times 5 = 60.$$

Mínimo común múltiplo m.c.m.(a,b)

Análogamente, para el m.c.m.:

El más pequeño de los múltiplos comunes a ambos números, a y b, tiene que ser divisible por todos los primos que aparecen en ambos, a y b, (comunes y no comunes). El exponente ha de ser el mayor de los dos.

Ejemplo 9:

$$a = 2^2 \times 3^2 \times 5 \times 7 = 1.260$$
$$b = 2^3 \times 3 \times 5^3 \times 11 = 33.000$$
$$m.c.m.(a, b) = 2^3 \times 3^2 \times 5^3 \times 7 \times 11 = 693.000.$$

Los siguientes son dos ejemplos notables de factorización.

Ejemplo 10: $n! = \prod_{p \le n} p^{S(p)}$, *siendo:*

$$S(p) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots + \left[\frac{n}{p^k}\right], \quad y \quad k = \left[\frac{\log n}{\log p}\right].$$

Hemos usado la expresión:

$$x = [x] + \{x\}, \quad [x] = \text{ parte entera de } x,$$
$$0 \le \{x\} < 1, \quad \{x\} = \text{ parte fraccionaria de } x.$$

Es claro que todo factor primo p de $n!$ es menor o igual que n, puesto que tiene que ser un divisor de algún $m \le n$. Para calcular el exponente al que aparece elevado el número primo p, observemos que el número de múltiplos de p entre 1 y n es $\left[\frac{n}{p}\right]$. Entre ellos, el cardinal de los que son divisibles por p^2 es $\left[\frac{n}{p^2}\right]$. Luego $\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]$ es exactamente el número de múltiplos de p, entre 1 y n, que no son divisibles por p^2, cada uno de los cuales contribuye con una unidad al exponente $S(p)$.

De la misma manera $\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]$ es exactamente el número de enteros entre 1 y n que es divisible por p^2 pero no por p^3, cada uno de los cuales contribuye con un factor 2 al exponente $S(p)$, obteniéndose $2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right)$ como contribución de todos ellos.

En general, $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$ es el número de múltiplos de p^k pero no de p^{k+1} entre 1 y n. En total dan una contribución $k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right)$ al exponente $S(p)$. Es decir:

$$S(p) = \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + 3\left(\left[\frac{n}{p^3}\right] - \left[\frac{n}{p^4}\right]\right) + \cdots = \sum_{k \ge 1} \left[\frac{n}{p^k}\right]$$

Finalmente observemos que la serie es finita, por cuanto

$$\left[\frac{n}{p^k}\right] = 0 \text{ si } p^k > n, \text{ es decir si } k > \left[\frac{\log n}{\log p}\right].$$

Ejemplo 11: *Sea* $N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. *Entonces*

$$N = \prod_{p \le 2n} p^{a(p)}, \qquad a(p) = \sum_{k=1}^{\left[\frac{\log(2n)}{\log p}\right]} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right).$$

Es decir el exponente $a(p)$ se obtiene del ejemplo anterior restando, para cada p, al exponente del numerador el que aparece en el denominador.

Dado un número $y = [y] + \{y\}$ *resulta que si* $0 \leq \{y\} < \frac{1}{2}$ *entonces* $[2y] = 2[y]$, *mientras que si* $\frac{1}{2} \leq \{y\} < 1$ *tenemos que* $[2y] = 2[y] + 1$. *Luego* $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]$ *puede tomar solo los posibles valores* 0 *o* 1. *En particular*

$$a(p) \leq \left[\frac{\log(2n)}{\log p}\right].$$

Ejercicios

Los siguientes ejercicios son para entrenarse, aclararse, profundizar y, por supuesto, para ser resueltos.

1) *Usar el algoritmo de Euclides para calcular:*

$$m.c.d.(488, 183),\ m.c.d.(386, 579),\ m.c.d.(138, 460),\ m.c.d.(2.167, 1.082).$$

2) *Hallar la descomposición en factores primos de los números siguientes:*

$$2.412,\ 24.353,\ 1.994,\ 819,\ 36.863.$$

3) *Los libros de una biblioteca no pasan de* 10.000 *y los podemos distribuir exactamente en lotes de* 12 *unidades, de* 27 *unidades y también de* 49 *unidades. ¿Cuántos libros hay exactamente en la biblioteca?*

4) *Al contar el número de alumnos de un colegio de* 4 *en* 4, *de* 5 *en* 5, *o de* 6 *en* 6, *resulta que siempre sobran* 2. *¿Cuál es el número de alumnos sabiendo que está comprendido entre* 100 *y* 150*?*

5) *En el conjunto de números* {16, 24, 25, 27, 30} *elegir tres que sean primos entre sí dos a dos.*

6) *Averiguar si son primos o compuestos los números siguientes:*

$$547,\ 793,\ 729,\ 989,\ 1.073,\ 1.103,\ 951$$
$$1.993,\ 1.167,\ 2.339,\ 843,\ 1.337,\ 2.809.$$

7) *Comprobar que la suma de dos impares consecutivos es siempre un múltiplo de* 4.

8) *Obtener todos los divisores de los números:* 504, 180, 240, 700.

9) *Observar que*

$$\begin{array}{rcrll} 15^2 & = & 225, & (2\text{—}25, & 2 = 1 \times 2) \\ 25^2 & = & 625, & (6\text{—}25, & 6 = 2 \times 3) \\ 35^2 & = & 1225, & (12\text{—}25, & 12 = 3 \times 4) \\ 45^2 & = & 2025, & (20\text{—}25, & 20 = 4 \times 5) \\ & & \cdots & \cdots & \end{array}$$

En general: $$\begin{aligned}(a5)^2 = (5+10a)^2 &= 5^2 + 100a^2 + 100a \\ &= 100a(a+1) + 25.\end{aligned}$$

Deducir un truco para impresionar a las amistades calculando con facilidad los cuadrados de los números terminados en 5.

10) *La fórmula* $n^2 + n + 41$ *produce números primos cuando se sustituyen los valores* $n = 0, 1, 2, 3, \ldots, 39$. *Ejemplos:* $n = 0$ *da* 41; $n = 1$, 43; $n = 2$, 47, ... *Compruébese. ¿Qué ocurre cuando* $n \geq 40$*?*

11) *Los griegos llamaban a un número perfecto si la suma de sus divisores era el doble del número. Ejemplos:*

i) 6 *es perfecto ya que sus divisores son*

$$\{1, 2, 3, 6\}$$

y $1 + 2 + 3 + 6 = 2 \times 6$;

ii) 28 *es perfecto ya que sus divisores son*

$$\{1, 2, 4, 7, 14, 28\}$$

y $1 + 2 + 4 + 7 + 14 + 28 = 2 \times 28$.

Cinco números perfectos son:

$$6,\ 28,\ 496,\ 8.128,\ 33.550.336.$$

Compruébese.

Es un problema abierto saber si existe algún número perfecto impar. Tampoco se sabe cuántos perfectos pares hay, ¿son un número finito?

12) *Comprobar que los siguientes números no son perfectos:*

$$3 \times 5,\ 3^2 \times 5,\ 3 \times 5^2,\ 3^2 \times 5^2,\ 3^3 \times 5,\ 3^3 \times 5^2.$$

13) *Demostrar que, cualesquiera que sean los exponentes* m *y* n, *el número*

$$3^m \times 5^n$$

no puede ser perfecto.

14) *Dados dos enteros positivos* a *y* b, *obsérvese que*

$$a \cdot b = m.c.d.(a, b) \times m.c.m.(a, b).$$

15) *Sea* $d = m.c.d.(a, b)$. *Demostrar que los enteros* a/d *y* b/d *son primos entre sí.*

2.5. La función $\pi(x)$

La sucesión de números primos ha fascinado a la humanidad desde tiempos remotos. Pero hasta hace bien poco no se conocían aplicaciones prácticas de su estudio. La situación cambió drásticamente con el descubrimiento de los sistemas de cifrado en clave pública, base de la seguridad de las comunicaciones, que están basados en las propiedades de la factorización de los naturales en producto de primos.

El objeto básico para entender cómo se distribuyen los primos dentro de $\mathbb{N}$*, es la función:*

$$\pi(x) = \text{ número de primos menores o iguales que } x.$$
$$\pi(2) = 1, \quad \pi(3) = 2, \quad \pi(4) = 2, \quad \pi(5) = 3, \quad \pi(6) = 3,$$
$$\pi(7) = 4, \quad \pi(8) = 4, \quad \pi(9) = 4, \quad \pi(10) = 4, \ldots$$

El resultado más importante es el teorema de los números primos, que dice lo siguiente:

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

En otras palabras, la proporción de números primos en torno a x *es:*

$$\frac{\pi(x)}{x} \approx \frac{1}{\log x}, \qquad \text{o bien:} \quad \pi(x) = \frac{x}{\log x} + E(x),$$

siendo

$$\lim_{x\to\infty} \frac{E(x)}{x/\log x} = 0$$

(el número de primos menores o iguales que x *es* $x/\log x$ *salvo un error que es pequeño en relación con* $x/\log x$*).*

El teorema de los números primos fue conjeturado por Gauss y Legendre en los comienzos del siglo XIX *y demostrado, casi cien años más tarde, por Hadamard y de la Vallée-Poussin, quienes usaron la teoría de las funciones analíticas de una variable compleja siguiendo el plan que había sido trazado por Riemann.*

Antes, Chebychev, con medios elementales pero ingeniosos, había logrado probar la existencia de dos constantes positivas, $0 < C_1 \leq C_2 < \infty$*, tales que:*

$$C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}.$$

Esfuerzos posteriores de otros autores permiten afinar las constantes:

$$C_1 = 0{,}9\ldots, \qquad C_2 = 1{,}1\ldots,$$

cuando restringimos el rango al caso de x *suficientemente grandes.*

En su trabajo Chebychev introdujo las funciones:

$$\Theta(x) = \sum_{p \le x} \log p, \qquad \Psi(x) = \sum_{p^m \le x} \log p.$$

La segunda suma merece una aclaración: se suma $\log p$ *por cada pareja formada por un primo* p *y un natural* m *tales que* $p^m \le x$. *Dado un primo* $p \le x$ *el número de veces que* $\log p$ *aparece en la suma* $\Psi(x)$ *es exactamente* $\left[\frac{\log x}{\log p}\right]$. *Luego tenemos la identidad:*

$$\Psi(x) = \sum_{p \le x} \log p \cdot \left[\frac{\log x}{\log p}\right].$$

Observemos que $\pi(x)$ *puede también escribirse de forma parecida:*

$$\pi(x) = \sum_{p \le x} 1.$$

Luego

$$\Theta(x) \le \Psi(x) \le \sum_{p \le x} \log p \, \frac{\log x}{\log p} = \log x \cdot \pi(x).$$

Dividiendo por x *obtenemos:*

$$\frac{\Theta(x)}{x} \le \frac{\Psi(x)}{x} \le \frac{\pi(x)}{x/\log x}.$$

Proposición. *Las funciones* $\dfrac{\Theta(x)}{x}$, $\dfrac{\Psi(x)}{x}$, $\dfrac{\pi(x)}{x/\log x}$ *tienen los mismos límites de indeterminación cuando* $x \to \infty$.

Demostración. *Sean*

$$A_1 = \limsup_{x\to\infty} \frac{\Theta(x)}{x}, \quad A_2 = \limsup_{x\to\infty} \frac{\Psi(x)}{x}, \quad A_3 = \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x}$$

$$a_1 = \liminf_{x\to\infty} \frac{\Theta(x)}{x}, \quad a_2 = \liminf_{x\to\infty} \frac{\Psi(x)}{x}, \quad a_3 = \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x}$$

Se trata de demostrar que

$$A_1 = A_2 = A_3 \quad y \quad a_1 = a_2 = a_3.$$

Sabemos que $A_1 \le A_2 \le A_3$ *y* $a_1 \le a_2 \le a_3$ *son consecuencia de las desigualdades*

$$\frac{\Theta(x)}{x} \le \frac{\Psi(x)}{x} \le \frac{\pi(x)}{x/\log x}$$

luego basta con probar que $A_3 \le A_1$, $a_3 \le a_1$.

Sea α, $0 < \alpha < 1$, tenemos que:

$$\begin{aligned}\Theta(x) = \sum_{p \le x} \log p &\ge \sum_{x^\alpha < p \le x} \log p > \alpha \log x \sum_{x^\alpha < p \le x} 1 \\ &= \alpha \log x \big(\pi(x) - \pi(x^\alpha)\big) \ge \alpha\big(\log x\big)\pi(x) - \alpha\big(\log x\big)x^\alpha.\end{aligned}$$

Luego:

$$\frac{\Theta(x)}{x} > \alpha \frac{\pi(x)}{x/\log x} - \alpha \frac{\log x}{x^{1-\alpha}}$$

pero como $\alpha < 1$ resulta que: $\lim_{x\to\infty} \dfrac{\log x}{x^{1-\alpha}} = 0$ y, por tanto,

$$A_1 = \limsup_{x\to\infty} \frac{\Theta(x)}{x} \ge \alpha \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x} = \alpha A_3$$

y dado que la desigualdad anterior es válida cualquiera que sea el número $\alpha < 1$, obtenemos que $A_1 \ge A_3$. La demostración de que $a_1 = a_2 = a_3$ se hace de igual manera. ■

Un corolario de la proposición anterior es que el Teorema de los números primos es equivalente a probar que

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

Y aunque la función $\Psi(x)$ parece más artificial que $\pi(x)$ resulta que tiene propiedades analíticas más fáciles de manejar.

Lema 1. $\Theta(n) \le 2n \log 2$.

Demostración. *(Por inducción) Observemos que para $n = 1$ y $n = 2$ el lema es cierto:*

$$\begin{aligned} 0 = \Theta(1) &\le 2\log 2 \\ \log 2 = \Theta(2) &\le 4 \log 2. \end{aligned}$$

Consideremos el número combinatorio

$$M = \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m+1}$$

que aparece dos veces en el desarrollo

$$(1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k}, \qquad \text{por lo que: } M \le 2^{2m}.$$

Los primos p tales que $m+1 < p \le 2m+1$ dividen al numerador de M pero no a su denominador, por lo tanto el producto de todos ellos es un divisor de M. En particular:

$$\prod_{m+1 < p < 2m+1} p \le M.$$

Tomando logaritmos resulta que:

$$\Theta(2m+1) - \Theta(m+1) \leq \log M \leq 2m \log 2.$$

Estamos ahora en condiciones de completar el argumento de inducción: Suponiendo que el lema es cierto para $k \leq n$, es decir $\Theta(k) \leq 2k \log 2$, consideremos $\Theta(n+1)$. Tenemos dos casos:

1º) Si $n+1$ es par, entonces $n+1$ no puede ser primo ($n > 1$) luego

$$\Theta(n+1) = \Theta(n) \leq 2n \log 2 \leq 2(n+1) \log 2$$

por hipótesis de inducción.

2º) Si $n+1 = 2m+1$ es impar, entonces:

$$\begin{aligned} \Theta(n+1) = \Theta(2m+1) &\leq 2m \log 2 + \Theta(m+1) \\ &\leq 2m \log 2 + 2(m+1) \log 2 = 2(2m+1) \log 2 \\ &= 2(n+1) \log 2. \end{aligned}$$

Y el argumento de inducción queda completo. ■

Lema 2. $\liminf_{x \to \infty} \dfrac{\Psi(x)}{x} \geq \log 2.$

Demostración. *Consideremos el número combinatorio*

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{a(p)} \leq \prod_{p \leq 2n} p^{\left[\frac{\log(2n)}{\log p}\right]}$$

Observemos que N es el término central, y el mayor, del desarrollo:

$$2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$$

luego $N \geq \dfrac{2^{2n}}{2n+1}$. Tomando logaritmos obtenemos:

$$2n \log 2 - \log(2n+1) \leq \log N \leq \sum_{p \leq 2n} \log p \Big[\frac{\log(2n)}{\log p}\Big] = \Psi(2n).$$

Para cualquier real positivo x tenemos que:

$$\begin{aligned} \Psi(x) \geq \Psi\big(2[\tfrac{x}{2}]\big) &> 2[\tfrac{x}{2}] \log 2 - \log\big(2[\tfrac{x}{2}] + 1\big) \\ &> x \log 2 - 2 \log 2 - \log\big(2[\tfrac{x}{2}] + 1\big) \end{aligned}$$

lo que implica la desigualdad: $\liminf_{x \to \infty} \dfrac{\Psi(x)}{x} \geq \log 2.$ ■

Corolario. (Teorema de Chebychev) *Existen dos constantes positivas* $0 < c \leq 1 \leq C < \infty$ *tales que:*

$$c\,\frac{x}{\log x} \leq \pi(x) \leq C\,\frac{x}{\log x}.$$

Proposición. (Postulado de Bertrand) *Para cualquier natural* n *existe al menos un primo* p *tal que* $n < p \leq 2n$.

Demostración. *El caso* $n \leq 520$ *lo podemos comprobar directamente en nuestra tabla de números primos. Por ejemplo, observando que el conjunto de primos* 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521 *tiene la propiedad de que cada uno es mayor que su precedente, pero menor que el doble de este.*

Para $n > 520$ *vamos a demostrar que la hipótesis de que el intervalo* $n < x \leq 2n$ *no contenga a ningún primo es absurda, produce una contradicción.*

Veamos: supongamos que no existe un primo p *tal que* $n < p \leq 2n$. *Consideremos el número*

$$N = \binom{2n}{n} = \frac{(2n!)}{(n!)^2}$$

y observemos que ningún primo p *en el intervalo* $2n/3 < p \leq n$ *puede ser divisor de* N. *La razón estriba en que* $4n/3 < 2p \leq 2n$ *por lo que el numerador* $(2n!)$ *es divisible por* p^2, *pero no por* p^3, *y lo mismo le ocurre al denominador* $(n!)^2$. *Luego el cociente* N *no puede ser divisible por* p. *La hipótesis de inducción implica entonces que* N *no es divisible por ningún* $p \geq \frac{2}{3}n$. *Es decir:*

$$N = \prod_{p \leq \frac{2}{3}n} p^{a(p)} = \prod_{p \leq (2n)^{1/2}} p^{a(p)} \cdot \prod_{(2n)^{1/2} < p \leq \frac{2}{3}n} p^{a(p)}$$

Observemos que:

1º) $p^{a(p)} \leq p^{\frac{\log(2n)}{\log p}} = 2n$ *para todo* p.

2º) Si $p > (2n)^{1/2}$, $a(p) \leq \left[\dfrac{\log(2n)}{\log p}\right] \leq 1$.

3º) $\Theta(m) \leq 2m \log 2$, *es decir:* $\displaystyle\prod_{p \leq m} p \leq 2^{2m}$.

4º) $2^{2n} < (2n+1)N$.

Luego:

$$\frac{2^{2n}}{2n+1} < N \leq (2n)^{(2n)^{1/2}} \cdot 2^{\frac{4}{3}n}.$$

O sea:

$$2^{\frac{2}{3}n} < (2n)^{(2n)^{1/2}} \cdot (2n+1).$$

Tomando logaritmos obtenemos la relación:

$$\Big(\frac{2}{3}\log 2\Big)n < \sqrt{2n}\,\log(2n) + \log(2n+1)$$

que resulta ser falsa cuando $n > 520$. ■

Ejercicios

16) *Demuéstrese que existen infinitos primos de las formas* $4n-1$ *y* $6n-1$.

17) *Demostrar que si* $2^m + 1$ *es un primo impar,* m *es una potencia de* 2.

18) *Demostrar que existen dos constantes positivas* $0 < c < C < \infty$ *tales que*

$$cn\log n < p_n < Cn\log n,$$

donde p_n *es el enésimo número primo.*

19) *Sea* $n = p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}$ *la descomposición de* n *en factores primos.*

i) Demuestra que n *tiene* $(n_1+1)(n_2+1)\cdots(n_s+1)$ *divisores positivos.*

ii) Indica cuántos divisores enteros (positivos y negativos) tiene n.

20) *Demuestra que*

$$\Big(\frac{a}{(a,b)}, \frac{b}{(a,b)}\Big) = 1\,.$$

21) *Encuentra todas las parejas* $a, b \in \mathbb{Z}$ *tales que* $(a,b) = 10$ *y* $[a,b] = 100$.

22) *Sea* q *un número entero tal que* $q \geq 1$. *Calcula* (q, q^2), $(q, q+1)$ *y* $(q, q+2)$.

23) *Dados* m *enteros consecutivos:* n, $n+1$, $n+2, \ldots, n+(m-1)$, *con* $m > 1$. *Demuestra que uno y solamente uno es divisible por* m.

24) *En una parada de autobús llegan tres líneas de autobuses: A, B y C. El autobús de la línea A tarda en hacer el recorrido completo 40 minutos; el de la línea B, una hora; y el de la línea C, 25 minutos. A las siete de la mañana han coincidido en la parada los tres autobuses. ¿A qué hora volverán a coincidir?*

25) *Sean* a, b, d *naturales no nulos tales que* $a = a_1 d$ *y* $b = b_1 d$ *con* $a_1, b_1 \in \mathbb{N}$. *Demuestra que si* $(a_1, b_1) = 1$ *entonces* $d = (a,b)$.

26) *Sean a, b, m números naturales con a y b coprimos. Demuestra que si $a|m$ y $b|m$ entonces $ab|m$. Encuentra un contraejemplo que muestre que si a y b no son coprimos el resultado no es cierto en general.*

27) *Demuestra que para todo $n \in \mathbb{N}$, $\sqrt{n} \in \mathbb{Q} \Leftrightarrow \sqrt{n} \in \mathbb{N}$.*

28) *Demuestra que todo número entero se puede expresar como combinación lineal de* 1001 *y* 30.

3

Los enteros

Queda curvo el firmamento,
compacto azul, sobre el día.
Es el redondeamiento
del esplendor: mediodía.
Todo es cúpula. Reposa,
central sin querer, la rosa,
a un sol en cenit sujeta.
Y tanto se da el presente
que el pie caminante siente
la integridad del planeta.

Jorge Guillén
(Perfección)

La construcción formal del anillo de los números enteros, que en lo sucesivo designaremos con la letra $\mathbb{Z}$*, comienza considerando el producto cartesiano* $\mathbb{N} \times \mathbb{N}$ *del conjunto de los naturales por sí mismo.*

Los elementos $(a, b) \in \mathbb{N} \times \mathbb{N}$ *son, pues, pares ordenados de números naturales* 0, 1, 2, 3, $\ldots$ *A continuación se establece una relación,* $\mathcal{R}$*, en* $\mathbb{N} \times \mathbb{N}$*, de acuerdo con el siguiente criterio:*

$$(a, b)\mathcal{R}(c, d) \text{ si y solo si } a + d = c + b.$$

Ejemplo 1: *Los pares* $(4, 2)$ *y* $(9, 7)$ *están relacionados:* $(4, 2)\mathcal{R}(9, 7)$*, por cuanto* $4{+}7 = 9{+}2$*. En cambio,* $(1, 1)$ *y* $(6, 7)$ *no lo están, ya que* $1{+}7 \neq 1{+}6$*.*

La relación que hemos definido goza de varias propiedades interesantes. A saber:

Reflexiva. Todo par está relacionado consigo mismo: $(a, b)\mathcal{R}(a, b)$*, puesto que* $a + b = a + b$*.*

Simétrica. Si $(a, b)\mathcal{R}(c, d)$ *entonces* $(c, d)\mathcal{R}(a, b)$ *ya que*

$$a + d = c + b \iff c + b = a + d.$$

Transitiva. Si $(a, b)\mathcal{R}(c, d)$ *y* $(c, d)\mathcal{R}(e, f)$*, entonces* $(a, b)\mathcal{R}(e, f)$*.*

Quizá la propiedad transitiva requiera alguna línea que nos aclare su cumplimiento. Ahora bien:

$$\begin{aligned}(a,b)\mathcal{R}(c,d) &\iff a+d=c+b\\ (c,d)\mathcal{R}(e,f) &\iff c+f=e+d.\end{aligned}$$

Sumando miembro a miembro ambas igualdades obtenemos:

$$a+d+c+f=c+b+e+d$$

que equivale a $a+f=e+b$, *es decir:* $(a,d)\mathcal{R}(e,f)$.

Como vimos en el primer capítulo, estas tres propiedades caracterizan a las relaciones llamadas de equivalencia, que pueden ser definidas en muchos otros conjuntos. Una de sus consecuencias más interesantes es que nos permiten dividir el conjunto $\mathbb{N}\times\mathbb{N}$ *en clases disjuntas, que llamaremos clases de equivalencia, de la siguiente manera:*

Definición. *La clase de equivalencia* $[(a,b)]$ *es el conjunto de todas las parejas* (c,d) *que están relacionadas con* (a,b)*:*

$$[(a,b)]=\{(c,d)\in\mathbb{N}\times\mathbb{N}\mid (a,b)\mathcal{R}(c,d)\}.$$

Ejemplo 2:

i) $[(2,0)]=\{(2,0),(3,1),(4,2),(5,3),(6,4),(7,5),(8,6),\dots\}$

ii) $[(3,6)]=\{(0,3),(1,4),(2,5),(3,6),(4,7),(5,8),(6,9),\dots\}$

Observemos que dadas dos clases, $[(a,b)]$ *y* $[(c,d)]$, *ora coinciden,* $[(a,b)]=[(c,d)]$, *ya son disjuntas,* $[(a,b)]\cap[(c,d)]=\emptyset$.

Efectivamente: si $[(a,b)]\cap[(c,d)]\neq\emptyset$ *tendrán, por lo menos, un elemento común:* (e,f). *Pero* $(e,f)\in[(a,b)]$ *si y solo si* $(e,f)\mathcal{R}(a,b)$, *y* $(e,f)\in[(c,d)]$ *si y solo si* $(e,f)\mathcal{R}(c,d)$. *Entonces por las propiedades simétrica y transitiva, resulta que* $(a,b)\mathcal{R}(c,d)$*: todo elemento de la clase* $[(a,b)]$ *está en* $[(c,d)]$, *y viceversa. Luego:* $[(a,b)]=[(c,d)]$.

Por tanto las clases de equivalencia dan lugar a una partición disjunta del conjunto $\mathbb{N}\times\mathbb{N}$ *y forman un nuevo conjunto (cuyos elementos son esas clases) que denominaremos conjunto cociente de* $\mathbb{N}\times\mathbb{N}$ *por la relación de equivalencia* $\mathcal{R}$. *En símbolos:*

$$(\mathbb{N}\times\mathbb{N})/\mathcal{R}.$$

Pues bien, este es el conjunto de los enteros, $\mathbb{Z}$*:*

$$\mathbb{Z}=(\mathbb{N}\times\mathbb{N})/\mathcal{R}.$$

En $\mathbb{Z}$ podemos definir dos operaciones, suma y producto, por el procedimiento siguiente:

$$\begin{aligned}[(a,b)] + [(c,d)] &= [(a+c, b+d)] \\ [(a,b)] \times [(c,d)] &= [(ac+bd, ad+bc)].\end{aligned}$$

Naturalmente, para que las definiciones anteriores sean correctas, hay que demostrar que, tanto la suma como el producto, son independientes de los representantes elegidos. Se trata del siguiente ejercicio:

Comprobar que si $(a,b)\mathcal{R}(a',b')$ y $(c,d)\mathcal{R}(c',d')$, entonces:

$$\begin{aligned}(a+c, b+d) &\quad \mathcal{R} \quad (a'+c', b'+d') \\ (ad+bc, ac+bd) &\quad \mathcal{R} \quad (a'd'+b'c', a'c'+b'd').\end{aligned}$$

Ejercicio 1. *Demostrar que la suma y el producto en $\mathbb{Z}$ verifican:*

1. *La suma es asociativa:*

$$\big([(a,b)] + [(c,d)]\big) + [(e,f)] = [(a,b)] + \big([(c,d)] + [(e,f)]\big).$$

2. *La suma es conmutativa:*

$$[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)].$$

3. *La clase $[(0,0)]$ es el elemento neutro para la suma:*

$$[(a,b)] + [(0,0)] = [(0,0)] + [(a,b)] = [(a,b)].$$

4. *La clase $[(b,a)]$ es el elemento opuesto de $[(a,b)]$. Es decir:*

$$[(b,a)] + [(a,b)] = [(a,b)] + [(b,a)] = [(0,0)].$$

5. *El producto es asociativo (enunciar y demostrar).*

6. *El producto es conmutativo (enunciar y demostrar).*

7. *La clase $[(1,0)]$ es el elemento neutro para el producto:*

$$[(1,0)] \times [(a,b)] = [(a,b)] \times [(1,0)] = [(a,b)].$$

8. *El producto es distributivo respecto de la suma:*

$$[(a,b)] \times ([(c,d)] + [(e,f)]) = [(a,b)] \times [(c,d)] + [(a,b)] \times [(e,f)].$$

La frase "$\mathbb{Z}$ es un anillo conmutativo con elemento unidad", resume el hecho de que $\mathbb{Z}$ está dotado de dos operaciones, suma y producto, que gozan de todas las propiedades anteriores. Pero en las matemáticas hay otros muchos conjuntos que tienen la misma estructura, por lo que se han dedicado esfuerzos a estudiar los resultados generales que pueden obtenerse con ella. Se trata de la Teoría de Anillos.

¿En qué se parece un número natural a un entero? Según la definición que hemos dado, la respuesta sería que no en mucho: un entero es una clase de equivalencia de pares ordenados de números naturales, lejos por tanto de ser un número natural.

Empero, esa respuesta es poco satisfactoria por cuanto el propósito original era "extender" los naturales para poder siempre restar y no crear unos objetos tan complicados. En realidad la situación se apaña de la manera siguiente:

> *Si la clase $[(a,b)]$ tiene un representante, (a,b), tal que $a > b$, entonces, también tiene al elemento $(a-b,0)$. Diremos que el entero $[(a,b)]$ es positivo y lo escribiremos: $[(a,b)] = +(a-b)$. Si, en cambio, $a < b$, entonces contiene al elemento $[(0,b-a)]$ y diremos que el entero $[(a,b)]$ es negativo, y lo designaremos por $-(b-a)$. Queda, claro está, el caso en que $a = b$, entonces la clase $[(a,a)]$ contiene al elemento $[(0,0)]$, y diremos que $[(a,a)]$ es el número entero 0. El entero $-1 = [(0,1)]$ verifica que $(-1)^2 = 1$ y, junto con 1, forman las unidades del anillo que son los elementos que tienen un inverso multiplicativo.*

Ahora estamos en condiciones de identificar a $\mathbb{N}$ con un subconjunto de $\mathbb{Z}$, el de los números positivos más el 0. Sea la aplicación:

$$\begin{array}{ccl} \mathbb{N} & \stackrel{\Phi}{\longrightarrow} & \mathbb{Z} \\ n & \longrightarrow & \Phi(n) = [(n,0)] = +n \\ 0 & \longrightarrow & \Phi(0) = [(0,0)] = 0. \end{array}$$

Obsérvese que Φ conserva las sumas y los productos:

$$\begin{aligned} \Phi(n+m) &= \Phi(n) + \Phi(m) \\ \Phi(n \cdot m) &= \Phi(n) \cdot \Phi(m) \end{aligned}$$

Se trata de una aplicación inyectiva que nos da una biyección entre $\mathbb{N}$ y $\Phi(\mathbb{N})$. En este sentido, en lo sucesivo, diremos que $\mathbb{N}$ es un subconjunto de $\mathbb{Z}$, e identificaremos el natural n con el entero $+n$.

En $\mathbb{Z}$ tenemos una extensión natural del orden $\leq$ de los naturales: $a \leq b$ si y solo si $b - a$ es positivo o cero. Una noción importante es la de valor absoluto $|a|$ que es el miembro no negativo de la pareja $\{a, -a\}$. Es claro que $|0| = 0$ y que $|a + b| \leq |a| + |b|$. También existe el algoritmo de la división: dados dos enteros a (dividendo) y $b \neq 0$ (divisor), hay dos únicos enteros c (cociente) y r (resto), tales que: $a = b \times c + r$, $0 \leq r < |b|$.

Dados dos enteros a y b, el conjunto $I = \{ax + by \mid x, y \in \mathbb{Z}\}$, es cerrado para la suma y para el producto por enteros de $\mathbb{Z}$:

$$\begin{aligned} (ax_1 + by_1) + (ax_2 + by_2) &= a(x_1 + x_2) + b(y_1 + y_2) \in I \\ z \cdot (ax + by) &= a(xz) + b(yz) \in I. \end{aligned}$$

Proposición. *Sean $a > 0$ y $b > 0$, entonces*

$$d = \text{ menor entero positivo en } I = m.c.d.(a, b).$$

Demostración. *Usaremos en esta prueba el siguiente resultado:*

Lema. *Todo elemento de I es múltiplo de d.*

Demostración. *Sea w un elemento de I y $w = d \times c + r$, $0 \leq r < d$ el resultado de su división por d.*
Entonces $r = w + d \times (-c)$ está en I por ser la suma de dos elementos de I. Como $0 \leq r < d$, tiene que ser $r = 0$ para no contradecir la propiedad "d es el menor entero positivo de I". ■

Sigamos ahora con la prueba de la proposición. Como $a = 1 \times a + 0 \times b$ y $b = 0 \times a + 1 \times b$ están en I, resulta que ambos son múltiplos de d. Por otro lado por ser $d \in I$ existen enteros x, y tales que:

$$d = ax + by.$$

Luego todo divisor común de a y de b ha de serlo también de d. Es decir:

$$d = m.c.d.(a, b).$$ ■

3.1. Clases de restos

La divisibilidad de los números naturales puede extenderse a la clase de los enteros. Sean a, b y $m > 1$ números enteros. Diremos que a es congruente con b módulo m si la diferencia $a - b$ es múltiplo de m, es decir $m|(a - b)$. La notación $a \equiv b \ mod(m)$ sirve para escribir esa relación, como hizo C. F. Gauss en su obra monumental Disquisitiones Arithmeticae (1801).

Los enteros a y b serán cualesquiera (positivos, negativos o cero), pero el módulo m lo tomaremos siempre mayor que uno. De la definición de congruencia se deduce fácilmente que goza de las tres propiedades:

i) *Reflexiva:* $a \equiv a \ mod(m)$, $\forall\, a \in \mathbb{Z}$.

ii) *Simétrica:* $a \equiv b \ mod(m) \implies b \equiv a \ mod(m)$.

iii) *Transitiva: Si* $a \equiv b \ mod(m)$ *y* $b \equiv c \ mod(m)$, *entonces* $a \equiv c \ mod(m)$.

Se trata pues de una relación de equivalencia que divide al conjunto $\mathbb{Z}$ *en clases disjuntas (llamadas clases de restos o clases residuales). El conjunto cociente, es decir, el conjunto de clases de equivalencia, se designa con el símbolo* $\mathbb{Z}_m$.

La aritmética modular forma parte de nuestra vida cotidiana: los días de la semana definen clases módulo 7 *y la hora la damos módulo* 24 *ya que a la pregunta "¿Qué hora es?" a nadie se le ocurriría responder con el número de horas transcurridas desde la Gran Explosión. Otro caso interesante es el Número de Identificación Fiscal (N.I.F.) cuya letra final depende solo de la clase residual, módulo* 23, *del número que la precede.*

Los enteros entre 0 *y* $m-1$ *están en clases residuales distintas. Todo entero* n *puede escribirse de forma única como:*

$$n = mc + r, \quad 0 \leq r \leq m-1,$$

por lo que resulta que todo entero es congruente, módulo m, *con uno de los números* $0, \ldots, m-1$ *(dos enteros son congruentes módulo* m *si y solo si dan el mismo resto al ser divididos por* m*). En particular existen exactamente* m *clases residuales distintas* $mod(m)$*:*

$\boxed{\mathbb{Z}_m \text{ tiene } m \text{ elementos.}}$

Un conjunto de m *enteros incongruentes entre sí dos a dos se llama un sistema residual completo módulo* m.

Proposición. *Sean* $a \equiv b \ mod(m)$ *y* $c \equiv d \ mod(m)$. *Tenemos que:*

i) $a + c \equiv b + d \ mod(m)$

ii) $ac \equiv bd \ mod(m)$.

La demostración es un ejercicio rutinario, pero que nos permite dotar a $\mathbb{Z}_m$ *con dos operaciones (suma y producto) que gozan de las propiedades de un anillo conmutativo con unidad.*

Si designamos con $[a]$ *y* $[b]$ *las clases respectivas,* $mod(m)$, *de los enteros* a *y* b, *tenemos que:*

$$\begin{aligned} [a] + [b] &= [a+b] \\ [a] \times [b] &= [a \times b]; \end{aligned}$$

y estas operaciones están bien definidas por ser independientes de los representantes escogidos en cada clase (comprobar esta afirmación).

Proposición. *Las operaciones suma y producto en $\mathbb{Z}_m$ tienen las propiedades siguientes:*

i) Conmutativa: $[a]+[b]=[b]+[a]$
$[a]\times[b]=[b]\times[a]$.

ii) Asociativa: $([a]+[b])+[c]=[a]+([b]+[c])$
$([a]\times[b])\times[c]=[a]\times([b]\times[c])$.

iii) Distributiva: $[a]\times([b]+[c])=[a]\times[b]+[a]\times[c]$.

iv) La clase del $[0]$ *es el elemento neutro para la suma, mientras que la del* $[1]$*, lo es para el producto.*

v) La clase $[m-a]$ *es el opuesto para la suma de la clase* $[a]$*:*

$$[m-a]+[a]=[0].$$

Además del conjunto $\{0,1,\ldots,m-1\}$ *hay otros muchos sistemas residuales completos. Un caso notable viene dado por la proposición siguiente.*

Proposición. *Si* $\{r_1,r_2,\ldots,r_m\}$ *es un sistema residual completo* $mod(m)$ *y si* $m.c.d.(a,m)=1$*, entonces* $\{ar_1,ar_2,\ldots,ar_m\}$ *es otro sistema residual completo* $mod(m)$*.*

Demostración. *Basta comprobar que los números* $\{ar_j\}_{j=1,\ldots,m}$ *son incongruentes entre sí dos a dos.*

Supongamos que $ar_j\equiv ar_k\ mod(m)$*. Por ser* $1=m.c.d.(a,m)$ *sabemos de la existencia de dos enteros* x*,* y *tales que* $1=ax+my$*. Luego:*

$$r_j\equiv ar_jx\ mod(m)\,,\qquad r_k\equiv ar_kx\ mod(m)$$

y la congruencia $ar_j\equiv ar_k\ mod(m)$ *implica que* $r_j\equiv r_k\ mod(m)$*, por lo que hemos de tener la igualdad* $j=k$*.* ■

Una cuestión importante es la de decidir cuándo un elemento de $\mathbb{Z}_m$ *tiene un inverso multiplicativo.*

Proposición. *La clase residual* $[a]\,mod(m)$ *tiene una inversa multiplicativa si y solo si* $m.c.d.(a,m)=1$*.*

Demostración. *Es fácil ver que si* $m.c.d.(a,m)=1$*, entonces tenemos también que* $m.c.d.(a',m)=1$ *para todo* $a'\equiv a\ mod(m)$*. De manera que la propiedad considerada en la proposición es independiente del representante elegido en la clase residual dada.*

Tenemos que $1=ax+my$ *para alguna pareja de enteros* x*,* y*. Luego* $ax\equiv 1\ mod(m)$ *y la clase* $[x]$ *es la inversa multiplicativa de la clase* $[a]$*.*

Recíprocamente, si $[a]\cdot[x]=[1]$*, entonces* $ax\equiv 1\ mod(m)$*. Es decir,* $1=ax+my$ *para algún entero* y*. De esta expresión se deduce que*

$$m.c.d.(a,m)=1.$$ ■

El número de elementos del conjunto $\{0, 1, \ldots, m-1\}$ *que son primos con* m *se designa con la función* $\phi(m)$ *(llamada función de Euler). Es también el número de clases residuales primas* $mod(m)$*, o número de clases residuales que admiten un inverso multiplicativo módulo* m*. El conjunto de estas últimas (subconjunto de* $\mathbb{Z}_m$*) se designa con la notación:*

$$\mathbb{Z}_m^* = \{ \text{ clases residuales primas con } m \},$$

y en ocasiones se habla de él como el conjunto de las unidades de $\mathbb{Z}_m$*, en cuyo caso se utiliza la notación* $U(\mathbb{Z}_m) = \mathbb{Z}_m^*$*.*

Un sistema residual reducido módulo m *consiste en un conjunto con un representante de cada clase residual prima.*

Ejemplos:

a) *Si* $m = p$ *es un número primo, entonces*

$$\phi(p) = p - 1$$

y $\{1, 2, \ldots, p-1\}$ *es un sistema residual reducido módulo* p*:*

$$\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}.$$

b) *Si* $m = p^k$*,* $k \geq 1$ *número natural, y* p *primo, entonces*

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1),$$

ya que, entre 1 *y* p^k*, los números que no son primos con* p*, y por lo tanto no son primos con* p^k*, son sus múltiplos:*

$$p,\ 2p,\ 3p,\ \ldots,\ p^{k-1}p$$

y hay p^{k-1} *de ellos.*

Proposición. *Sea* $m.c.d.(a, m) = 1$ *y* $\{r_1, \ldots, r_{\phi(m)}\}$ *un sistema residual reducido módulo* m*. Entonces* $\{ar_1, \ldots, ar_{\phi(m)}\}$ *también lo es.*

Demostración. *En primer lugar, cada elemento* ar_j *es primo con* m *y, por lo que vimos antes, tiene un inverso multiplicativo módulo* m*. Luego todas las clases* $[ar_j]$ *son primas con* m*. Basta entonces ver que son distintas, es decir, que* $ar_j \equiv ar_k \ mod(m)$ *implica que* $r_j \equiv r_k \ mod(m)$ *y, por tanto,* $r_j = r_k$*.*

Pero esto es una consecuencia de que a *tenga inverso multiplicativo,* x*, módulo* m*:* $ax \equiv 1 \ mod(m)$*. En efecto, multiplicando por* x *ambos miembros de la congruencia* $ar_j \equiv ar_k \ mod(m)$*, obtenemos*

$$xar_j \equiv xar_k \ mod(m) \implies r_j \equiv r_k \ mod(m). \qquad \blacksquare$$

Sea a primo con m ($m.c.d.(a,m)=1$) y $\{r_1,\ldots,,r_{\phi(m)}\}$ un sistema residual reducido módulo m. Entonces $\{ar_1,\ldots,ar_{\phi(m)}\}$ es otro sistema residual reducido módulo m. Por lo tanto, para cada j, $1\leq j\leq\phi(m)$, existe un único $k=f(j)$, $1\leq k\leq\phi(m)$ tal que

$$ar_j\equiv r_k\ mod(m)$$

es decir

$$\left.\begin{array}{rcl} ar_1 & \equiv & r_{f(1)} \\ ar_2 & \equiv & r_{f(2)} \\ & \vdots & \\ ar_{\phi(m)} & \equiv & r_{f(\phi(m))} \end{array}\right\} \ mod(m)$$

Multiplicando estas congruencias obtenemos que:

$$a^{\phi(m)}\,r_1r_2\cdots r_{\phi(m)}\equiv r_1r_2\cdots r_{\phi(m)}\ mod(m).$$

Si tenemos ahora en cuenta que cada r_j tiene un inverso multiplicativo módulo m, podemos simplificar, multiplicando por dichos inversos, y obtener la congruencia:

$$a^{\phi(m)}\equiv 1\ mod(m).$$

Teorema. *(Fermat–Euler). Si $m.c.d.(a,m)=1$, entonces*

$$a^{\phi(m)}\equiv 1\ mod(m).$$

Ejemplo 3: *Si $m=p$ es primo, entonces $a^p\equiv a\ mod(p)$ cualquiera que sea el entero a.*

Ejercicio 2. *¿Cuál es el resto de la división de 1324^{1000} entre 17?*

Proposición. *Si $m.c.d.(m,n)=1$, entonces $\phi(m\cdot n)=\phi(m)\cdot\phi(n)$.*

Demostración. *Consideremos los números entre 0 y $m\cdot n-1$, que forman un sistema residual completo módulo $m\cdot n$, dispuestos en filas de la manera siguiente:*

$$\begin{array}{rrcrcr} 0, & 1, & \ldots, & j, & \ldots, & n-1 \\ n, & n+1, & \ldots, & n+j, & \ldots, & 2n-1 \\ 2n, & 2n+1, & \ldots, & 2n+j, & \ldots, & 3n-1 \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ (m-1)n, & (m-1)n+1, & \ldots, & (m-1)n+j, & \ldots, & mn-1 \end{array}$$

Es decir, formando una matriz rectangular de m filas y n columnas.

Se trata de contar cuántos elementos de esta matriz son primos con n y con m simultáneamente. Cada fila es un sistema residual completo módulo n y, por tanto, contiene exactamente $\phi(n)$ clases residuales primas con n. Observemos que cada columna está formada por elementos congruentes entre sí módulo n. Así los elementos primos con n están ubicados en $\phi(n)$ columnas.

Ahora bien, cada columna es un sistema residual completo módulo m (puesto que $m.c.d.(n,m) = 1$), y, por tanto, contiene exactamente $\phi(m)$ elementos primos con m.

Uniendo ambos cómputos obtenemos $\phi(n)$ columnas primas con n, cada una de las cuales contiene exactamente $\phi(m)$ elementos primos con m, luego en total hay

$$\phi(n) \cdot \phi(m) \text{ elementos primos con } n \cdot m.$$ ■

Corolario. *Si $n = p_1^{a_1} \cdots p_k^{a_k}$ es la descomposición en factores primos del número n, resulta que:*

$$\begin{aligned} \phi(n) &= \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \\ &= (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) \\ &= p_1^{a_1} \cdots p_k^{a_k} \Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big) \\ &= n \prod_{p|n} \Big(1 - \frac{1}{p}\Big). \end{aligned}$$

Ejercicio 3. *Demostrar la fórmula de Gauss:*

$$\sum_{d|n} \phi(d) = n.$$

3.2. Ecuaciones en congruencias

Proposición. *Si $m.c.d.(a,m) = 1$, entonces la congruencia lineal*

$$ax \equiv b \ mod(m)$$

tiene exactamente una solución módulo m.

Demostración. *Sabemos que existen enteros s y t tales que $1 = as + mt$, es decir, $as \equiv 1 \ mod(m)$. Por lo tanto $b = asb + mtb$ nos da la solución $x = sb$: $b \equiv ax \ mod(m)$.*

Si tuviésemos dos soluciones: $ax_1 \equiv b \ mod(m)$, $ax_2 \equiv b \ mod(m)$

al restarlas obtendríamos:

$$a(x_1 - x_2) \equiv 0 \ mod(m),$$

y una sencilla multiplicación por s daría lugar a la congruencia:

$$x_1 - x_2 \equiv 0 \ mod(m).$$ ■

Proposición. *Si* $m.c.d.(a, m) = d$, *entonces la congruencia*

$$ax \equiv b \ mod(m)$$

tiene solución si y solo si $d \mid b$. *En caso afirmativo hay exactamente* d *soluciones módulo* m, *que podemos escribir en la forma:*

$$x_1,\ x_1 + m_1,\ \ldots,\ x_1 + (d-1)m_1$$

donde $m = dm_1$, *y* x_1 *es la solución de la congruencia* $a_1 x \equiv b_1 \ mod(m_1)$, $a = da_1$, $b = db_1$.

Demostración. *Si la congruencia tiene una solución* x *entonces podremos escribir* $ax = b + my$, *para un cierto entero* y. *Es decir:* $b = ax - my$ *y como* $d \mid a$ *y* $d \mid m$, d *debe ser un divisor de* $ax - my$, *es decir de* b. *Por tanto, una condición necesaria para que* $ax \equiv b \ mod(m)$ *tenga solución es que* $d = m.c.d.(a, m)$ *sea divisor de* b.

Supongamos ahora que ese es el caso: $a = da_1$, $b = db_1$ *y* $m = dm_1$ *siendo* $m.c.d.(a_1, m_1) = 1$.

La congruencia $a_1 x \equiv b_1 \ mod(m_1)$ *tiene una única solución* x_1 *módulo* m_1, *como demostramos en la proposición anterior.*

Pero la clase residual de x_1 *módulo* m_1 *se desdobla en exactamente* d *clases residuales distintas módulo* $m = d \cdot m_1$, *a saber:*

$$x_1,\ x_1 + m_1,\ \ldots,\ x_1 + (d-1)m_1$$

que dan lugar a las d *soluciones distintas de la congruencia*

$$ax \equiv b \ mod(m)$$

■

Ejercicio 4. *Hallar todas las soluciones de la ecuación*

$$60x \equiv 24 \ mod(48).$$

Las congruencias polinómicas (de grado mayor que uno) son algo más complicadas. No obstante, cuando el módulo es primo, tenemos el siguiente resultado de Lagrange:

Proposición. *Sea* p *primo y* $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ *un polinomio de grado* n *con coeficientes enteros, tales que* $c_n \not\equiv 0 \ mod(p)$. *Entonces la congruencia* $f(x) \equiv 0 \ mod(p)$ *tiene, a lo más,* n *soluciones.*

Demostración. *(Por inducción). El caso* $n = 1$ *ha sido analizado anteriormente y resulta cierto.*

Supongamos cierta la proposición P_k para $k \leq n$. Si x_1 es un solución de $c_0 + c_1 x + \cdots + c_{n+1} x^{n+1} \equiv 0 \ mod(p)$, entonces la ecuación

$$c_1(x - x_1) + \cdots + c_{n+1}(x^{n+1} - x_1^{n+1}) \equiv 0 \ mod(p)$$

debe ser satisfecha por cualquier otra solución. Observemos que

$$(x^k - x_1^k) = (x - x_1)(x^{k-1} + x^{k-2} x_1 + \cdots + x_1^{k-1}),$$

es decir:

$$c_1(x - x_1) + \cdots + c_{n+1}(x^{n+1} - x_1^{n+1}) = (x - x_1)(a_0 + a_1 x + \cdots + a_n x^n),$$

para ciertos enteros a_j tales que $a_n = c_{n+1} \not\equiv 0 \ mod(p)$.

Como p es primo, las soluciones de nuestra congruencia distintas de x_1 deben serlo también de $a_0 + a_1 x + \cdots + a_n x^n \equiv 0 \ mod(p)$ y, por la hipótesis de inducción, existen a lo sumo n de ellas. Luego P_{n+1} es también verdadera. ■

Corolario. *Si la congruencia $c_0 + c_1 x + \cdots + c_n x^n \equiv 0 \ mod(p)$ tiene más de n soluciones, entonces los coeficientes c_0, c_1, ..., c_n han de ser múltiplos de p.*

Ejemplo 4: *$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \ mod(p)$. El polinomio tiene grado $p-2$ y, sin embargo, tiene $p-1$ soluciones por el pequeño teorema de Fermat. Luego todos sus coeficientes son múltiplos de p. En particular el término independiente:*

$$(p-1)! + 1 \equiv 0 \ mod(p).$$

El caso de un sistema de congruencias de primer grado.

Consideremos un sistema de congruencias de primer grado:

$$\left.\begin{array}{c} a_1 x \equiv b_1 \ mod(m_1) \\ \cdots\cdots \\ a_n x \equiv b_n \ mod(m_n) \end{array}\right\}$$

del que suponemos que cada una de las ecuaciones, por separado, admite solución y, por lo tanto, puede ser llevado a la forma equivalente:

$$\left.\begin{array}{c} x \equiv x_1 \ mod(m_1) \\ \cdots\cdots \\ x \equiv x_n \ mod(m_n) \end{array}\right\}$$

Teorema. (Teorema chino del resto) *Si los módulos son primos entre sí dos a dos, entonces el sistema admite una solución única módulo* $M = m_1 \cdot \ldots \cdot m_n$.

Demostración. *Bajo la hipótesis* $m.c.d.(m_i, m_j) = 1$, *para* $i \neq j$ *podemos escribir:*

$$M = m_1 \cdots m_n = m_1 M_1 = m_2 M_2 = \cdots = m_n M_n$$

y calcular los inversos multiplicativos

$$M_1',\ M_2',\ \ldots,\ M_n',$$

de $M_1, \ldots, M_n$ *respecto de los módulos* $m_1, \ldots, m_n$ *respectivamente. Es decir:*

$$M_1 M_1' \equiv 1\ mod(m_1),\ \ldots,\ M_n M_n' \equiv 1\ mod(m_n).$$

Entonces las soluciones del sistema son: $x \equiv x_0\ mod(M)$, *donde* $x_0 = M_1 M_1' x_1 + \cdots + M_n M_n' x_n$.

Efectivamente, es claro que:

$$\left.\begin{array}{l} x_0 \equiv M_1 M_1' x_1 \equiv x_1\ mod(m_1) \\ x_0 \equiv M_2 M_2' x_2 \equiv x_2\ mod(m_2) \\ \quad \ldots\ldots \\ x_0 \equiv M_n M_n' x_n \equiv x_n\ mod(m_n) \end{array}\right\}$$

Por otro lado cualquier solución de

$$x \equiv x_j\ mod(m_j)$$

ha de ser, necesariamente, solución de $x \equiv x_0\ mod(m_j)$ *y, puesto que*

$$m.c.d.(m_i, m_j) = 1,\ i \neq j,$$

esto fuerza a $x \equiv x_0\ mod(m_1 \cdots m_n)$. ■

Ejemplo 5: *Resolver el sistema:*

$$\left.\begin{array}{r} 2x \equiv 1\ mod(3) \\ 7x \equiv 2\ mod(5) \\ 10x \equiv 4\ mod(7) \end{array}\right\}$$

Como $2 \times 2 \equiv 1\ mod(3)$, $7 \times 3 \equiv 1\ mod(5)$, $10 \times 5 \equiv 1\ mod(7)$ *el sistema es equivalente a:*

$$\left.\begin{array}{l} x \equiv 2\ mod(3) \\ x \equiv 6 \equiv 1\ mod(5) \\ x \equiv 20 \equiv 6\ mod(7) \end{array}\right\}$$

Sea $M = 3 \times 5 \times 7 = 105$, *y*

$$\begin{aligned} M_1 &= 5 \times 7 = 35 \equiv 2 \ mod(3) \\ M_2 &= 3 \times 7 = 21 \equiv 1 \ mod(5) \\ M_3 &= 3 \times 5 = 15 \equiv 1 \ mod(7). \end{aligned}$$

Entonces, $M_1' = 2$, $M_2' = 1$, $M_3' = 1$ *verifican:*

$$\left.\begin{array}{l} M_1 M_1' \equiv 1 \ mod(3) \\ M_2 M_2' \equiv 1 \ mod(5) \\ M_3 M_3' \equiv 1 \ mod(7) \end{array}\right\}$$

Luego la solución buscada es:

$$x = 35 \times 2 \times 2 + 21 \times 1 \times 1 + 15 \times 1 \times 6 = 251 \equiv 41 \ mod(105).$$

3.3. Bases de numeración. Aritmética binaria

Hay 10 *tipos de personas en el mundo, quienes conocen el sistema binario y quienes no lo conocen*

Nuestro sistema decimal de numeración es una maravilla y está basado en el uso de diez cifras o dígitos y un algoritmo que atribuye a cada dígito un valor que depende de su posición relativa. Por ejemplo

$$\begin{aligned} 2976 &= 2 \times 10^3 + 9 \times 10^2 + 7 \times 10 + 6 \\ \textit{mientras que} \quad 6792 &= 6 \times 10^3 + 7 \times 10^2 + 9 \times 10 + 2. \end{aligned}$$

Parece ser que su origen se remonta a los sumerios, siendo luego desarrollado por los indios y por los árabes. Su introducción en Europa suele atribuirse a la actividad de los comerciantes italianos de los siglos XIII *y* XIV *y se simboliza en Leonardo de Pisa, alias Fibonacci, quien fue ya mencionado en el capítulo 1, aunque hay sobrada evidencia de su introducción en España en tiempos del rey Alfonso X el Sabio.*

La operación de contar, y el propio nombre de dígitos, tiene una estrecha relación con los diez dedos de las manos, pero desde tiempos remotos se han utilizado también otros sistemas (recordemos que los huevos todavía se cuentan por docenas, la circunferencia se divide en trescientos sesenta grados, que la hora tiene sesenta minutos y el minuto sesenta segundos).

Dado un entero b *estrictamente mayor que uno, podemos establecer un sistema de numeración que consta de* b *dígitos, a saber* $0, \ldots, b-1$, *que constituyen un sistema residual completo módulo la base* b.

Si b es menor o igual que diez, entonces podemos bastarnos con los símbolos que ya conocemos, pero, en caso contrario, es conveniente inventarlos para los dígitos correspondientes a los números comprendidos entre 10 y $b-1$. Por ejemplo, en base doce podríamos utilizar el sistema:

$$0\,,\,1\,,\,2\,,\,\ldots\,,\,9\,,\,\alpha\,,\,\beta$$

donde α = diez, β = once son los símbolos que habría que añadir a los habituales del sistema decimal.

La expresión $x_k x_{k-1} \ldots x_2 x_1 x_0$, donde cada x_j es un dígito en nuestra base b, representa al entero:

$$x_0 + x_1 \times b + x_2 \times b^2 + \cdots + x_k \times b^k.$$

Ejemplos:

a) *En base 4 tenemos cuatro dígitos $\{0,1,2,3\}$. El número 3012 escrito en base cuatro corresponde (es igual) a*

$$2 + 1 \times 4 + 0 \times 4^2 + 3 \times 4^3 = 198$$

en el sistema decimal.

b) *En base 5 los dígitos son $\{0,1,2,3,4\}$ y el número mil novecientos cuarenta y nueve se escribe de la siguiente manera 30244. A veces resulta conveniente escribirlo en la forma $30244_{(5}$ que especifica la base de numeración adoptada. Usando pues esta notación tenemos la igualdad:*

$$1949_{(10} = 30244_{(5}.$$

c) *En base doce (usando el convenio anterior α = diez, β = once) resulta que el número $\alpha 17 \beta$ se convierte en:*

$11+7\times12+1\times12^2+10\times12^3 = 17519$ *escrito en el sistema decimal.*

Ejercicio 5. *Cambios de sistemas de numeración.*

5.1. *Escribir en las bases de numeración $b = 2\,,\,5\,,\,8\,,\,12$ los siguientes números dados en base diez:* $1711\,,\,25348\,,\,343$.

5.2. *Encontrar la expresión en base 10 de los números siguientes:*

$$12345_{(7}\,,\,1011101_{(2}\,,\,201201_{(3}.$$

El caso particular $b = 2$ es de especial importancia por ser el sistema natural usado internamente en los computadores modernos, debido a su fácil adaptación a las características de los circuitos electrónicos.

En el sistema binario cada número natural está representado por una fila de ceros y unos. Por ejemplo:

Binario	*Decimal*
0	*0*
1	*1*
10	*2*
11	*3*
100	*4*
101	*5*
110	*6*
111	*7*
1000	*8*
⋮	⋮
111100011	*483*

Aritmética binaria

Las reglas de la suma binaria son idénticas a las del sistema decimal. La tabla elemental es la siguiente:

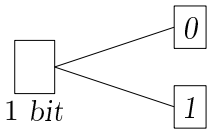
$$\begin{aligned} 0+0 &= 0 \\ 0+1 &= 1 \\ 1+1 &= 10 \end{aligned}$$

donde la tercera fila ilustra el latiguillo de "me llevo" cuando la suma excede a dos (a diez en el caso del sistema decimal). Ejemplo:

$$\begin{array}{cccccc} & & 1 & 1 & 0 \\ + & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 1 \end{array}$$

Ejercicio 6. *Recuperar la aritmética de la infancia haciendo cuentas (sumas, restas, multiplicaciones y divisiones) en el sistema binario.*

Los computadores representan datos en forma de sucesiones de bits. Un bit es la unidad mínima de almacenamiento de información en una memoria, y puede adquirir dos estados 0 *o* 1*. Resulta que toda la información que recibe, almacena o produce un computador es, en última instancia, un rosario de bits. Esta es la razón por la que el sistema binario es el natural para los ordenadores:*



dos estados posibles

Un grupo de ocho bits, un octeto, suele designarse por byte en el argot de la computación y tiene $2^8 = 256$ *estados posibles:*

0	1	1	0	0	0	1	1
1	0	1	0	0	1	0	1

Los múltiplos, kilobyte, megabyte, gigabyte, terabyte... forman parte del lenguaje común para describir la capacidad de memoria de los ordenadores. Pero hay que tener en cuenta que estamos en el sistema binario y un kilobyte, abreviadamente 1 KB, no es equivalente a 1.000 *bytes sino a* $2^{10} = 1.024$ *bytes. Similarmente un megabyte, 1 MB, es igual a* 1.024 $KB = 1.048.576$ *bytes mientras que:*

$$\begin{aligned}
&1\ GB = 1\,gigabyte = 1024\,MB = 2^{30}\ B\\
&1\ TB = 1\,terabyte = 1024\,GB = 2^{40}\ B\\
&1\ PB = 1\,petabyte = 1024\,TB = 2^{50}\ B\\
&1\ EB = 1\,exabyte\ = 1024\,PB = 2^{60}\ B\\
&1\ YB = 1\,yotabyte = 1024\,EB = 2^{70}\ B\\
&1\ ZB = 1\,zetabyte = 1024\,YB = 2^{80}\ B.
\end{aligned}$$

3.4. Ejemplos de ecuaciones diofánticas

Diofanto, como Euclides, fue un miembro distinguido de la escuela de Alejandría cuya obra sobrevivió al incendio de la Biblioteca. Escribió un tratado sobre las soluciones enteras de ecuaciones algebraicas cuyos coeficientes son también números enteros. Traducido al latín influyó decisivamente en la matemática europea del siglo XVII*, especialmente en Pierre de Fermat, quien usó los márgenes de un ejemplar del* libro de Diofanto *para escribir muchas de sus observaciones y descubrimientos.*

Consideremos la ecuación $ax + by = c$ *donde* a, b *y* c *son números enteros y, siguiendo a Diofanto, preguntémonos sobre soluciones en* $\mathbb{Z}$. *Es decir parejas de enteros* $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ *que verifiquen la identidad:* $am + bn = c$.

Es claro que si $d = m.c.d.(a, b)$ *no es un divisor de* c *entonces la ecuación carece de soluciones. Lo que demostró Diofanto es que esta condición necesaria es también suficiente. Veamos:*

Sean $d = m.c.d.(a, b)$, $a = da_1$, $b = db_1$, $c = dc_1$, *entonces resolver la ecuación* $ax + by = c$ *es equivalente a encontrar las soluciones de la ecuación*

$$a_1 x + b_1 y = c_1.$$

Por lo tanto, nuestro problema se reduce al caso en que los coeficientes a *y* b *son primos entre sí.*

Proposición. *La ecuación diofántica* $ax + by = c$, $m.c.d.(a, b) = 1$ *tiene como soluciones la familia:*

$$\begin{cases} x = sc + bn \\ y = tc - an \end{cases} \qquad n \in \mathbb{Z}$$

siendo s *y* t *dos enteros tales que* $as + bt = 1$.

Demostración. *Por ser* $m.c.d.(a, b) = 1$ *el algoritmo de Euclides nos permite encontrar dos enteros* s *y* t *tales que* $as + bt = 1$. *Multiplicando esta ecuación por* c *obtenemos una solución particular* $x_0 = sc$, $y_0 = tc$ *de la ecuación diofántica:* $ax_0 + by_0 = c$.

Ahora bien

$$a\big(x_0 + bn\big) + b\big(y_0 - an\big) = ax_0 + by_0 = c$$

cualquiera que sea el entero $n \in \mathbb{Z}$. *Por otro lado, si* (x, y) *es una solución, restando las identidades*

$$ax + by = c \quad y \quad ax_0 + by_0 = c$$

obtenemos $a(x - x_0) = b(y_0 - y)$.

Luego a *por ser primo con* b *debe dividir a* $y_0 - y$. *Análogamente* b *es un divisor de* $x - x_0$, *y la identidad anterior fuerza las igualdades:* $y_0 - y = an$, $x - x_0 = bn$ *para un mismo entero* n. *Es decir:*

$$x = x_0 + bn \qquad y = y_0 - an$$

luego la solución (x, y) *pertenece a la familia.* ■

Ejemplo 6: *El libro de Diofanto contiene una colección de ejemplos parecidos al siguiente.*

Problema: Una señora va de compras y se gasta un total de 900 *euros en vestidos (*137 *euros la unidad), camisas (*41 *euros la unidad) y camisetas (a* 13 *euros cada una). En total ha adquirido* 16 *prendas. ¿Cuántas compró de cada clase?*

Sean $x =$ *número de vestidos*
$y =$ *número de camisas*
$z =$ *número de camisetas.*

Entonces

$$\left.\begin{array}{rcl} x + y + z & = & 16 \\ 137x + 41y + 13z & = & 900 \end{array}\right\}$$

Sustituimos:

$$137x + 41y + 13\big(16 - x - y\big) = 900$$

luego, $124x + 28y = 692$. *Es decir,*

$$31x + 7y = 173.$$

Tenemos que

$$31 \times (-2) + 7 \times 9 = 1$$

por lo tanto:

$$\begin{aligned} x &= -2 \times 173 + 7n \\ y &= 9 \times 173 - 31n\,, \qquad n \in \mathbb{Z} \end{aligned}$$

es la solución general de la ecuación diofántica.

Para acabar el problema tenemos ahora que determinar los valores del parámetro n que originan soluciones válidas al enunciado de la compra: $x \geq 0$, $y \geq 0$, $z \geq 0$. Ahora bien

$$x \geq 0 \Longleftrightarrow 7n \geq 2 \times 173 \quad \Longleftrightarrow n \geq \frac{2 \times 173}{7} = 49 + \frac{3}{7} \quad \Longleftrightarrow n \geq 50$$

$$y \geq 0 \Longleftrightarrow 31n \leq 9 \times 173 \quad \Longleftrightarrow n \leq \frac{9 \times 173}{31} = 50 + \frac{7}{31} \quad \Longleftrightarrow n \leq 50$$

luego solo nos queda la posibilidad de tomar $n = 50$, y obtenemos:

$$\begin{aligned} x &= -2 \times 173 + 7 \times 50 = 4 \\ y &= 9 \times 173 - 31 \times 50 = 7 \\ z &= 16 - 11 = 5 \end{aligned}$$

que es la solución buscada.

Las ecuaciones diofánticas pueden tener más variables x, y, z, ... También podemos considerar polinomios con coeficientes enteros de grado mayor. Un ejemplo notable es la ecuación $x^2 + y^2 = z^2$ que fue estudiada por los pitagóricos y cuyas soluciones originan todos los triángulos rectángulos de lados enteros. Por ejemplo: $3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$, ...

Proposición. *(Ternas Pitagóricas). Las soluciones enteras de la ecuación $x^2 + y^2 = z^2$ son las siguientes:*

$$\left\{ \begin{array}{rcl} x &=& 2m\,n \\ y &=& n^2 - m^2 \\ z &=& n^2 + m^2 \end{array} \right. \qquad \left\{ \begin{array}{rcl} x &=& n^2 - m^2 \\ y &=& 2m\,n \\ z &=& n^2 + m^2 \end{array} \right.$$

donde m y n son enteros arbitrarios.

Es decir obtenemos dos familias biparamétricas de soluciones: dando cualquier valor entero a los parámetros m y n obtenemos una terna. Sustituyendo en la primera obtenemos:

$$\begin{aligned} m = 1\,,\, n = 2 \quad &\Longrightarrow \quad x = 4\,,\, y = 3\,,\, z = 5 \\ m = 1\,,\, n = 3 \quad &\Longrightarrow \quad x = 6\,,\, y = 8\,,\, z = 10 \\ &\cdots\cdots \end{aligned}$$

La ecuación $x^2 + y^2 = z^2$ es simétrica en las variables x, y, lo que explica la duplicidad en las familias de soluciones.

Demostración. *Es claro que si multiplicamos las tres componentes de una terna pitagórica por el mismo número obtenemos otra de ellas:*

$$\text{si } x^2 + y^2 = z^2 \text{ entonces } (nx)^2 + (ny^2) = (nz)^2 \ \forall n \in \mathbb{Z}.$$

Luego para conocer todas las soluciones de $x^2 + y^2 = z^2$ basta con que nos limitemos a encontrar las primitivas, es decir aquellas en las que

$$m.c.d.(x, y) = m.c.d.(y, z) = m.c.d.(x, z) = 1.$$

En este caso solo uno de los números x, y, z puede ser par y los otros dos impares. Pero es fácil ver que z no es el par ya que si $x = 2m+1$, $y = 2n+1$ y $z = 2p$ entonces:

$$x^2 + y^2 = (2m + 1)^2 + (2n + 1)^2 = 4(m^2 + n^2 + m + n) + 2 \neq 4p^2 = z^2.$$

Sin pérdida de generalidad podemos pues suponer que $x = 2x_1$ y así

$$x^2 = 4x_1^2 = (z - y)(z + y) \implies x_1^2 = \frac{z - y}{2} \cdot \frac{z + y}{2}.$$

Los enteros $\frac{z-y}{2}$, $\frac{z+y}{2}$ son primos entre sí ya que cualquier divisor común lo debería también ser de su suma z y de su diferencia y. Al ser su producto el cuadrado perfecto x_1^2 cada uno de ellos debe ser igual, a su vez, a un cuadrado perfecto:

$$\frac{z + y}{2} = n^2\,, \qquad \frac{z - y}{2} = m^2.$$

Por tanto:

$$\begin{cases} z &= n^2 + m^2 \\ y &= n^2 - m^2 \\ x &= 2m\,n \end{cases}$$

que es lo que queríamos probar. ■

Según la leyenda Pierre de Fermat se sintió fascinado por estos resultados y en su ejemplar del libro de Diofanto sugirió haber encontrado una ingeniosa demostración de que la ecuación

$$x^n + y^n = z^n\,, \qquad x \cdot y \cdot z \neq 0\,, \quad n \geq 3$$

carece de soluciones enteras, pero que el margen a su disposición no era suficiente para dar cabida a la prueba.

En 1994 A. Wiles logró culminar el esfuerzo de varias generaciones con una demostración cuya complicación excede el nivel de este libro, haciendo uso de ideas muy avanzadas respecto a las matemáticas conocidas en los tiempos de Fermat.

Existen dudas razonables acerca de si Fermat tenía, o no tenía, una demostración. No obstante, en el caso particular $n = 4$ sí nos legó un método ingenioso que la reduce al caso de las ternas pitagóricas: Fermat probó que la ecuación $x^4 + y^4 = z^2$ carece de soluciones no triviales, es decir tales que $x \cdot y \cdot z \neq 0$. Observemos que este resultado es más fuerte que afirmar la no existencia de tales soluciones para $x^4 + y^4 = z^4$ $(= (z^2)^2)$.

La demostración de Fermat es por reducción al absurdo. Supongamos que el conjunto de soluciones no triviales fuese distinto del vacío y escojamos una de ellas (x_0, y_0, z_0) de manera que z_0 sea mínimo (es claro que basta considerar enteros positivos x, y, z).

Esa solución "mínima" verifica que

$$m.c.d.(x_0, y_0) = m.c.d.(y_0, z_0) = m.c.d.(x_0, z_0) = 1$$

pues en caso contrario habría otra menor. Considerándola como una terna pitagórica

$$\left(x_0^2\right)^2 + \left(y_0^2\right)^2 = z_0^2$$

podemos concluir la existencia de dos enteros positivos m y n tales que:

$$\begin{aligned} x_0^2 &= 2mn \\ y_0^2 &= n^2 - m^2 \\ z_0 &= n^2 + m^2 \end{aligned}$$

siendo n y m de distinta paridad. Pero n no puede ser par porque entonces tendríamos la congruencia $y_0^2 \equiv -m^2 \equiv -1 \ mod(4)$ que carece de soluciones.

Luego $m = 2\,m_1$ para un entero m_1 y n es impar. Observemos que x_0 es también par, $x_0 = 2\,x_1$, y que los enteros m y n son primos entre sí. Tenemos que:

$$x_1^2 = m_1 \cdot n$$

y como $m.c.d.(m_1, n) = 1$ resulta que ambos son cuadrados perfectos. Es decir:

$$m_1 = a^2\,, \qquad n = b^2$$

donde a y b son enteros positivos primos entre sí.

La terna pitagórica $y_0^2 + m^2 = n^2$ nos da la existencia de enteros c, d tales que:

$$\begin{aligned} m &= 2\,m_1 = 2cd \\ y_0 &= c^2 - d^2 \\ n &= c^2 + d^2 \end{aligned}$$

Comoquiera que $m.c.d.(c, d) = 1$ de la ecuación $cd = m_1 = a^2$ deducimos que $c = f^2$, $d = g^2$ son cuadrados perfectos. Sustituyendo en $n = c^2 + d^2$ obtenemos que

$$b^2 = n = c^2 + d^2 = f^4 + g^4$$

es otra solución de la ecuación original y como

$$b \leq b^4 = n^2 < n^2 + m^2 = z_0$$

tenemos una contradicción con la elección de z_0. *Esto nos permite concluir la demostración.* ■

Una ecuación diofántica general involucra expresiones (polinomios) en varias indeterminadas x_1, x_2, x_3, ..., x_n *del tipo*

$$\sum_{0 \leq a_j \leq d} C_{a_1 \ldots a_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = P(x_1, \ldots, x_n)$$

donde los coeficientes, $C_{a_1 \ldots a_n}$, *son números enteros y los exponentes,* a_j, *son enteros no negativos.*

La cuestión planteada es encontrar, si las hay, soluciones enteras, $x_j \in \mathbb{Z}$, $j = 1, \ldots, n$ *de la ecuación*

$$P(x_1, \ldots, x_n) = 0.$$

Con la ayuda de un computador, creando un programa adecuado, podemos ir evaluando el polinomio en los distintos valores enteros y comprobando si este se anula o no se anula, ordenándole que se pare la primera vez que encuentre una solución. Aunque para algunas ecuaciones haya que tener mucha paciencia, en principio podríamos así resolver aquellas que tienen soluciones enteras.

Pero, ¿qué ocurre con las que carecen de ellas? En este caso el computador seguiría ad nauseam y no se pararía. ¿Existe un algoritmo que permita saber a priori que esto no va a ocurrir?

Esta interesante pregunta fue uno de los problemas (el décimo) de la famosa lista que D. Hilbert elaboró en el congreso internacional celebrado en París en el año 1900. *La respuesta, como se dice ahora, es "pues va a ser que no", y fue obtenida por Yuri Matiyasevich basándose en los trabajos de Davis, Putnam y Robinson.*

La construcción de Matiyasevich tiene conexión con la Teoría de la computabilidad y con el famoso problema de la "parada" de las máquinas de Turing.

Ejercicios

1) *Hallar el resto de dividir entre* 13 *el número*

$$999\,998\,997 \ldots\ldots 003\,002\,001\,000.$$

2) *El número n expresado en base 2 tiene la expresión*

$$10010100111010100010100111.$$

Decidir si es múltiplo de 3.

3) *D. José estudió en un colegio que tenía entre 150 y 300 alumnos. Aunque no se acuerda del número exacto de ellos, sí se queja de no haber podido practicar el fútbol, el balonmano ni el baloncesto porque, cuando en cada deporte intentaban organizar el colegio en equipos, siempre faltaba o sobraba uno. ¿Cuántos colegiales había?*

4) *Probar el recíproco del teorema de Wilson: "si $(n-1)!+1 \equiv 0\ mod(n)$, entonces n es primo".*

5) *Probar que todo número de la forma $4n^2+1$ es producto de primos de la forma $4m+1$.*

6) *Hallar todos los p tales que p, $p+4$, $p+6$, $p+10$, $p+12$, $p+16$ y $p+22$ sean primos simultáneamente.*

7) *Hallar todas las soluciones de la congruencia*

$$x^3+2x^2-x+6 \equiv 0\ mod(14).$$

8) *Resolver las siguientes congruencias:*

i) $243x+17 \equiv 103\ mod(125)$;

ii) $6x+3 \equiv 4\ mod(10)$;

iii) $2x \equiv 16\ mod(14)$.

9) *Resolver las congruencias simultáneas:*

$$\left.\begin{array}{l} x \equiv 3\ mod(5) \\ 5x \equiv 7\ mod(8) \end{array}\right\}$$

10) *En una isla desierta, cinco hombres y un mono recogen cocos durante todo el día, y después se duermen. El primer hombre se despierta y decide tomar su parte. Divide los cocos en cinco grupos iguales y le sobra un coco que le da al mono. Después toma su parte y vuelve a dormirse. Entonces despierta el segundo, y haciendo un montón con los cocos que quedaron, lo divide en cinco partes iguales, y le sobra un coco, que da al mono. Sucesivamente ocurre lo mismo con cada uno de los tres hombres restantes. Se pide encontrar el número mínimo de cocos que formaban el montón original.*

11) *Escribir las tablas de sumar y de multiplicar en $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_6$ y $\mathbb{Z}_7$.*

12) *Demostrar que si dos números son primos entre sí, su suma y su diferencia son primos con su producto.*

13) *Demostrar que hay infinitos números primos en la progresión aritmética:*

$$a_n = 4n - 1\,, \qquad n = 1, 2, 3, \ldots$$

14) *Hallar fórmulas para la suma y el producto de todos los divisores del número cuya descomposición en factores primos es:* $m = p_1^{a_1} \cdots p_r^{a_r}$. *Aplicarlo al caso* $m = 617400$.

15) *Demostrar que el número* $2^{a-1}\big(2^a - 1\big)$ *es perfecto siempre que* $2^a - 1$ *sea primo. Dar ejemplos.*

16) *Calcular el resto* $mod(7)$ *de* 4525^{1000}.

17) *Demostrar que si* $2^n - 1$ *es primo entonces* n *es primo. ¿Es cierta la recíproca?*

18) *Encontrar una fórmula para todas las parejas* (x, y) *de enteros tales que*

$$133\,x - 355\,y = 1.$$

19) *Encontrar el entero positivo menor que da restos* $1, 2, \ldots, 9$, *respectivamente, cuando lo dividimos por* $2, 3, \ldots, 10$.

20) *Calcular los valores* n, $0 \leq n \leq 50$, *tales que* $\phi(n) = 2^a$ *para algún* $a \geq 0$.

21) *Si* p *es un primo impar y si* $a + b = p - 1$, *demostrar que*

$$a!\,b! \,+\, (-1)^a \equiv 0 \ mod(p).$$

22) *Resolver los sistemas*

$$\left.\begin{array}{l} x \equiv 3 \ mod(9) \\ x \equiv 5 \ mod(10) \\ x \equiv 7 \ mod(11) \end{array}\right\} \qquad \left.\begin{array}{l} 9x \equiv 3 \ mod(15) \\ 5x \equiv 7 \ mod(21) \\ 7x \equiv 4 \ mod(13) \end{array}\right\}$$

4

Los números racionales

> *... Porque me he dado cuenta de que sois la otra mitad. El vizconde que vive en el castillo, el malo, es una mitad. Y vos sois la otra mitad, que se creía perdida en la guerra y que ahora ha regresado. Es una mitad buena...*
>
> Italo Calvino
>
> *(El vizconde demediado)*

Los números enteros nos sirven para contar, sumar y restar. Pero es también importante dividir, pesar y medir.

Supongamos que queremos medir longitudes y que nuestra unidad es el metro. Con los números enteros podemos considerar cantidades tales como uno, dos o cinco mil metros. Pero todos sabemos que hay distancias más cortas que no llegan al metro, por ejemplo, medio metro, o distancias que están comprendidas entre dos múltiplos enteros consecutivos de la unidad, pero sin coincidir con ninguno de ellos, como es el caso de cinco metros y medio.

En principio, podríamos pensar que la situación se arregla cambiando la unidad de medida y adoptando como tal el medio metro, en cuyo caso el número 1 *representaría medio metro, mientras que* 11 *correspondería a los cinco metros y medio. Claro que esto no mejora mucho las cosas, ya que alguien podría tener el capricho, o la necesidad, de medir la tercera parte de un metro.*

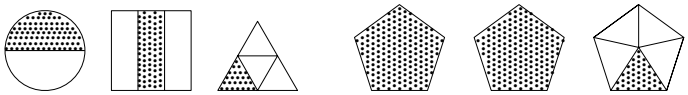
Bueno, quizás todavía haya esperanzas de manejarnos con los enteros si somos lo suficientemente perspicaces y adoptamos como unidad de medida la sexta parte de un metro. Entonces el número 3 *representaría medio metro,* 33 *a cinco metros y medio, y* 2 *a la tercera parte, pero alguien podría necesitar medir la séptima parte de un metro...*

El proceso de cambiar la unidad de medida, además de agotador, no parece tener mucho futuro. Lo que haremos, en su lugar, es introducir los números racionales.

4.1. Quebrados o fracciones

Ejemplos de quebrados o fracciones son: un medio, 1/2, un tercio, 1/3, un cuarto, 1/4, once quintos, 11/5, cinco catorceavos, 5/14, . . . ; en general:

Definición. *Una fracción a/b, $b \neq 0$, consta de un número entero a, llamado numerador, y otro b, necesariamente distinto de cero, que es el denominador.*



$$\frac{1}{2} \qquad \frac{1}{3} \qquad \frac{1}{4} \qquad\qquad 1 \quad + \quad 1 \quad + \quad \frac{1}{5} \quad = \quad \frac{11}{5}$$

Operaciones. *Las operaciones aritméticas, suma y producto, pueden también efectuarse con los quebrados, lo que confiere a estos características similares a los enteros.*

$$\begin{array}{lll}
\text{Suma:} & \dfrac{a}{b}+\dfrac{c}{d} & = \quad \dfrac{ad+bc}{bd} \\
\textit{Ejemplos:} & \dfrac{1}{3}+\dfrac{3}{4} & = \quad \dfrac{4+9}{12}=\dfrac{13}{12} \\
& \dfrac{5}{8}+\dfrac{2}{3} & = \quad \dfrac{5\times 3+2\times 8}{3\times 8}=\dfrac{31}{24} \\
\text{Producto:} & \dfrac{a}{b}\times\dfrac{c}{d} & = \quad \dfrac{a\times c}{b\times d} \\
\textit{Ejemplos:} & \dfrac{3}{7}\times\dfrac{4}{11} & = \quad \dfrac{12}{77} \\
& \dfrac{5}{4}\times\dfrac{2}{3} & = \quad \dfrac{10}{12}.
\end{array}$$

Ejercicio 1. *Realizar las operaciones siguientes:*

$$\frac{11}{10}+\frac{2}{3}; \quad \frac{1}{7}+\frac{-3}{2}; \quad \frac{1}{2}\times\left(\frac{1}{3}+\frac{1}{4}\right); \quad \frac{1}{2}\times\frac{1}{3}+\frac{1}{2}\times\frac{1}{4}.$$

4.2. Los números racionales

Los quebrados o fracciones tales como 1/2, 1/3 y 1/4 aparecen de manera natural a la hora de pesar y medir cantidades, pero también al dividir enteros. Sabemos que 2 no es divisible por 7, no existe ningún entero que multiplicado por 7 nos dé 2. Entre los enteros no siempre es posible hacer divisiones exactas. Sin embargo las fracciones nos proveen de un medio adecuado y cómodo para poder dividir enteros arbitrarios: el cociente del entero 2 por el 7 está descrito por la fracción 2/7.

Ahora bien, si esto es así, querremos que la fracción $2/1$ *sea equivalente al número* 2*, como también lo deben ser* $6/3$ *o* $4/2$*. Es decir, tendremos que establecer un criterio para saber cuándo dos fracciones son equivalentes o representan el mismo cociente. El criterio es el siguiente:*

Diremos que las fracciones a/b *y* c/d *son iguales y escribiremos:*

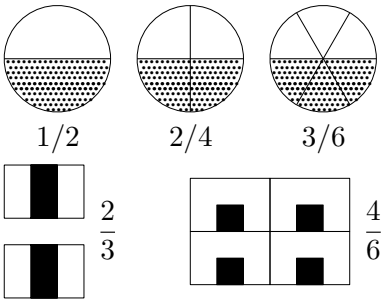
$$\frac{a}{b} = \frac{c}{d},$$

si se verifica que $ad = bc$*.*

Ejemplos: $\frac{1}{2} = \frac{2}{4}$ *ya que* $1 \times 4 = 2 \times 2$

$\frac{2}{4} = \frac{3}{6}$ *ya que* $2 \times 6 = 4 \times 3$

$\frac{2}{3} = \frac{4}{6}$ *ya que* $2 \times 6 = 3 \times 4$.



Es claro que esta relación es: reflexiva (toda fracción es igual a sí misma: $a/b = a/b$ *pues* $ab = ab$*); simétrica (si* $a/b = c/d$ *entonces* $c/d = a/b$*); y, sobre todo, transitiva, si* $a/b = c/d$ *y* $c/d = e/f$ *entonces* $a/b = e/f$ *(*$ad = bc$ *y* $cf = ed$*, igualdades que llevan a* $adf = bcf$ *y* $bcf = bed$*, de donde* $adf = bed$ *es decir,* $af = be$*).*

Estas tres propiedades (reflexiva, simétrica y transitiva) hacen que estemos ante una verdadera relación de equivalencia de fracciones, de manera que estas quedan clasificadas en clases disjuntas de equivalencia. En cada clase están todas las fracciones equivalentes a una dada.

$$\frac{2}{1} = \frac{4}{2} = \frac{6}{3} = \ \ldots\ldots\ = \frac{-2}{-1} = \frac{-4}{-2} = \frac{-6}{-3} = \quad \ldots$$
$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ \frac{4}{8} = \frac{5}{10} = \ \ldots\ = \frac{-1}{-2} = \frac{-2}{-4} = \quad \ldots$$
$$\frac{1}{3} = \frac{2}{6} = \frac{3}{9} = \frac{4}{12} = \frac{5}{15} = \ \ldots\ = \frac{-1}{-3} = \frac{-2}{-6} = \quad \ldots$$

Ejercicio 2. *Entre las fracciones siguientes detectar las que son iguales:*

$$\frac{-2}{7},\ \frac{2}{3},\ \frac{3}{13},\ \frac{105}{455},\ \frac{-5}{7},\ \frac{60}{84},\ \frac{15}{-105}.$$

Es fácil ver que cada clase contiene una única fracción irreducible a/b, esto es, una fracción cuyos numerador y denominador son enteros primos entre sí. Entonces el resto de las fracciones de la clase de equivalencia se obtienen a partir de la irreducible, a/b, sin más que multiplicar al numerador y al denominador por el mismo entero n:

$$\frac{a}{b}, \frac{2a}{2b}, \frac{3a}{3b}, \frac{4a}{4b}, \dots$$
$$\frac{1}{5}, \frac{2}{10}, \frac{3}{15}, \frac{4}{20}, \dots$$

En realidad hay una pega: hemos dicho que la fracción irreducible a/b es única en cada clase, pero esto no es estrictamente cierto ya que $(-a)/(-b) = a/b$ y si a/b es irreducible, resulta que $(-a)/(-b)$ también lo es (por ejemplo $(-2)/3 = 2/(-3)$).

Pero esta es la única ambigüedad posible y se resuelve aceptando el criterio de escoger a/b, si b es positivo, o $(-a)/(-b)$ si b es negativo (con lo cual $-b$ es positivo). En el ejemplo anterior nos quedaremos con $(-2)/3$.

Ejercicio 3. *Simplificar una fracción, a/b, consiste en encontrar otra equivalente cuyos términos sean primos entre sí. Simplificar:*

$$\frac{12}{20}, \frac{14}{84}, \frac{77}{1991}, \frac{260}{84}, \frac{665}{285}, \frac{17}{21}.$$

Fijémonos en el siguiente ejemplo:

$$\frac{60}{42} = \frac{3 \cdot 4 \cdot 5}{2 \cdot 3 \cdot 7} = \frac{10}{7}, \quad \text{o bien} \quad \frac{60}{42} = \frac{60:6}{42:6} = \frac{10}{7},$$

ya que $m.c.d.(60, 42) = 6$.

Reducir a común denominador varias fracciones consiste en encontrar fracciones equivalentes con el mismo denominador. Por ejemplo:

$$\frac{1}{4} = \frac{30}{120}, \ \frac{1}{5} = \frac{24}{120}, \ \text{y} \ \frac{1}{6} = \frac{20}{120},$$

son fracciones con denominador común $120 = 4 \times 5 \times 6$. La manera más eficiente es tomar como denominador común al mínimo común múltiplo de los denominadores. Así, en el ejemplo anterior tendríamos:

$$\frac{1}{4} = \frac{15}{60}, \ \frac{1}{5} = \frac{12}{60}, \ \text{y} \ \frac{1}{6} = \frac{10}{60},$$

al ser $60 = m.c.m.(4, 5, 6)$.

Definición. *Una clase de equivalencia de fracciones se llama un número racional y cualquiera de sus fracciones puede tomarse como un representante de la clase.*

El número racional "un medio" puede ser presentado por medio de las fracciones equivalentes:

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \frac{5}{10} = \dots$$

mientras que "dos tercios" tiene como fracciones representantes a:

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9} = \frac{8}{12} = \frac{10}{15} = \dots$$

El conjunto de los números racionales se designa por $\mathbb{Q}$ y de una manera natural contiene a $\mathbb{Z}$, el conjunto de los enteros, puesto que identificamos al entero n con el racional representado por la fracción $n/1$:

$\boxed{\mathbb{Z} \text{ es un subconjunto de } \mathbb{Q}.}$

Esta clasificación de los quebrados en clases es muy útil en el empeño de aumentar nuestra libertad de cálculo y poder dividir siempre. Es también una relación natural en el arte de pesar y medir. Es lo mismo tener dos cuartos que medio kilo de azúcar. Sin embargo, alguien podría objetar que no es lo mismo tener dos medio amigos que un amigo de verdad. Es decir, los racionales sirven para lo que sirven, que no es poco, pero no para medir amistades.

4.3. Operaciones con los números racionales

La suma y el producto de fracciones dan lugar a sendas operaciones entre los números racionales. El punto crucial es que si tenemos fracciones equivalentes a los sumandos (o factores), entonces las fracciones que resulten al sumar (o multiplicar), son también equivalentes. Es decir, la clase de equivalencia de la suma y del producto de dos fracciones solo depende de las clases de cada una de ellas.

Ejemplo 1: *Como* $\frac{2}{3} = \frac{4}{6}$ *y* $\frac{5}{7} = \frac{15}{21}$, *es fácil comprobar que:*

$$\begin{aligned} \frac{2}{3} + \frac{5}{7} &= \frac{29}{21} = \frac{174}{126} = \frac{4}{6} + \frac{15}{21} \\ \frac{2}{3} \times \frac{5}{7} &= \frac{10}{21} = \frac{60}{126} = \frac{4}{6} \times \frac{15}{21}. \end{aligned}$$

En general, si a/b y c/d son irreducibles, entonces toda fracción equivalente debe ser de la forma $(na)/(nb)$, $(mc)/(md)$ para ciertos enteros n y m.

Entonces:

$$\begin{aligned}\frac{na}{nb}+\frac{mc}{md} &= \frac{namd+nbmc}{nbmd}=\frac{(nm)(ad+bc)}{(nm)(bd)}\\ &= \frac{ad+bc}{bd}=\frac{a}{b}+\frac{c}{d}\\ \frac{na}{nb}\times\frac{mc}{md} &= \frac{namc}{nbmd}=\frac{(nm)(ac)}{(nm)(bd)}\\ &= \frac{ac}{bd}=\frac{a}{b}\times\frac{c}{d}.\end{aligned}$$

Denominador común. *La fórmula de la suma se simplifica notablemente si las fracciones tienen el mismo denominador:*

$$\frac{a}{d}+\frac{c}{d}=\frac{ad+dc}{d^2}=\frac{d(a+c)}{d^2}=\frac{a+c}{d}.$$

Si las fracciones tienen el mismo denominador, su suma se obtiene sumando los numeradores y manteniendo el denominador común.

Es una buena estrategia la de obtener fracciones equivalentes a los sumandos de denominador común antes de proceder a realizar la suma.

Propiedades:

Asociativa

$$\begin{cases}\textit{Suma:} & (\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})\\ \textit{Producto:} & (\frac{a}{b}\times\frac{c}{d})\times\frac{e}{f}=\frac{a}{b}\times(\frac{c}{d}\times\frac{e}{f})\end{cases}$$

Conmutativa

$$\begin{cases}\textit{Suma:} & \frac{a}{b}+\frac{c}{d}=\frac{a}{b}+\frac{c}{d}\\ \textit{Producto:} & \frac{a}{b}\times\frac{c}{d}=\frac{a}{b}\times\frac{c}{d}\end{cases}$$

Elemento neutro

$$\begin{cases}\textit{Suma:} & \frac{a}{b}+0=\frac{a}{b}\quad(0=\frac{0}{d},\ d\neq 0)\\ \textit{Producto:} & \frac{a}{b}\times 1=\frac{a}{b}\quad(1=\frac{c}{c},\ c\neq 0)\end{cases}$$

Elemento opuesto (suma): $\frac{a}{b}+\frac{-a}{b}=0$

Elemento inverso (producto): $\frac{a}{b}\times\frac{b}{a}=1$ *(si* $a\neq 0$, $b\neq 0$*)*

Distributiva: $\frac{a}{b}\times(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}\times\frac{c}{d}+\frac{a}{b}\times\frac{e}{f}.$

Estas propiedades nos simplifican muchos cálculos. Por ejemplo, la propiedad asociativa es muy importante ya que nos permite sumar (o multiplicar) cualquier número de fracciones en el momento en que sabemos hacerlo con dos de ellas, sin preocuparnos de la manera en que las vamos asociando. Es decir, para sumar $3/4$, $5/7$ *y* $2/11$, *podemos sumar primero:*

$$\frac{3}{4}+\frac{5}{7}=\frac{41}{28}$$

y al resultado añadirle $2/11$*:*

$$\frac{41}{28}+\frac{2}{11}=\frac{507}{308}\,,$$

o bien, añadirle $3/4$ *al resultado de sumar*

$$\frac{5}{7}+\frac{2}{11}=\frac{69}{77},\qquad \frac{3}{4}+\frac{69}{77}=\frac{507}{308}.$$

La propiedad asociativa nos permite escribir sumas del tipo:

$$\frac{1}{2}+\frac{2}{3}+\frac{3}{4}+\cdots+\frac{99}{100}$$

sin necesidad de indicar la manera precisa de cómo empezamos a sumar. Lo mismo ocurre con la multiplicación, y esto es un gran alivio, ya que sería horrible tener que andar con paréntesis,

$$\frac{1}{2}+\Big(\frac{2}{3}+\Big(\frac{3}{4}+\Big(\frac{4}{5}+\cdots+\Big(\frac{98}{99}+\frac{99}{100}\Big)\cdots\Big)\Big)\Big),$$

y con sumo cuidado de cómo se asocian los sumandos (o los factores) de sumas (o productos) múltiples. Gracias a la bendita propiedad asociativa eso no es necesario.

Finalmente, los números racionales pueden dividirse siempre que el divisor sea distinto de cero:

$$\boxed{\frac{a}{b}:\frac{c}{d}=\frac{a}{b}\times\frac{d}{c}=\frac{ad}{bc}.}$$

Potencias de números racionales. *La noción de potencia de un número entero tiene una extensión natural a los racionales. Veamos:*

$$\begin{aligned}\frac{a}{b}\times\frac{a}{b} &= \frac{a\times a}{b\times b}=\frac{a^2}{b^2}\\ \frac{a}{b}\times\frac{a}{b}\times\frac{a}{b} &= \frac{a\times a\times a}{b\times b\times b}=\frac{a^3}{b^3}\end{aligned}$$

En general definiremos: $\boxed{\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.}$

Las propiedades de las potencias de números enteros siguen siendo válidas para números racionales:

1) $q^n \times q^m = q^{n+m}$ 2) $(q \times r)^n = q^n \times r^n$

3) $(q^n)^m = q^{n \cdot m}$ 4) $q^0 = 1$ *cualquiera que sea el racional* $q \neq 0$.

Ejemplos:

$$\begin{aligned}
\left(\frac{2}{3}\right)^6 &= \frac{2^6}{3^6} = \frac{64}{729} \\
\left(\frac{1}{2}\right)^3 \cdot \left(\frac{1}{2}\right)^4 &= \left(\frac{1}{2}\right)^7 = \frac{1}{128} \\
\left(\frac{1}{2} \cdot \frac{3}{5}\right)^3 &= \left(\frac{1}{2}\right)^3 \cdot \left(\frac{3}{5}\right)^3 = \frac{1}{8} \cdot \frac{27}{125} = \frac{27}{1000} \\
\left\{\left(\frac{2}{3}\right)^2\right\}^3 &= \left(\frac{2}{3}\right)^6 = \frac{2^6}{3^6} = \frac{64}{729}.
\end{aligned}$$

4.4. Representación geométrica de los números racionales

Recordemos que entre los números enteros los hay positivos y negativos, además del cero. El orden $m \leq n$ *significa que* $n - m$ *no es negativo. Esta relación puede extenderse también a los números racionales.*

Relación de orden. *Dadas dos fracciones,* a/b *y* c/d*, con denominadores positivos, diremos que los números racionales que representan verifican*

$$\frac{a}{b} \leq \frac{c}{d}$$

($\leq$ *"menor o igual") si se verifica que* $bc - ad$ *es un entero no negativo.*

Ejemplos: $(1/2) \leq (3/2)$ *puesto que* $2 \times 3 - 1 \times 3 = 4$.

$(3/7) \leq (5/9)$ *puesto que* $7 \times 5 - 3 \times 9 = 8$.

El símbolo "$\geq$*" tiene el significado de "mayor o igual":*

$$\frac{c}{d} \geq \frac{a}{b} \quad \textit{si y solo si} \quad \frac{a}{b} \leq \frac{c}{d}.$$

Usaremos además los símbolos $<$ *y* $>$*, que designan a las desigualdades estrictas "menor" y "mayor" respectivamente.*

La relación de orden nos permitirá, en lo sucesivo, hablar de racionales positivos, los que son mayores que el cero, y negativos, los menores que él.

Es también importante la noción de valor absoluto $|a/b|$, que es el mayor entre a/b y $-(a/b)$:

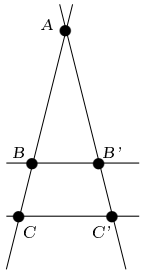
$$\left|\frac{a}{b}\right| = \text{máximo de } \left\{\frac{a}{b}, \frac{-a}{b}\right\}.$$

Ejemplos: $(2/3) \leq (4/6)$, $\quad (3/5) < (5/7)$, $\quad |(-2/3)| = (2/3)$

$$\left|\frac{3}{5} + \frac{-6}{7}\right| = \left|\frac{21-30}{35}\right| \leq \left|\frac{21}{35}\right| + \left|\frac{-30}{35}\right| = \left|\frac{3}{5}\right| + \left|\frac{-6}{7}\right| = \frac{3}{5} + \frac{6}{7}.$$

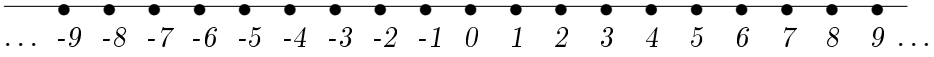
Teorema de Tales. *Los segmentos determinados por rectas paralelas en dos concurrentes son proporcionales.*

$$\frac{AB}{BC} = \frac{AB'}{B'C'}.$$



Si en una línea recta escogemos un origen, al que asociamos el número 0, y una ubicación para la unidad 1, automáticamente tenemos situados a todos los números enteros:

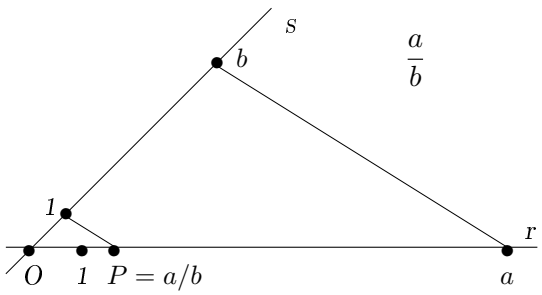
$$\mathbb{Z}$$



El entero n estará, a la derecha de 0 si es positivo, y a la izquierda si es negativo. En cualquiera de los casos distará $|n|$ unidades de longitud del origen.

Los números racionales también pueden representarse por puntos de la recta. Por ejemplo: a $1/2$ le corresponde el punto medio del segmento entre 0 y 1; a $3/4$ el punto medio entre $1/2$ y 1; etcétera.

En general, para representar el número racional $a/b \geq 0$ podemos proceder de la manera siguiente:

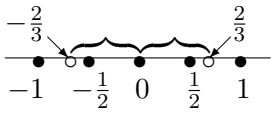


Trazamos una recta auxiliar que corta al eje por el origen. Con un compás marcamos los puntos situados a distancia a del origen, en la recta r, y b del origen, en la recta s. Unimos estos dos puntos por una recta y trazamos una paralela que pase por el punto 1 de la recta s. La recta así obtenida corta a r en un punto P, cuya distancia al origen OP verifica:

$$OP = \frac{OP}{1} = \frac{a}{b}$$

por el Teorema de Tales de Mileto.

El punto que representa a $(-2)/3$ está a la izquierda del origen y a la misma distancia que $2/3$.



Una observación sencilla, pero interesante, es que si a/b es mayor que c/d, entonces el punto que representa al primero está ubicado a la derecha del segundo.

El orden de $\mathbb{Q}$ tiene una diferencia muy importante con el de los enteros $\mathbb{Z}$. Entre los enteros sabemos que $n+1$ es el siguiente de n, pero con los racionales pasa todo lo contrario: entre dos racionales $(c/d) < (a/b)$ siempre podemos colocar otro, por ejemplo:

$$\frac{c}{d} < \frac{a+c}{b+d} < \frac{a}{b}.$$

Problema. *Encontrar un racional comprendido entre $2/3$ y $4/5$.*

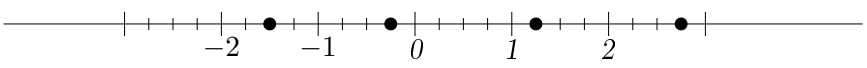
SOLUCIÓN: $\dfrac{2}{3} < \dfrac{2+5}{3+4} < \dfrac{5}{4}$. *La fracción $(a+c)/(b+d)$ es la mediana entre a/b y c/d.*

Ejercicios

1) *En una recta donde 0 es el origen y el segmento unidad es de 1 cm, representar los números*

$$1,\ 2,\ 3,\ \frac{1}{3},\ \frac{1}{5},\ \frac{1}{7},\ -\frac{3}{2},\ 0,\ -\frac{1}{5},\ \frac{7}{10},\ \frac{-18}{10},\ \frac{2}{10}\ .$$

2) *Los puntos de la recta marcados con un círculo se corresponden con números racionales. Calcúlense.*



3) *Dividir el segmento AB en cinco partes iguales usando la regla y el compás.*

4) *Dividir el segmento rectilíneo limitado por 0,9 y 1 en diez partes iguales. ¿Qué número racional corresponde a cada una de las partes obtenidas?*

5) *Ordenar de mayor a menor los números $1/3$, $7/4$, $-5/2$, 1 y $5/2$.*

6) *Considérense las fracciones positivas irreducibles y propias (numerador menor que denominador) cuyo denominador sea menor que 7, y ordénense de menor a mayor. Calcúlense las diferencias entre los términos consecutivos que se obtienen. ¿Se observa alguna propiedad interesante?*

4.5. Fracciones decimales

El sistema de numeración usual es el decimal, y es una maravilla. Con los diez dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9, podemos representar a cualquier número. Por ejemplo, dos mil cuatrocientos treinta y nueve:

$$2439 = 2\times 1000 + 4\times 100 + 3\times 10 + 9 = 2\times 10^3 + 4\times 10^2 + 3\times 10 + 9.$$

La concisión y la comodidad del sistema de numeración decimal resulta evidente si la comparamos, por ejemplo, con la numeración romana o la babilónica. Sumar y multiplicar "a la romana" es mucho más complicado.

No es de extrañar que las fracciones cuyo denominador es una potencia de 10 desempeñen un papel especial y, de ahora en adelante, las llamaremos fracciones decimales.

Como ejemplo podemos tomar:

$$\frac{2349}{10\,000} = \frac{9 + 4\times 10 + 3\times 100 + 2\times 1000}{10\,000} = \frac{2}{10} + \frac{3}{10^2} + \frac{4}{10^3} + \frac{9}{10^4}$$

que, en perfecta consonancia con la expresión decimal de los números enteros, escribiremos en la manera abreviada:

$$\frac{2349}{10\,000} = \frac{2}{10} + \frac{3}{10^2} + \frac{4}{10^3} + \frac{9}{10^4} = 0{,}2349.$$

Usaremos pues la notación $0{,}abcd\ldots$, donde cada letra representa a uno de los diez dígitos, para designar al número:

$$0{,}abcd\ldots = \frac{a}{10} + \frac{b}{10^2} + \frac{c}{10^3} + \frac{d}{10^4} + \ldots$$

que son las fracciones decimales propias.

En general una fracción decimal positiva puede tener una parte entera distinta de cero:

$$243{,}728 = 243 + \frac{7}{10} + \frac{2}{10^2} + \frac{8}{10^3} = 2\times 10^2 + 4\times 10 + 3 + \frac{7}{10} + \frac{2}{10^2} + \frac{8}{10^3}.$$

El número 243 *es la parte entera de la fracción* 243,728*, y escribiremos* $243 = [243{,}728]$*, usando el corchete* $[x]$ *para designar a la parte entera del número racional* x*, es decir al "mayor entre los enteros menores o iguales que* x*":*

$$[1{,}2] = 1, \quad \left[\frac{5}{2}\right] = 2, \quad \left[\frac{-7}{3}\right] = -3.$$

Una de las ventajas de la notación decimal es la siguiente: multiplicar por 10 *una fracción decimal equivale a correr la coma un lugar a la derecha; dividir por* 10 *es lo mismo que trasladar la coma un lugar hacia la izquierda.*

$$\begin{aligned} 10 \times 243{,}728 &= 10\left(2\times 10^2 + 4\times 10 + 3 + \frac{7}{10} + \frac{2}{10^2} + \frac{8}{10^3}\right) \\ &= 2\times 10^3 + 4\times 10^2 + 3\times 10 + 7 + \frac{2}{10} + \frac{8}{10^2} \\ &= 2437{,}28; \end{aligned}$$

$$\begin{aligned} 243{,}728 : 10 &= \left(2\times 10^2 + 4\times 10 + 3 + \frac{7}{10} + \frac{2}{10^2} + \frac{8}{10^3}\right) : 10 \\ &= 2\times 10 + 4 + \frac{3}{10} + \frac{7}{10^2} + \frac{2}{10^3} + \frac{8}{10^4} \\ &= 24{,}3728. \end{aligned}$$

Toda fracción decimal es igual a un entero más una fracción decimal propia, es decir, contenida entre 0 *y* 1*:* $0 \le 0{,}abcde\ldots < 1$.

Veamos cómo son las fracciones decimales propias.

En la primera generación, es decir con una sola cifra decimal, tenemos las fracciones:

$$0 = \frac{0}{10} < \frac{1}{10} < \frac{2}{10} < \frac{3}{10} < \frac{4}{10} < \frac{5}{10} < \frac{6}{10} < \frac{7}{10} < \frac{8}{10} < \frac{9}{10} < \frac{10}{10} = 1$$

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

$$I_0 \quad I_1 \quad I_2 \quad I_3 \quad I_4 \quad I_5 \quad I_6 \quad I_7 \quad I_8 \quad I_9$$

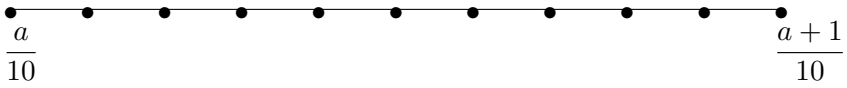
que dividen al intervalo entre 0 *y* 1 *en diez partes que hemos designado* I_j*,* $j = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$*. De manera que* I_0 *consta de los números* q *entre* 0 *y* 1/10 *(*$0 \le q < 1/10$*);* I_1 *contiene a aquellos* q *tales que* $1/10 \le q < 2/10$*;* $q \in I_2$ *quiere decir que* $2/10 \le q < 3/10$*, y así sucesivamente.*

La segunda generación de fracciones son las que obtenemos con dos cifras decimales y hay $100 = 10^2$ *de ellas:* $a/10 + b/100$ *donde* a *y* b *toman cada una los diez valores:* 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Es claro que

$$\frac{a}{10} \leq \frac{a}{10} + \frac{b}{100} < \frac{a+1}{10}\,,$$

luego, para un a *fijo, las fracciones* $a/10+b/100$ *forman, al variar* b *entre* 0 *y* 9, *una partición del intervalo* I_a *en diez intervalos iguales, con extremos:* $a/10$, $a/10 + 1/100$, $a/10 + 2/100$, ..., $a/10 + 9/100$, $a/10 + 10/100 = (a+1)/10$



Tenemos pues 100 *intervalos que designaremos con la notación* $I_{a,b}$. *Así el intervalo* $I_{a,b}$ *contiene a todos los racionales* q *tales que:*

$$\frac{a}{10} + \frac{b}{100} \leq q < \frac{a}{10} + \frac{b+1}{100}.$$

Por ejemplo: $I_{1,3}$ *consta de los números* q *tales que:*

$$\frac{1}{10} + \frac{3}{100} \leq q < \frac{1}{10} + \frac{4}{100}$$

como pueden ser: $133/1000$, $137/1000$, $132/1000 = 33/250$, ...

Observemos que la longitud de un intervalo de la primera generación, que es la distancia entre sus extremos, vale $1/10$, *mientras que en la segunda generación miden* $1/100$.

Si continuamos la construcción, las fracciones de la tercera generación

$$\frac{a}{10} + \frac{b}{100} + \frac{c}{1000}\,,$$

se obtienen al dividir cada intervalo, $I_{a,b}$, *de la segunda generación en diez partes iguales. Tenemos pues* 1000 *fracciones decimales de la tercera generación, y* 1000 *intervalos disjuntos* $I_{a,b,c}$, *de longitud* $1/1000$; *y así sucesivamente.*

Una pregunta natural, a estas alturas, es la de saber qué números racionales tienen representantes que sean fracciones decimales. Ejemplos inmediatos son: $1/10$, $7/10 + 2/(10^4)$; *pero también* $1/5$ *ya que* $1/5 = 2/10$, $1/2 = 5/10$, *y* $13/(2^3 5^2) = (13 \times 5)/(2^3 5^3) = (65)/(1000)$.

Por el contrario $\dfrac{1}{3}$ *no es una fracción decimal ya que la igualdad* $\dfrac{1}{3} = \dfrac{n}{10^k}$ *implica que* $10^k = 3n$, *que es absurda por cuanto* 3 *no es divisor de* 10^k.

Estos ejemplos ilustran el siguiente resultado, que no es más que una sencilla consecuencia del Teorema Fundamental de la Aritmética:

> *La fracción irreducible a/b es decimal si y solo si los únicos factores primos del denominador, b, son 2 y 5. En otras palabras, si y solo si el denominador es de la forma $b = 2^n 5^m$.*

Luego $1/3$ no es una fracción decimal, pero, sin embargo, podemos aproximarla por fracciones decimales, tanto como queramos:

$$\begin{aligned}
0 &\leq \frac{1}{3} < 1;\\
0{,}3 = \frac{3}{10} &\leq \frac{1}{3} < \frac{4}{10} = 0{,}4;\\
0{,}33 = \frac{3}{10} + \frac{3}{100} &\leq \frac{1}{3} < \frac{3}{10} + \frac{4}{100} = 0{,}34;\\
0{,}333 = \frac{3}{10} + \frac{3}{100} + \frac{3}{1000} &\leq \frac{1}{3} < \frac{3}{10} + \frac{3}{100} + \frac{4}{1000} = 0{,}334;\\
&\cdots\cdots
\end{aligned}$$

En general, es fácil comprobar que:

$$0{,}333\ldots333 < \frac{1}{3} < 0{,}333\ldots334.$$

Definición. *La fracción propia q tiene como desarrollo decimal la expresión $0{,}abcde\ldots$ si se verifica que:*

$$\begin{aligned}
\frac{a}{10} &\leq q < \frac{a+1}{10};\\
\frac{a}{10} + \frac{b}{100} &\leq q < \frac{a}{10} + \frac{b+1}{100};\\
\frac{a}{10} + \frac{b}{100} + \frac{c}{1000} &\leq q < \frac{a}{10} + \frac{b}{100} + \frac{c+1}{1000};
\end{aligned}$$

y así sucesivamente. En otras palabras: el desarrollo decimal del número q nos da información precisa sobre los intervalos decimales de cada generación a los que pertenece el número q.

Ejemplos: *El desarrollo decimal de $2/3$ es $0{,}66666\ldots$:*

$$\begin{aligned}
\frac{6}{10} &< \frac{2}{3} < \frac{7}{10}\\
\frac{6}{10} + \frac{6}{100} &< \frac{2}{3} < \frac{6}{10} + \frac{7}{100}\\
\frac{6}{10} + \frac{6}{100} + \frac{6}{1000} &< \frac{2}{3} < \frac{6}{10} + \frac{6}{100} + \frac{7}{1000}\\
&\cdots\cdots
\end{aligned}$$

El desarrollo decimal de $4/3$ *es* $1{,}33333\ldots$
Para verlo basta observar que $4/3 = 1 + 1/3$, *luego:*

$$\begin{aligned}
1 + \frac{3}{10} &< 1 + \frac{1}{3} < 1 + \frac{4}{10} \\
1 + \frac{3}{10} + \frac{3}{100} &< 1 + \frac{1}{3} < 1 + \frac{3}{10} + \frac{4}{100} \\
1 + \frac{3}{10} + \frac{3}{100} + \frac{3}{1000} &< 1 + \frac{1}{3} < 1 + \frac{3}{10} + \frac{3}{100} + \frac{4}{1000} \\
&\ldots\ldots
\end{aligned}$$

La interpretación geométrica de las cifras decimales es muy sugestiva y describe maravillosamente cómo aproximar un número racional arbitrario por fracciones decimales, con el grado de precisión que se desee. Sin embargo parece complicada de implementar para calcular efectivamente las cifras decimales.

Por el contrario, en la escuela primaria, todos aprendimos aquel magnífico algoritmo de la división: se añade un cero a la derecha del dividendo y se prosigue la división después de poner una coma en la última cifra entera del cociente.

```
1          |3
10           0,333333...
 10
  10
   10
    10
     10
      10
       1...
```

Afortunadamente ambos algoritmos, el geométrico y el de la escuela primaria, coinciden:

El primer cociente, 0, *es la parte entera de* $1/3$, $0 = [1/3]$, *o bien:* $1 = 0 \times 3 + 1$.
La primera cifra decimal se calcula según la regla:

$$\frac{a}{10} \leq \frac{1}{3} < \frac{a+1}{10}\,,$$

es decir: $a \leq (10/3) < a + 1$. *Luego,* $a = [10/3] = 3$, *que corresponde al segundo paso de la división anterior: se añade un* 0 *al primer resto, que es* 1, *y lo que resulta,* 10, *se divide por* 3, *dando como cociente* 3 *que es la primera cifra decimal y así sucesivamente.*

Ejemplos:

$7 \quad \lfloor 6$ $10 \quad 1{,}166\ldots$ 40 40 $4\ldots$	$13 \quad \lfloor 11$ $20 \quad 1{,}1818\ldots$ 90 20 90 $2\ldots$

Todos los ejemplos tienen algo importante en común: los desarrollos decimales de los números racionales son muy previsibles, se repiten a partir de un término en adelante, son periódicos.

Si nos detenemos un poco a pensar en el proceso de obtención de las cifras decimales, nos convenceremos de que la periodicidad no es una sorpresa. Por el contrario, es lo que cabe esperar, ya que los restos sucesivos de las divisiones son siempre menores que el divisor y, por lo tanto, tendrán que repetirse desde uno en adelante.

Todo número racional q tiene un desarrollo decimal de la forma

$$m, xy\ldots z\,abc\ldots e\,abc\ldots e\,abc\ldots e\,abc\ldots e$$
$$= m, xy\ldots z\,\overbrace{abc\ldots e}$$

que es periódico desde un término en adelante:

- $m = [q]$ *es la parte entera;*
- $xy\ldots z$ *designan las cifras del anteperiodo;*
- $abc\ldots e$ *son las cifras que se repiten, o que forman el periodo. Es tradicional usar la notación* $\overbrace{abc\ldots e}$ *para designarlo.*

Ejemplos:

$$\frac{1}{3} \quad \textit{tiene como desarrollo} \quad 0,\overset{\frown}{3}$$
$$\frac{7}{6} \quad \textit{tiene como desarrollo} \quad 1{,}1\overset{\frown}{6}$$
$$\frac{13}{11} \quad \textit{tiene como desarrollo} \quad 1,\overset{\frown}{18}$$
$$\frac{7227}{999} \quad \textit{tiene como desarrollo} \quad 7,\overbrace{234}$$

La propiedad anterior tiene una recíproca que también es verdadera:

"Todo desarrollo decimal periódico proviene de un número racional".

Ejemplos: *a)* $0{,}232323\cdots = 0{,}\overset{\frown}{23}$. *Una manera inteligente de proceder sería la siguiente: supongamos que hay un racional* q *con ese desarrollo, entonces ha de verificarse que:*

$$\begin{aligned} 0{,}23 &\leq q < 0{,}24 \\ 0{,}2323 &\leq q < 0{,}2324 \\ 0{,}232323 &\leq q < 0{,}232324 \\ &\cdots \end{aligned}$$

Si multiplicamos por 100 *estas desigualdades obtenemos:*

$$\begin{aligned} 23 &\leq 100q < 24 \\ 23{,}23 &\leq 100q < 23{,}24 \\ 23{,}2323 &\leq 100q < 23{,}2324 \\ &\cdots \end{aligned}$$

Restemos 23 *a todos los términos:*

$$\begin{aligned} 0 &\leq 100q - 23 < 1 \\ 0{,}23 &\leq 100q - 23 < 0{,}24 \\ 0{,}2323 &\leq 100q - 23 < 0{,}2324 \\ &\cdots \end{aligned}$$

Luego si q *es el número que buscamos, resulta que* $100q - 23$ *también tendría el mismo desarrollo, por lo que se cumple la igualdad:*

$$100q - 23 = q, \quad \textit{es decir} \quad 99q = 23, \quad \textit{y así} \quad q = \frac{23}{99}.$$

Veamos:

$$\begin{array}{l|l} 2\,3\,0 & 9\,9 \\ \cline{2-2} 2\,3\,0 & 0,2\,3\ldots \\ \quad 3\,2\,0 & \\ \quad\quad 2\,3 & \\ \quad\quad\quad \ddots & \end{array}$$

¡Funciona!

b) $1074{,}124\,76\,76\,76\cdots = 1074{,}124\,\overset{\frown}{76}$.

La técnica anterior nos indica que el número $q - 1074{,}124$ *debe tener el desarrollo* $0{,}000\,\overset{\frown}{76}$. *Luego* $1000(q - 1074{,}124)$ *tiene como desarrollo* $0,\overset{\frown}{76}$. *Ahora bien,* $0,\overset{\frown}{76}$ *es el desarrollo del número* $76/99$, *por lo mismo que antes. Luego buscamos un número* q *que verifique:*

$$1000q - 1074124 = \frac{76}{99}$$

ya está:

$$q = \frac{1074124}{1000} + \frac{76}{99000}.$$

¡Compruébese!

Ejercicios

1) *Calcular los desarrollos decimales de los siguientes números:*

$$\frac{22}{7}, \quad \frac{14}{33}, \quad \frac{1074}{193}, \quad \frac{5}{3}, \quad \frac{7}{13}.$$

2) *Hallar los números racionales cuyos desarrollos decimales son:*

$$21{,}0\,\overset{\frown}{34}, \quad 0,\overset{\frown}{7}, \quad 1,\overset{\frown}{715}, \quad 2{,}3\,\overset{\frown}{51}, \quad 0,\overset{\frown}{1234}.$$

3) *¿Puede haber un desarrollo decimal de la forma* $0{,}a_1 \dots a_n 99999 \dots$ *?*

4.6. Potencias negativas: la notación científica

Sabemos que si $n \geq m$ *entonces podemos escribir*

$$\frac{a^n}{a^m} = a^{n-m}.$$

Esta identidad nos marca una pauta para extender la definición de potencias al caso de exponentes negativos:

$$\boxed{a^{-m} = \frac{1}{a^m}}$$

de manera que se sigan cumpliendo las leyes del cálculo de potencias positivas:

$$\frac{a^n}{a^m} = a^{n-m} = a^{n+(-m)} = a^n \cdot a^{-m} = a^n \cdot \frac{1}{a^m}.$$

Cuando tenemos que manejar números muy grandes o muy pequeños, resulta conveniente escribirlos en la forma

$$\boxed{N = a \cdot 10^k}$$

donde a *es un número decimal cuya parte entera está comprendida entre* 1 *y* 9*. Es decir, tiene un solo dígito, y es distinto de* 0*. El exponente,* k*, es un entero, positivo, negativo o nulo.*

$$\boxed{1{,}30 \cdot 10^2; \quad 2{,}7814 \cdot 10^4; \quad 1{,}3 \cdot 10^{-5}}$$

Ejemplos:

Velocidad de la luz:	299.792.458 *metros por segundo* $= 3 \cdot 10^5 \text{km/s}$.
Volumen de la Tierra:	1.080.759 *miles de billones de metros cúbicos* $= 1{,}080759 \cdot 10^{21}\text{m}^3$.
Radio del electrón:	$2{,}817939 \cdot 10^{-15}$ *metros.*
Número de Avogadro:	$6{,}02 \cdot 10^{23}$.
Carga del electrón:	$1{,}6 \cdot 10^{-19}$ *culombios.*
Masa del protón:	$1{,}7 \cdot 10^{-27}\text{kg}$.

La ventaja de esta notación es que una mirada al exponente k nos da una idea del orden de magnitud, pequeño o grande, del número que estamos considerando. Resulta también útil a la hora de calcular.

Ejemplo 2: *La estrella α–centauro se encuentra a 40,7 billones de kilómetros de la Tierra. ¿Cuánto tiempo tarda la luz de esa estrella en llegar a nuestro planeta?*

SOLUCIÓN: *40,7 billones de* $\text{km} = 4{,}07 \cdot 10^{13}\text{km}$, $c = 3{,}00 \cdot \text{km/seg}$, *y en un año hay* $3600 \cdot 24 \cdot 365 = 3{,}15 \cdot 10^7\text{seg}$. *Luego la luz tarda*

$$\frac{4{,}07 \cdot 10^{13}}{3 \cdot 10^5} / (3{,}15 \cdot 10^7) = 4{,}3 \text{ años.}$$

Ejercicios

1) *Expresar en notación científica los números:*

184.900.000 0,000137 0,000000012 1.239.000.000.000 0,00000079 .

2) *Expresar en forma decimal las siguientes cantidades:*

- *Constante de Planck:* $6{,}6 \times 10^{-34}$ *julios por segundo.*
- *Energía del primer nivel del átomo de hidrógeno:* $-21{,}8 \times 10^{-19}$ *julios.*
- *Carga del electrón:* $e = 1{,}6 \times 10^{-19}$ *culombios.*

3) *La velocidad de la luz en el vacío es de 300.000 kilómetros por segundo. ¿Cuántos kilómetros recorre la luz en un año?*

4) *En una época del año, las distancias de la Tierra al Sol y a la Luna son, respectivamente,* $1{,}4 \times 10^8$ *y* $3{,}9 \times 10^5$ *kilómetros. ¿Cuántas veces mayor es la distancia de la Tierra al Sol que a la Luna?*

5) *Recordemos la primitiva definición del metro: la diezmillonésima parte del cuadrante del meridiano terrestre. Usémosla, junto con el desarrollo decimal del número* π*, para calcular el volumen de la Tierra (en kilómetros cúbicos).*

6) *Escribir en forma de fracción los decimales periódicos siguientes:*

$$5{,}4\,\overset{\frown}{7}\,, \quad 10{,}33\,\overset{\frown}{6}\,, \quad 8,\overset{\frown}{4}\,, \quad 7{,}1\,\overset{\frown}{35}.$$

7) *Consideremos el "desarrollo" decimal*

$$0{,}1010010001000010000010000001\ldots$$

(cada cifra 1 está seguida de un bloque de ceros cuya longitud aumenta en cada paso). ¿Puede existir un número racional que lo tenga por desarrollo decimal?

8) *Efectuar las operaciones siguientes:*

$$\left(3,\overset{\frown}{8}+4,\overset{\frown}{12}\right)\cdot\frac{1,\overset{\frown}{3}}{0,\overset{\frown}{7}} \quad y \quad \frac{4,\overset{\frown}{03}}{1,\overset{\frown}{10}} : 3,\overset{\frown}{5}$$

9) *En el caso en que sea posible, hallar una fracción equivalente*

i) a $3/8$ *de manera que el numerador sea 93;*

ii) a $-2/7$ *con denominador 49;*

iii) a $2/9$ *con denominador* -59.

10) *En la estantería de un supermercado hay cuatro botellas de aceite que contienen, respectivamente,* $30/21$ *litros,* 2 *litros,* $15/14$ *litros y* $2/7$ *de litro. ¿Qué botella contiene más y cuál menos?*

4.7. En fila de a uno: estricta formación

La relación $\leq$ *entre los racionales es un orden total (dados dos racionales,* q_1*,* q_2*, siempre se verifica una de las dos relaciones:* $q_1 \leq q_2$ *o* $q_2 \leq q_1$*). Sin embargo, difiere del orden de los enteros en una propiedad importante como es la existencia o ausencia de sucesores. Entre dos racionales distintos,* a/b *y* c/d*, siempre cabe otro (y por tanto infinitos) a saber:* $(a+c)/(b+d)$.

Sin embargo, es posible dotar a $\mathbb{Q}$ *de otras ordenaciones que sí son hileras como las de los naturales. Si un conjunto tiene un número finito de*

elementos, puede ponerse en correspondencia biyectiva con un subconjunto $\{1, 2, 3, \ldots, n\}$ *de los naturales. Los conjuntos finitos son, pues, numerables o contables.*

Definición. *Un conjunto infinito numerable,* X*, es aquél que admite una biyección con el conjunto* $\mathbb{N}$ *de los naturales.*

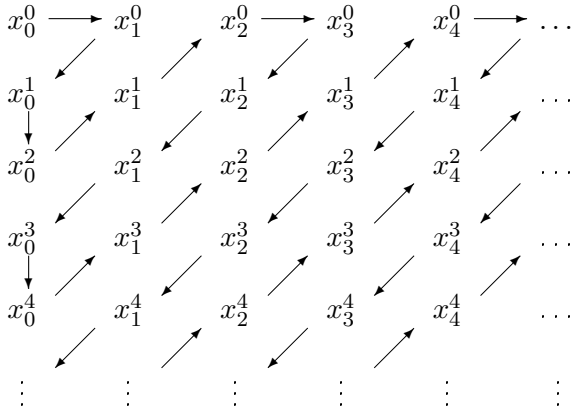
Sea $\Phi : \mathbb{N} \longrightarrow X$ *una aplicación biyectiva. Podemos poner el conjunto* X *en fila de a uno por el procedimiento siguiente:*

> $x_0 = \Phi(0)$, $x_1 = \Phi(1)$, $\ldots$, $x_n = \Phi(n)$, $\ldots$ *El orden de un elemento* $x \in X$ *es el natural* $\Phi^{-1}(x)$*. Es decir el conjunto* X *es la sucesión:*
>
> $$x_0\,,\, x_1\,,\, x_2\,,\, x_3\,,\, \ldots\,,\, x_n\,,\, \ldots$$

Supongamos que tenemos un conjunto numerable de tales filas (es decir un conjunto numerable de conjuntos numerables). Podemos representar esta situación por una doble hilera de sucesiones:

$$\begin{array}{lcl} X_0 & : & x_0^0\,,\, x_1^0\,,\, x_2^0\,,\, x_3^0\,,\, \ldots\,,\, x_n^0\,, x_{n+1}^0\,,\, \ldots \\ X_1 & : & x_0^1\,,\, x_1^1\,,\, x_2^1\,,\, x_3^1\,,\, \ldots\,,\, x_n^1\,, x_{n+1}^1\,,\, \ldots \\ X_2 & : & x_0^2\,,\, x_1^2\,,\, x_2^2\,,\, x_3^2\,,\, \ldots\,,\, x_n^2\,, x_{n+1}^2\,,\, \ldots \\ X_3 & : & x_0^3\,,\, x_1^3\,,\, x_2^3\,,\, x_3^3\,,\, \ldots\,,\, x_n^3\,, x_{n+1}^3\,,\, \ldots \\ & & \ldots\ldots \end{array}$$

El superíndice k *en* x_j^k *significa que es un elemento de la* k*–ésima fila, mientras que el subíndice* j *nos da su posición en dicha fila, la* j*–ésima columna. Pues bien, G. Cantor, que fue uno de los creadores de la Teoría de Conjuntos, observó que es posible poner todo el cuadro en fila de a uno. Por ejemplo, siguiendo la línea quebrada de flechas:*



De ese modo podemos "numerar" todos los x_j^k *del cuadro infinito...*

Pero si lo que pretendemos es tener una biyección entre $\mathbb{N}$ *y el conjunto unión* $\bigcup X_k$*, hay que recordar que los* X_k *pueden* no ser disjuntos*, y evitar que un mismo elemento reciba dos "posiciones distintas en la fila".*

Se puede hacer del modo siguiente: consideremos para cada natural n *el conjunto*

$$E_n := \left\{ x_j^k \mid k+j=n \right\} \setminus \bigcup_{m=1}^{n-1} E_m, \qquad E_0 := \{x_0^0\},$$

donde el signo $\setminus$ *indica la* diferencia *de conjuntos: los* x_j^k *de la "diagonal"* $j+k=n$ *que no hayan aparecido en ninguna anterior.*

Como E_n *contiene un número finito de elementos, podemos ponerlos en un orden lineal. A continuación organizamos la fila en* $\bigcup X_k$ *de la manera siguiente: empezamos con* x_0^0*, luego ponemos en su orden los elementos de* E_1*, después los de* E_2*, y así sucesivamente.*

Proposición. *La unión numerable de conjuntos numerables es numerable.*

Corolario. *El conjunto* $\mathbb{Q}$ *de los números racionales es numerable.*

Demostración. $\mathbb{Q}$ *es la unión de los conjuntos*

$$E_n := \left\{ \frac{m}{n} \mid m.c.d.(m,n)=1,\ m,n \in \mathbb{Z}, n \geq 1 \right\}$$

cada uno de los cuales es numerable. ■

Ejercicio 4. *Suponiendo que sí fuesen disjuntos los* X_k*, y que cada diagonal se recorra hacia la derecha y arriba, probar que cada* x_j^k *recibirá el número de orden:*

$$f(x_j^k) = \frac{(j+k)(j+k+1)}{2} + j.$$

Una biyección φ *entre el conjunto finito* A *y el subconjunto* $\mathbb{N}_n$ *de los números naturales comprendidos entre* 1 *y* n*, es, simplemente, una manera de contar los elementos de* A*. Es decir, de ponerlos en fila de a uno:*

$$\begin{aligned} &\varphi : \mathbb{N}_n \longrightarrow A \\ &\quad \varphi(1)=a_1,\ \varphi(2)=a_2,\ \ldots,\ \varphi(n)=a_n \\ &\quad A = \{a_1,\ a_2,\ \ldots,\ a_n\}. \end{aligned}$$

Pero hay $n!$ *maneras distintas de hacerlo, tantas como permutaciones de los elementos de* A*.*

Definición. *card*$(A)=n$ *si existe una tal biyección entre* A *y* $\mathbb{N}_n$*.*

La consistencia de la definición anterior exige comprobar que un conjunto finito A *no puede ser biyectable a la vez con* $\mathbb{N}_n$ *y* $\mathbb{N}_m$ *si* $n \neq m$*. Se trata del siguiente ejercicio:*

Ejercicio 5. *a) Si $m \neq n$ demostrar que no existe una biyección entre $\mathbb{N}_n$ y $\mathbb{N}_m$.*

Sugerencia: usar el principio de inducción. Suponiendo que $\mathbb{N}_n$ no es biyectable con $\mathbb{N}_m$ $(m < n)$ demostrar que $\mathbb{N}_{n+1}$ tampoco puede ponerse en correspondencia biyectiva con N_j, $j \leq n$.

b) Demostrar que un conjunto finito A nunca es equipotente, es decir, biyectable, con un subconjunto propio.

Lema. *Todo conjunto infinito E (no biyectable con ningún $\mathbb{N}_n$) contiene a un subconjunto equipotente con $\mathbb{N}$.*

Demostración. *Como $E \neq \emptyset$ podemos escoger un primer elemento $e_1 \in E$. En general, elegidos $e_1, \ldots, e_n$ en E, el conjunto $E \setminus \{e_1, \ldots, e_n\}$ es distinto del vacío (porque en caso contrario tendríamos que $E = \{e_1, \ldots, e_n\}$ y sería biyectable con $\mathbb{N}_n$, en contra de la hipótesis de partida), luego podemos elegir un nuevo elemento $e_{n+1} \in E \setminus \{e_1, \ldots, e_n\}$.*

Por inducción construimos una aplicación inyectiva

$$\varphi : \mathbb{N} \longrightarrow E$$
$$\varphi(n) = e_n$$

que nos da una biyección entre $\mathbb{N}$ y su imagen $\mathrm{Im}(\varphi) = \{e_n\}_{n=1,2,\ldots} \subset E$. ■

Consideremos ahora la unión disjunta

$$E = \{e_n\}_{n=1,2,\ldots} \cup E', \qquad E' = E \setminus \{e_1, e_2, \ldots\}.$$

Tenemos que $F = \{e_{2n}\}_{n=1,2,\ldots} \cup E'$ es un subconjunto propio de E. La aplicación:

$$\psi : E \longrightarrow F$$
$$\psi(e') = e' \quad si \quad e' \in E'$$
$$\psi(e_j) = e_{2j}, \quad j = 1, 2, \ldots$$

es una biyección de los conjuntos E y F. Esto demuestra lo siguiente:

Corolario. *Todo conjunto infinito es biyectable con un subconjunto propio. Un conjunto es finito si y solo si no es biyectable con ningún subconjunto propio.*

Siguiendo a Cantor diremos que un conjunto infinito tiene cardinal $\aleph_0$ ("alef subcero") si es equipotente con el conjunto de todos los números naturales, es decir, si es infinito numerable.

4.8. Sucesiones de Farey

Una manera especialmente interesante de colocar los racionales consiste en fijar un entero positivo n y escribir, de menor a mayor, las fracciones irreducibles propias cuyo denominador es menor o igual que n. El conjunto ordenado resultante F_n se llama sucesión de Farey, en honor del geólogo británico que descubrió sus propiedades.

He aquí algunos ejemplos:

$$F_1 : \frac{0}{1}, \frac{1}{1}$$

$$F_2 : \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$$

$$F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$$

$$F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$$

$$F_5 : \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$$

$$F_6 : \frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}$$

$$F_7 : \frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}$$

En una primera inspección vemos que si $\frac{a}{b}$ *y* $\frac{a'}{b'}$ *son términos consecutivos de* F_n *entonces* $b + b' > n$*: como* $\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}$ *se verifica siempre, la desigualdad* $b + b' \leq n$ *contradiría la hipótesis de ser* $\frac{a}{b}$ *y* $\frac{a'}{b'}$ *términos consecutivos de la sucesión de Farey* F_n*.*

Observemos también que dos términos sucesivos de F_n*,* $\frac{a}{b}$*,* $\frac{a'}{b'}$ *tienen denominador distinto* ($b \neq b'$)*: esto es verdad porque entre* $\frac{a}{b}$ *y* $\frac{a+1}{b}$ ($a + 1 < b$) *siempre podemos intercalar la fracción* $\frac{a}{b-1}$*.*

Unas propiedades importantes de las fracciones de Farey son las siguientes:

Proposición. *Si* $\frac{a}{b} < \frac{a'}{b'}$ *son dos términos consecutivos de* F_n *entonces*

$$a'b - ab' = 1.$$

Corolario. *Si* $\frac{a}{b} < \frac{a'}{b'} < \frac{a''}{b''}$ *son tres términos consecutivos de* F_n *entonces* $\frac{a'}{b'} = \frac{a+a''}{b+b''}$*.*

Estas dos propiedades se observan en los ejemplos presentados antes. El corolario resulta especialmente útil a la hora de obtener F_{n+1} *a partir de* F_n*: basta con intercalar la mediana de dos fracciones sucesivas de* F_n*, siempre que aquélla tenga denominador menor o igual que* $n + 1$*.*

Demostración. *Sean* $\frac{a}{b} < \frac{a'}{b'}$ *términos consecutivos de* F_n *y consideremos la siguiente ecuación diofántica:*

$$bx - ay = 1.$$

Dada una solución particular $bx_0 - ay_0 = 1$, *la general es de la forma:*

$$(x, y) = (x_0 + am\,,\, y_0 + bm)\,, \quad m \in \mathbb{Z}$$

y como $b \le n$, *podemos escoger* m *de modo que sea:*

$$0 < n - b < y \le n.$$

Además, $bx - ay = 1$ *implica que*

$$\frac{x}{y} = \frac{1}{b}\Big(a + \frac{1}{y}\Big) \le \frac{a+1}{b} \le 1\,,$$

luego $\frac{x}{y}$ *está en* F_n *y la demostración concluiría si logramos probar la igualdad:* $\frac{x}{y} = \frac{a'}{b'}$.

Pero, en caso contrario, tendríamos que $\frac{x}{y} > \frac{a'}{b'}$, *por ser* $\frac{a}{b}$ *y* $\frac{a'}{b'}$ *fracciones consecutivas de* F_n. *De la igualdad* $bx - ay = 1$ *deducimos:*

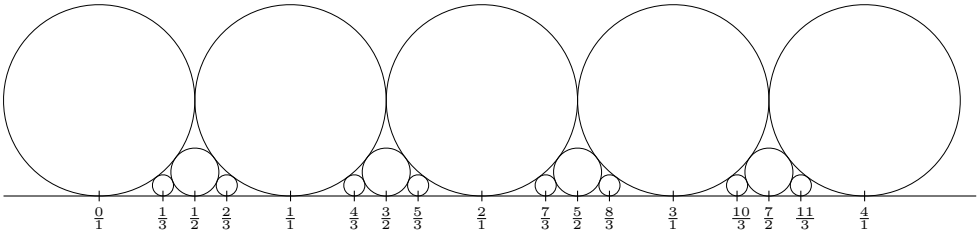
$$\begin{aligned}\frac{1}{by} &= \frac{x}{y} - \frac{a}{b} = \frac{x}{y} - \frac{a'}{b'} + \frac{a'}{b'} - \frac{a}{b} = \frac{xb' - ya'}{yb'} + \frac{a'b - b'a}{bb'} \\ &\ge \frac{1}{b'}\Big\{\frac{1}{y} + \frac{1}{b}\Big\} = \frac{y+b}{b'} \cdot \frac{1}{by} > \frac{1}{by}\,,\end{aligned}$$

ya que $y + b > n \ge b'$, *lo que es una contradicción.* ■

La demostración del corolario se obtiene despejando a' *y* b' *en las identidades:*

$$\left.\begin{array}{ll} a'b & - b'a \;\; = 1 \\ b'a'' & - b''a' \;\; = 1 \end{array}\right\} \quad \Longleftrightarrow \quad \frac{a'}{b'} = \frac{\frac{a+a''}{a''b-ab''}}{\frac{b+b''}{a''b-ab''}} = \frac{a+a''}{b+b''}.$$ ■

Dadas una coordenadas cartesianas en el plano, representemos en el eje de abscisas a los números racionales y, sobre cada uno de ellos $(\frac{p}{q},\ m.c.d.(p,q){=}1)$ *tracemos un círculo* $C_{\frac{p}{q}}$ *de diámetro* $\frac{1}{q^2}$ *y con centro en el punto de coordenadas* $\big(\frac{p}{q}\,,\, \frac{1}{2}\,\frac{1}{q^2}\big)$.



Para entender esta geometría basta con restringirnos al caso de las fracciones propias $\frac{a}{b}$. *Entonces resulta que la condición necesaria y suficiente para que* $C_{\frac{a}{b}}$ *y* $C_{\frac{a'}{b'}}$ *sean tangentes en un punto es que* $\frac{a}{b}$ *y* $\frac{a'}{b'}$ *sean términos consecutivos de una sucesión de Farey* F_n:

Los círculos $C_{\frac{a}{b}}$, $C_{\frac{a'}{b'}}$ *tienen, respectivamente, centros* $\left(\frac{a}{b}\,,\,\frac{1}{2}\,\frac{1}{b^2}\right)$, $\left(\frac{a'}{b'}\,,\,\frac{1}{2}\,\frac{1}{(b')^2}\right)$ *y radios* $\frac{1}{2}\,\frac{1}{b^2}$, $\frac{1}{2}\,\frac{1}{(b')^2}$.
La distancia d *entre sus centros satisface:*

$$\begin{aligned} d^2 &= \left(\frac{a}{b} - \frac{a'}{b'}\right)^2 + \left(\frac{1}{2}\,\frac{1}{b^2} - \frac{1}{2}\,\frac{1}{(b')^2}\right)^2 \\ &= \frac{(ab' - a'b)^2 - 1}{(bb')^2} + \left(\frac{1}{2}\,\frac{1}{b^2} + \frac{1}{2}\,\frac{1}{(b')^2}\right)^2. \end{aligned}$$

Luego si $ab' - a'b > 1$ *la distancia entre sus centros es estrictamente mayor que la suma de los radios y los círculos no se cortan, mientras que si* $ab' - a'b = 1$ *resultan ser tangentes.* ■

¿Cuántos términos tiene la sucesión F_n*? La respuesta es fácil si se nos permite usar la función de Euler* $\phi(n) = card\{k \mid 1 \leq k \leq n, (k,n) = 1\}$ *ya que:*

$$card(F_n) = 1 + \phi(1) + \phi(2) + \cdots + \phi(n).$$

Pero no existe una manera elemental de evaluar la suma anterior, aunque sí sabemos su orden de magnitud, que es el siguiente:

$$1 + \phi(1) + \phi(2) + \cdots + \phi(n) \simeq \frac{3}{\pi^2}\, n^2\,;$$

o dicho de modo más preciso, sabemos que:

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} \phi(n)}{n^2} = \frac{3}{\pi^2} = 0{,}3039\ldots$$

El cómputo de este límite exige un poco de cálculo diferencial y puede perfectamente omitirse en una primera lectura. Recordemos la fórmula

$$\phi(k) = k \prod_{p|k} \left(1 - \frac{1}{p}\right)$$

donde el producto se extiende sobre todos los divisores primos de k*. Desarrollando ese producto podemos escribirlo como una suma sobre los divisores:*

$$\phi(k) = k \sum_{d|k} \frac{\mu(d)}{d}$$

donde la función μ *(función de Möbius) está definida por la fórmula:*

$$\mu(m) = \begin{cases} 0 & \text{si } m \text{ es divisible por el cuadrado de un primo} \\ (-1)^k & \text{si } m \text{ es el producto de } k \text{ primos distintos.} \end{cases}$$

Entonces:

$$\sum_{k=1}^{n}\phi(k)=\sum_{k=1}^{n}k\sum_{d|k}\frac{\mu(d)}{d}=\sum_{d=1}^{n}\mu(d)\sum_{j=1}^{\left[\frac{n}{d}\right]}j=\frac{1}{2}\,n^2\sum_{d=1}^{n}\frac{\mu(d)}{d^2}\;+\;E(n)$$

siendo $|E(n)|\leq n\,\log n+1$. *Luego*

$$\sum_{k=1}^{n}\phi(k)=\frac{1}{2}\,n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\;+\left(E(n)-\frac{n^2}{2}\sum_{d=n+1}^{\infty}\frac{\mu(d)}{d^2}\right)$$

y el cálculo se termina observando que

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}$$
$$\left|\sum_{d=n+1}^{\infty}\frac{\mu(d)}{d^2}\right|\leq\sum_{d=n+1}^{\infty}\frac{1}{d^2}\leq\frac{1}{n}.$$

La identidad $\dfrac{6}{\pi^2}=\sum\limits_{d=1}^{\infty}\dfrac{\mu(d)}{d^2}$ *se debe a Euler y es equivalente a esta otra:* $\dfrac{\pi^2}{6}=\sum\limits_{n=1}^{\infty}\dfrac{1}{n^2}$, *por la razón siguiente:*

$$\lim_{N\to\infty}\prod_{k=1}^{N}\left(1-\frac{1}{p_k^2}\right)=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$$
$$\lim_{N\to\infty}\prod_{k=1}^{N}\left(1-\frac{1}{p_k^2}\right)^{-1}=\lim_{N\to\infty}\prod_{k=1}^{N}\left(1+\frac{1}{p_k^2}+\frac{1}{p_k^4}+\frac{1}{p_k^6}+\cdots\right)=\sum_{n=1}^{\infty}\frac{1}{n^2}.$$

En las identidades anteriores hemos usado el Teorema Fundamental de la Aritmética para escribir los productos, donde $p_1=2$, $p_2=3$, $p_3=5$, $\ldots$ *designa a la sucesión de los primos.*

La manera más sencilla que conocemos de demostrar la fórmula de Euler es la siguiente:

Sea

$$\begin{aligned}\zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}&=\sum_{n=0}^{\infty}\frac{1}{(2n+1)^2}\;+\sum_{n=1}^{\infty}\frac{1}{(2n)^2}\\&=\sum_{n=0}^{\infty}\frac{1}{(2n+1)^2}+\frac{1}{4}\,\zeta(2).\end{aligned}$$

Luego

$$\begin{aligned}\zeta(2) &= \frac{4}{3}\sum_{n=0}^{\infty}\frac{1}{(2n+1)^2} = \frac{4}{3}\sum_{n=0}^{\infty}\left(\int_0^1 x^{2n}\,\mathrm{d}x\right)\left(\int_0^1 y^{2n}\,\mathrm{d}y\right)\\ &= \frac{4}{3}\int_0^1\int_0^1\sum_{n=0}^{\infty}(x^2y^2)^n\,\mathrm{d}x\,\mathrm{d}y = \frac{4}{3}\int_0^1\int_0^1\frac{1}{1-x^2y^2}\,\mathrm{d}x\,\mathrm{d}y\\ &= \frac{1}{3}\int_{-1}^{+1}\int_{-1}^{+1}\frac{1}{1-x^2y^2}\,\mathrm{d}x\,\mathrm{d}y.\end{aligned}$$

El cambio de variables:

$$x=\tanh(s)=\frac{\sinh(s)}{\cosh(s)}=\frac{e^s-e^{-s}}{e^s+e^{-s}}\,,\ \ y=\tanh(t)=\frac{\sinh(t)}{\cosh(t)}=\frac{e^t-e^{-t}}{e^t+e^{-t}}$$

nos da:

$$\begin{aligned}\zeta(2) &= \frac{1}{3}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{\mathrm{d}s\,\mathrm{d}t}{\cosh^2(s)\cosh^2(t)-\sinh^2(s)\sinh^2(t)}\\ &= \frac{1}{3}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{\mathrm{d}s\,\mathrm{d}t}{\cosh(s+t)\,\cdot\,\cosh(s-t)}\end{aligned}$$

El cambio $s+t=u$, $s-t=v$ produce

$$\zeta(2)=\frac{1}{6}\left(\int_{-\infty}^{+\infty}\frac{\mathrm{d}u}{\cosh(u)}\right)^2=\frac{\pi^2}{6}\,,$$

ya que haciendo $e^u=z$ obtenemos:

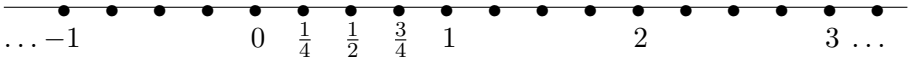
$$\int_{-\infty}^{+\infty}\frac{\mathrm{d}u}{\cosh(u)}=\int_{-\infty}^{+\infty}\frac{2\mathrm{d}u}{e^u+e^{-u}}=\int_0^{\infty}\frac{2\mathrm{d}z}{1+z^2}=2\arctan z\Big]_0^{\pi/2}=\pi.\quad\blacksquare$$

— 5 —

Los números reales

> *También Lamuro vivió en aquella época, como Morencio, primero entre los historiadores; Takehiko Mitsukuri, autor de la* Ética de la decisión *y de otros famosos libros; Martino, padre de* Las condiciones de la Razón *y de la* Observación de mi cuñada*; Cebrino, creador de la* Analítica de los sucesos*; y Polícrito, definidor del número y de la Divinidad, e investigador de los irracionales...*
>
> Miguel de Espinosa
>
> *(Escuela de Mandarines)*

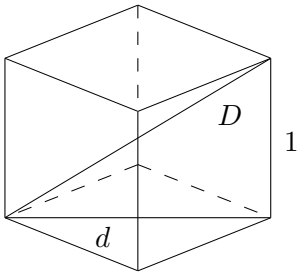
Los números racionales pueden ser representados por puntos de una recta

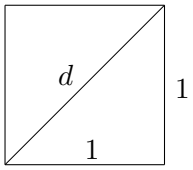


de manera que entre dos cualesquiera de ellos siempre hay otro: entre 0 *y* 1 *se encuentra* 1/2*; entre* 1/2 *y* 1*, está ubicado* 3/4*. En general, entre los números racionales* a *y* b *se encuentra situado* $(a+b)/2$*, que corresponde al punto medio del segmento que los tiene por extremos. Esta propiedad de los racionales, que los diferencia de los enteros, es muy interesante. Diremos que son densos en la recta: entre dos puntos cualesquiera de la recta siempre hay un racional y, de hecho, infinitos de ellos.*

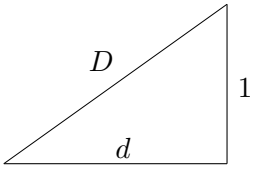
Sin embargo, los racionales no llenan la recta porque dejan muchos huecos. Uno de estos agujeros fue detectado por los pitagóricos y, como estudiamos en la primera lección, dio lugar a una de las primeras revoluciones del pensamiento científico.

Consideremos un cubo de lado la unidad:





$d^2 = 1^2 + 1^2 = 2$



$D^2 = d^2 + 1^2 = 3$

Sus caras son cuadrados de lado 1 y la diagonal de una de ellas verifica la relación $d^2 = 1^2 + 1^2 = 2$, *que es un caso particular del Teorema de Pitágoras. Análogamente, la diagonal* D *del cubo es la hipotenusa de un triángulo rectángulo cuyos catetos miden* d *y* 1*; luego:* $D^2 = d^2 + 1^2 = 3$.

Ahora bien, con todo lo que ya sabemos, no resulta difícil comprobar que no puede haber ningún número racional m/n *que verifique alguna de las dos relaciones:*

$$\frac{m^2}{n^2} = 2, \qquad o \qquad \frac{m^2}{n^2} = 3.$$

Como la primera de ellas ha sido ya analizada, veamos qué pasa con la segunda: la igualdad $3n^2 = m^2$ *carece de soluciones enteras porque el exponente de 3 en la descomposición en factores primos de* n^2 *tiene que ser par, mientras que en* $3n^2$ *es impar. El Teorema Fundamental de la Aritmética impide que puedan ser iguales.*

Ejercicio 1. *Comprobar que el razonamiento anterior sirve también para* $5n^2 = m^2$; $7n^2 = m^2$; $11n^2 = m^2$. *En general, dado un número primo* p *no existe un racional* m/n *tal que* $p = m^2/n^2$.

Ejercicio 2. *Aplicar la técnica del ejercicio anterior, es decir, el Teorema Fundamental de la Aritmética, para mostrar que no existen racionales* m/n *que verifiquen las igualdades:*

a) $\left(\dfrac{m}{n}\right)^3 = 2$;

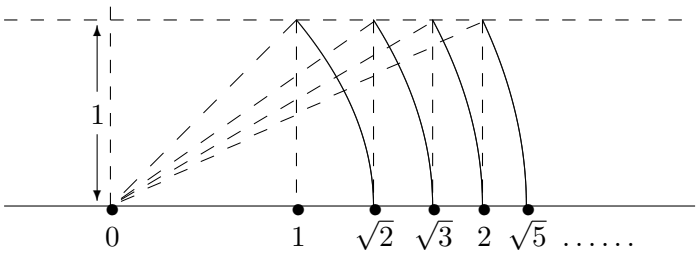
b) $\left(\dfrac{m}{n}\right)^5 = 7$;

c) *en general,* $(m/n)^k = p$, *donde* p *es un número primo, y* k *es un número natural.*

Ejercicio 3. *Sea* $n = p_1^{a_1} \cdots p_k^{a_k}$ *la descomposición de* n *en factores primos. ¿Cuándo será* $\sqrt[b]{n}$ *un número racional?*

Luego, con solo los números racionales, no podemos medir estas longitudes que, en adelante, escribiremos $d = \sqrt{2}$ *y* $D = \sqrt{3}$. *El empeño de asignar*

un número a cada punto de la recta, o, lo que es equivalente, poder medir cualquier longitud, nos impulsa a ampliar el conjunto $\mathbb{Q}$. *El resultado serán los números reales que designaremos por la letra* $\mathbb{R}$.



Presentaremos la búsqueda de los números reales en forma de una sucesión de objetivos:

Objetivo 1. Los números reales constarán de los racionales junto a otros nuevos que, por contraposición, llamaremos irracionales.

Objetivo 2. La propiedad de densidad que tienen los puntos racionales permitirá aproximar a los irracionales por racionales, con tanta precisión como queramos prescribir.

Un ejemplo	*Otra manera de escribirlo*
$1^2 < 3 < 2^2$	$1 < \sqrt{3} < 2$
$(1{,}7)^2 < 3 < (1{,}8)^2$	$1{,}7 < \sqrt{3} < 1{,}8$
$(1{,}73)^2 < 3 < (1{,}74)^2$	$1{,}73 < \sqrt{3} < 1{,}74$
$(1{,}732)^2 < 3 < (1{,}733)^2$	$1{,}732 < \sqrt{3} < 1{,}733$
$(1{,}7320)^2 < 3 < (1{,}7321)^2$	$1{,}7320 < \sqrt{3} < 1{,}7321$
$(1{,}73205)^2 < 3 < (1{,}73206)^2$	$1{,}73205 < \sqrt{3} < 1{,}73206$
...	...

En el ejemplo previo hemos puesto de manifiesto a los intervalos decimales de cada generación que contienen al número $\sqrt{3}$.

Los números de la izquierda, $1 < 1{,}7 < 1{,}73 < 1{,}732 < 1{,}7320 < \ldots$, *son aproximaciones racionales por defecto del irracional* $\sqrt{3}$; *mientras que los de la derecha, nos dan aproximaciones por exceso:* $2 > 1{,}8 > 1{,}74 > 1{,}733 > 1{,}7321 > \ldots$

La bondad de las aproximaciones la podemos estimar por medio de las diferencias:

$$1 = 2 - 1;\ \frac{1}{10} = 1{,}8 - 1{,}7;\ \frac{1}{100} = 1{,}74 - 1{,}73;\ \frac{1}{1000} = 1{,}733 - 1{,}732;\ \ldots$$

Por ejemplo, podemos decir que 1,732 *y* 1,733 *son aproximaciones racionales del número* $\sqrt{3}$ *(por defecto y por exceso, respectivamente), con un error menor que una milésima.*

Un número real puede ser aproximado por números racionales con tanta precisión como se desee.

Objetivo 3. A todo número real le podemos asignar un desarrollo decimal. Este será periódico en el caso de los racionales y no será periódico para los irracionales. Recíprocamente: todo desarrollo decimal corresponde a un número real.

$\frac{1}{3} = 0{,}333333\ldots$	$\sqrt{2} = 1{,}41421356\ldots$
$\frac{22}{7} = 3{,}142857142857\ldots$	$\sqrt{3} = 1{,}73205080\ldots$
$\frac{5}{66} = 0{,}0757575\ldots$	$\sqrt{5} = 2{,}23606797\ldots$

El sentido preciso de las igualdades anteriores lo iremos matizando en el futuro. El desarrollo decimal nos indica, en cada caso, los intervalos decimales de cada generación que contiene al número real dado. Por ejemplo: $2{,}23606 < \sqrt{5} < 2{,}23607$.

Objetivo 4. Querremos poder sumar, restar, multiplicar y dividir números reales como una extensión de las operaciones con racionales.

Objetivo 5. Querremos que los números reales sean completos en el sentido de que toda sucesión de Cauchy tenga un límite.

Quizá el número irracional más famoso sea π*: la razón de la circunferencia y su diámetro. El uso de la letra* π *es natural puesto que así comienza, en griego, la palabra que designa la longitud de una circunferencia (recordemos perímetro, periferia, . . .). La irracionalidad de* π *se logró demostrar en el siglo* XVIII*. La prueba se debe a Lambert y la entenderemos más adelante. De momento basta con saberlo y también conocer algunas de las primeras cifras de su desarrollo decimal:*

$$\begin{aligned} \pi &= 3{,}14159265358979\ldots \\ \sqrt{\pi} &= 1{,}7724538509\ldots \end{aligned}$$

Otro número especialmente importante de las matemáticas es el número e*, que también es irracional:*

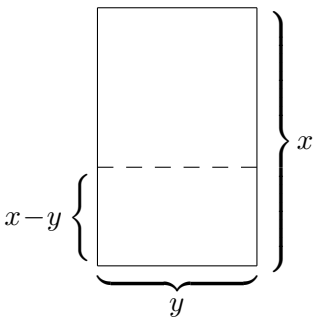
$$e = 2{,}718281828459045\ldots$$

Finalmente, en este sucinto Gotha de números famosos, hay que incluir al número de oro, la razón áurea o divina proporción:

$$\Phi = \frac{1+\sqrt{5}}{2} = 1{,}618033988\ldots$$

Aquí la letra griega Φ *se usa en honor del gran escultor Fidias, cuyo nombre griego comienza, naturalmente, con la letra* Φ*. Fidias utilizó sistemáticamente la divina proporción en sus bellas y armoniosas esculturas.*

Según los clásicos, los rectángulos más perfectos son aquellos cuyos lados guardan esta proporción. El Partenón estaba diseñado de esta manera:



Si $\dfrac{x}{y} = \dfrac{1+\sqrt{5}}{2}$*, observemos que:*

$$\begin{aligned}\frac{y}{x-y} &= \frac{1}{\frac{x}{y}-1} = \frac{1}{\frac{\sqrt{5}+1}{2}-1} \\ &= \frac{2}{\sqrt{5}-1} = \frac{2(\sqrt{5}+1)}{(\sqrt{5}-1)(\sqrt{5}+1)} \\ &= \frac{1+\sqrt{5}}{2}.\end{aligned}$$

Si a un rectángulo cuyos lados, x*,* y*, guardan la divina proporción, le quitamos un cuadrado de lado* y *(*$x > y$*), el rectángulo que resulta es también de oro.*

Observemos que:

$$\Phi = \frac{1+\sqrt{5}}{2} = 1 + \frac{\sqrt{5}-1}{2} = 1 + \frac{1}{\Phi}.$$

Si repetimos esta fórmula sucesivamente, resulta que:

$$\Phi = 1 + \frac{1}{\Phi} = 1 + \frac{1}{1+\frac{1}{\Phi}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{\Phi}}} = \ldots$$

Otra relación interesante satisfecha por el número Φ *es la siguiente:*

$$\Phi^2 = 1 + \Phi;$$

luego:

$$\Phi = \sqrt{1+\Phi} = \sqrt{1+\sqrt{1+\Phi}} = \sqrt{1+\sqrt{1+\sqrt{1+\Phi}}} = \ldots$$

5.1. La construcción de los números reales

Aunque el descubrimiento de las magnitudes inconmensurables se remonta a los pitagóricos y tenga, por lo tanto, más de veintiséis siglos de existencia, la construcción formal de los números reales es mucho más reciente. Hacia finales del siglo XIX, *G. Cantor y también R. Dedekind, de manera independiente, nos enseñaron cómo conseguir la noción precisa de número real. A continuación vamos a seguir el camino trazado por Cantor.*

Definición. *Diremos que una sucesión,* $\{q_n\}$, *de números racionales es de Cauchy si para todo entero positivo,* N, *existe otro,* $m = m(N)$, *tal que*

$$|\, q_j - q_k \,| \leq \frac{1}{N} \quad \textit{siempre que } j, k \geq m.$$

Ejemplos de sucesiones de Cauchy de números racionales son los siguientes:

a) $1, \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{4}, \ldots, \dfrac{1}{n}, \ldots$, *de otra forma:* $\{q_n\}$ *con* $q_n = \dfrac{1}{n}$.

b) $0{,}3\,,\ 0{,}33\,,\ 0{,}333\,,\ 0{,}3333\,,\ \ldots$, *o bien:* $\{q_n\}$, $q_n = \displaystyle\sum_1^n \frac{3}{10^n}$.

c) $1\,,\ 1{,}4\,,\ 1{,}41\,,\ 1{,}4142\,,\ 1{,}41421\,,\ \ldots$:

$$q_n^2 < 2 < \left(q_n + \frac{1}{10^{n-1}}\right)^2.$$

d) $3\,,\ 3{,}1\,,\ 3{,}14\,,\ 3{,}141\,,\ 3{,}1415\,,\ 3{,}14159\,,\ \ldots$:

$$q_n = \frac{[10^{n-1}\pi]}{10^{n-1}} = \frac{\textit{parte entera de } (10^{n-1}\pi)}{10^{n-1}}.$$

e) $1, 1 + \dfrac{1}{1!}, 1 + \dfrac{1}{1!} + \dfrac{1}{2!}, 1 + \dfrac{1}{1!} + \dfrac{1}{2!} + \dfrac{1}{3!}, \ldots$:

$$q_n = \sum_{k=0}^{n} \frac{1}{k!}.$$

f) $1, 1 - \dfrac{1}{2}, 1 - \dfrac{1}{2} + \dfrac{1}{3}, 1 - \dfrac{1}{2} + \dfrac{1}{3} - \dfrac{1}{4}, \ldots$:

$$q_n = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k}.$$

Existe, no obstante, una diferencia importante entre las seis. A saber: a) y b) son convergentes, es decir, tienen un límite dentro de $\mathbb{Q}$*:*

$$\lim_{n\to\infty} \frac{1}{n} = 0, \qquad \lim_{n\to\infty} \sum_{1}^{n} \frac{3}{10^n} = \frac{1}{3}.$$

Por el contrario c), d), e) y f) no tienen límite racional: $\sqrt{2}$*,* π*,* e *y* $\log 2$ *no son números racionales.*

Dada una sucesión $\{q_n\}$*, diremos que* $\{r_n\}$ *es una subsucesión si existe una función monótona creciente,* $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$*, de manera que:*

$$r_n = q_{\varphi(n)}.$$

Ejercicio 4. *Demostrar que:*

a) si la sucesión de números racionales $\{q_n\}$ *es de Cauchy, entonces también lo son todas sus subsucesiones;*

b) si la sucesión de números racionales $\{q_n\}$ *es convergente en* $\mathbb{Q}$*, entonces también lo son sus subsucesiones y todas tienen el mismo límite.*

La razón principal de la construcción de los números reales radica, precisamente, en tratar de subsanar este estado de cosas, y conseguir que todas las sucesiones de Cauchy sean convergentes o que tengan un límite real.

Entre todas las sucesiones de Cauchy de números racionales que son convergentes merecen una mención especial las que convergen a cero, como ocurre en el ejemplo a).

La sucesión $\{q_n\}$ *converge a* 0*, o tiene límite* 0 *(*$\lim q_n = 0$*), si para todo entero positivo,* N*, existe otro,* $n = n(N)$*, tal que* $|q_j| \leq 1/N$ *siempre que* $j \geq n$*.*

Designemos por $\mathcal{C}$ *al conjunto de todas las sucesiones de Cauchy de números racionales, y por* $\mathcal{N}$ *al subconjunto de las convergentes a cero. En* $\mathcal{C}$ *definimos la siguiente relación:*

$$\{q_n\} R \{r_n\} \quad \text{si y solo si } \{q_n - r_n\} \in \mathcal{N}.$$

Resulta fácil (y se deja como ejercicio para el lector) ver que R *tiene las propiedades reflexiva, simétrica y transitiva. Se trata pues de una relación de equivalencia, que divide al conjunto* $\mathcal{C}$ *en clases de equivalencia disjuntas. Pues bien, el conjunto de los números reales,* $\mathbb{R}$*, es el conjunto cociente de* $\mathcal{C}$ *por esta relación: "cada número real es una clase de equivalencia de sucesiones de Cauchy de números racionales".*

Aunque, a primera vista, la definición resulta algo rebuscada, si la analizamos detenidamente, no lo es tanto. Por ejemplo: el algoritmo de hallar raíces cuadradas que aprendimos en la escuela, nos va dando las sucesivas cifras decimales de $\sqrt{2} = 1{,}41421356\ldots$ *Eso significa, según queríamos en uno de nuestros objetivos iniciales, que el tal número,* $\sqrt{2}$*, puede ser aproximado, con la precisión que se desee, por los términos de la sucesión de Cauchy:*

$$a_1 = 1;\ a_2 = 1{,}4;\ a_3 = 1{,}41;\ a_4 = 1{,}414;\ \ldots$$

Pero también por los de la sucesión

$$b_n = a_n + \frac{1}{10^n}\,;$$

o por los de la sucesión $c_n = a_n + 1/(10^{n^2})$*; etcétera.*

De ahí a decir que $\sqrt{2}$ *es simplemente la clase de equivalencia de todas esas sucesiones hay un solo paso, que fue dado por G. Cantor.*

5.2. El cuerpo $\mathbb{R}$

Para que los números reales adquieran la categoría de números verdaderos, es fundamental que podamos sumarlos, restarlos, multiplicarlos y dividirlos (siempre que el divisor sea distinto de cero). El ejercicio siguiente contiene las claves necesarias para hacerlo.

Ejercicio 5. *Demostrar que si* $\{a_n\}$*,* $\{b_n\}$*,* $\{a'_n\}$*,* $\{b'_n\}$ *son sucesiones de Cauchy en* $\mathcal{C}$ *tales que:*

$$\{a_n\} R \{a'_n\} \quad y \quad \{b_n\} R \{b'_n\}$$

entonces:

$$\begin{aligned} \{a_n + b_n\} \quad & R \quad \{a'_n + b'_n\} \\ \{a_n \cdot b_n\} \quad & R \quad \{a'_n \cdot b'_n\}. \end{aligned}$$

Ejercicio 6. *Demostrar que si* $\{a_n\}$ *y* $\{b_n\}$ *son elementos de* $\mathcal{N}$ *y* $q \in \mathbb{Q}$*, entonces las sucesiones:*

$$\{a_n + b_n\}, \quad \{a_n \cdot b_n\}, \quad \{qa_n\}$$

son todas elementos de $\mathcal{N}$*.*

Definición. *Podemos ahora definir la suma y el producto de números reales. Sean* $r = [\{a_n\}]$*,* $s = [\{b_n\}]$*, dos números reales (clases de equivalencia de sucesiones), entonces:*

$$\begin{aligned} r + s &= [\{a_n + b_n\}] \\ r \cdot s &= [\{a_n \cdot b_n\}]. \end{aligned}$$

Ejercicio 7. *Demostrar que la suma y el producto de números reales gozan de las propiedades siguientes:*

i) *asociativa;*

ii) *conmutativa;*

iii) *distributiva del producto respecto de la suma;*

iv) *existencia de elemento neutro para la suma:* $0 = [\{0\}] = \mathcal{N}$;

v) *existencia de elemento opuesto para la suma;*

vi) *existencia de elemento neutro para el producto:* $1 = [\{1\}]$.

vii) *La notación* $\{q\}$ *designa a la sucesión de racionales cuyos elementos son todos iguales a* q: $a_n = q$, *para todo* $n \in \mathbb{N}$. *Probar que la aplicación inyectiva* $\varphi : \mathbb{Q} \longrightarrow \mathbb{R}$ *dada por* $\varphi(q) = [\{q\}]$ *preserva la suma y el producto. Esto nos permite identificar* $\mathbb{Q}$ *con* $\varphi(\mathbb{Q}) \subset \mathbb{R}$.

Definición. *Diremos que* $r \in \mathbb{R}$ *es positivo* ($r > 0$), *si dada* $\{a_n\} \in r$, *existen enteros positivos,* N *y* n, *tales que* $a_m > 1/N$ *para todo* $m \geq n$.

Para que la definición sea legal, es preciso demostrar la independencia respecto a la sucesión elegida en la clase r. *Es decir, supongamos que* $\{b_n\} \in r$ *es otra de las sucesiones de* r. *La relación de equivalencia* $\{a_n\}R\{b_n\}$ *implica la existencia de un entero* n_0 *tal que* $|a_n - b_n| \leq 1/(2N)$ *siempre que* $n \geq n_0$. *Por lo tanto:*

$$b_m > a_m - \frac{1}{2N} > \frac{1}{N} - \frac{1}{2N} = \frac{1}{2N}$$

siempre que $m \geq \text{máx}\{n, n_0\}$.

Luego la definición $r > 0$ *está bien dada. A partir de ella diremos que* $r = [\{b_n\}] < 0$ *si* $-r = [\{-b_n\}] > 0$.

Definición. *El orden natural* $s \leq r$ *significa que, o bien* $s = r$, *o bien* $r - s > 0$.

Ejercicios

1) *Demostrar que* $\leq$ *es una relación de orden en* $\mathbb{R}$ *(es decir tiene las propiedades reflexiva, antisimétrica y transitiva).*

2) *Demostrar que* $\leq$ *es un orden total: dados* r *y* s *en* $\mathbb{R}$, *o bien* $r \leq s$ *o bien* $s \leq r$.

3) *Demostrar que si* $r > 0$ *y* s *son dos números reales, entonces existe* $n \in \mathbb{N}$ *tal que* $n \cdot r \geq |s|$.

4) *Demostrar que dado $r \neq 0$ existe $s = 1/r$ de manera que $s \cdot r = 1$. Sugerencia: sea $r = [\{a_n\}] > 0$; comprobar que existen $\varepsilon > 0$ y $n_0 \in \mathbb{N}$ de manera que $a_n \geq \varepsilon$ para todo $n \geq n_0$. Definir $s = [\{b_n\}]$, donde $b_n = (a_{n+n_0})^{-1}$. Comprobar que $\{b_n\}$ es efectivamente una sucesión de Cauchy de números racionales tal que*

$$\lim_{n\to\infty} a_n \cdot b_n = 1.$$

5) *La noción de sucesión de Cauchy de números reales es la extensión natural de la de racionales. Sea $\{a_n\}$ una sucesión de Cauchy de números reales. Para cada n, sea q_n un número racional tal que $|a_n - q_n| < 1/n$. Consideremos la sucesión $\{q_n\}$. Demostrar que:*

i) *$\{q_n\}$ es de Cauchy.*

ii) *Sea $r = [\{q_n\}]$, entonces: $\lim_{n\to\infty} a_n = r$.*

Este ejercicio nos dice que $\mathbb{R}$ es completo: Toda sucesión de Cauchy de números reales tiene un único límite real.

5.3. Desarrollos decimales

Las nociones de parte entera y parte fraccionaria tienen una extensión inmediata a $\mathbb{R}$: $r = [r] + (r)$, donde $[r] \in \mathbb{Z}$ y $0 \leq (r) < 1$. Por otro lado, todo número real $x \in [0, 1)$ admite un único desarrollo decimal:

$$x = 0{,}x_1x_2x_3 \ldots x_nx_{n+1} \ldots$$

donde cada cifra, x_j, es uno de los diez dígitos del sistema decimal de numeración, $x_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, y tales que no son todos iguales a 9 desde uno en adelante; es decir: existen infinitos $x_j < 9$.

La expresión anterior significa que tenemos la cadena infinita de desigualdades:

$$\frac{x_1}{10} + \frac{x_2}{10^2} + \cdots + \frac{x_n}{10^n} \leq x < \frac{x_1}{10} + \frac{x_2}{10^2} + \cdots + \frac{x_n + 1}{10^n}$$

válida para cada $n = 1, 2, 3, \ldots$

Es decir, las cifras decimales de x determinan la sucesión de intervalos decimales encajados que contienen al punto x, y viceversa. Recordemos que los números racionales coinciden con los desarrollos decimales periódicos (desde un punto en adelante). Por tanto, los números que llamaremos irracionales, $I = \mathbb{R} - \mathbb{Q}$, se corresponden con los desarrollos decimales que no son periódicos.

Ejemplo 1: *$3{,}101001000100001000001\ldots$ es el desarrollo de un número irracional (en su parte decimal, entre cada dos unos aparece un bloque de cada vez un cero más: un 1, un 0; un 1, dos 0; un 1, tres 0; ...).*

Ejercicio 8.

a) *Demostrar que el desarrollo decimal* $x = 0{,}x_1x_2x_3\ldots$ *es equivalente a la igualdad:*

$$x = \sum_{j=1}^{\infty} \frac{x_j}{10^j} = \lim_{n\to\infty} \sum_{j=1}^{n} \frac{x_j}{10^j}.$$

Donde supondremos siempre la condición de que hay infinitas cifras distintas de 9.

b) *Cada natural* $n > 1$ *puede ser la base de un sistema de numeración. Cuando* $n = 2$ *solo tenemos dos dígitos:* 0 *y* 1*; y los desarrollos binarios de* $x \in [0, 1)$ *son de la forma:*

$$x = 0{,}x_1x_2x_3\ldots, \qquad x_j \in \{0, 1\}$$
$$x = \sum_{j=1}^{\infty} \frac{x_j}{2^j}.$$

En este caso la condición es que existan infinitas $x_j = 0$.

Cuando $n = 3$ *tenemos tres dígitos,* 0, 1 *y* 2*. Elaborar la teoría de los desarrollos decimales en bases* 2 *y* 3*, describiendo los intervalos de* $[0, 1)$ *que dan lugar a las distintas cifras.*

c) *Hallar el desarrollo en base* 2 *del número racional un tercio.*

d) *Encontrar las tres primeras cifras decimales en base dos y en base tres de los números:* e, π *y* $\sqrt{2}$.

5.4. Ejemplos de números irracionales

Además de $\sqrt{2}$, $\sqrt{3}$, *el Teorema Fundamental de la Aritmética nos permite demostrar la irracionalidad de otras muchas raíces. Por ejemplo:* $\sqrt{p}$, p *primo, es siempre irracional, ya que si tuviéramos* $\sqrt{p} = a/b$, *con* a, b *enteros primos entre sí, entonces* $pb^2 = a^2$, *por lo que* p *debe ser un divisor de* a: $a = pa_1$. *Sustituyendo en la igualdad anterior, obtenemos que* $pb^2 = p^2a_1^2$, *es decir,* $pa_1^2 = b^2$. *Luego* p *debe ser un divisor de* b, *y esto es una contradicción con la hipótesis de partida de que* $\text{m.c.d.}(a, b) = 1$.

Ejercicio 9. *Sea* $n = p_1^{a_1} \cdots p_r^{a_r}$ *la descomposición de* n *en factores primos. Demostrar que* $\sqrt[k]{n}$ *es racional si y solo si* $k \mid a_j$ *para todo* $j = 1, \ldots, r$.

Dados dos números racionales distintos, p/q *y* p_1/q_1, *tenemos que*

$$\left|\frac{p}{q} - \frac{p_1}{q_1}\right| = \left|\frac{pq_1 - qp_1}{qq_1}\right| \geq \frac{1}{qq_1} \qquad \textit{y así:} \qquad q_1\left|\frac{pq_1 - qp_1}{qq_1}\right| \geq \frac{1}{q}.$$

Esta observación nos permite enunciar el siguiente criterio de irracionalidad: "Sea r un número real para el que podemos encontrar una sucesión de racionales distintos p_n/q_n, m.c.d.$(p_n, q_n) = 1$, tales que

$$\lim_{n\to\infty} q_n \left| r - \frac{p_n}{q_n} \right| = 0;$$

entonces r es irracional".

Un ejemplo notable es el número:

$$e = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{1}{k!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots$$

Observemos que $\dfrac{p_n}{q_n} = 1 + \dfrac{1}{1!} + \dfrac{1}{2!} + \dfrac{1}{3!} + \cdots + \dfrac{1}{n!}$ *verifica la estimación:*

$$\begin{aligned} q_n \left| e - \frac{p_n}{q_n} \right| &\leq n! \left\{ \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots \right\} \\ &= \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \dots \\ &< \frac{1}{n+1} \left\{ 1 + \frac{1}{2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \dots \right\} \\ &= \frac{2}{n+1} \longrightarrow 0, \quad n \to \infty. \end{aligned}$$

Por lo tanto e es irracional.

La demostración anterior se remonta al Siglo de las Luces, y se debe a J. Lambert. Funciona porque la representación

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \frac{1}{(n+1)!} + \dots$$

es muy buena, ya que la serie converge rápidamente.

En el caso de π tenemos fórmulas tales como

$$\pi = 4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots\right)$$

pero que no convergen con la rapidez suficiente para que podamos utilizar la estrategia anterior. No obstante, el mismo J. Lambert logró demostrar que π es también un número irracional.

Soy y seré a todos asequible
3 1 4 1 5 9
mi nombre tengo que daros
2 6 5 3 5
cociente diametral siempre inmedible
8 9 7 9
soy de los redondos aros.
3 2 3 8 4

La siguiente es una prueba por reducción al absurdo. Supongamos que π *fuese un número racional, digamos:* $\pi = m/n$, *m.c.d.*$(m, n) = 1$. *Consideremos el polinomio de segundo grado*

$$P(x) = nx(m - nx),$$

que se anula en $x = 0$ *y en* $x = m/n = \pi$, *y es positivo en el intervalo* $0 < x < \pi$. *La función "continua"*

$$e^{P(x)} = \sum_{k=0}^{\infty} \frac{P(x)^k}{k!} = \lim_{N\to\infty} \sum_{k=0}^{N} \frac{P(x)^k}{k!}$$

está acotada en $[0, \pi]$. *La integral:*

$$I = \int_0^\pi \operatorname{sen} x\, e^{P(x)}\, \mathrm{d}x = \sum_{k=0}^{\infty} \int_0^\pi \operatorname{sen} x\, \frac{P(x)^k}{k!}\, \mathrm{d}x$$

es un número real positivo, $I > 0$, *como cada uno de los números:*

$$I_k = \int_0^\pi \operatorname{sen} x\, \frac{P(x)^k}{k!}\, \mathrm{d}x.$$

La contradicción se obtiene comprobando que cada I_k *es un número entero estrictamente positivo, y, por lo tanto, mayor que* 1: *"el número* I *no puede ser la suma de infinitos enteros positivos".*

Para concluir la demostración observemos que el polinomio

$$P_k^j(x) = \mathrm{D}_x^j \left(\frac{P(x)^k}{k!} \right),$$

obtenido al derivar j *veces el polinomio de grado* $2k$ *que aparece entre paréntesis, toma siempre valores enteros cuando sustituimos* $x = 0$ *y* $x = m/n = \pi$. *Eso es una consecuencia de que , si* $j < k$, *entonces*

$$P_k^j(0) = P_k^j \left(\frac{m}{n} \right) = 0,$$

mientras que si $k \le j \le 2k$, $P_k^j(0) \neq 0$, *y al haber derivado al menos* k *veces el factor* x^k, *se obtiene el factor* $k!$, *que cancela al denominador. Igualmente ocurre en* m/n *con el factor* $(m - nx)^k$.

El cálculo de I_k se hace integrando por partes:

$$\begin{aligned}
I_k &= \int_0^\pi \operatorname{sen} x \, \frac{P(x)^k}{k!} \, \mathrm{d}x = -\int_0^\pi \frac{P(x)^k}{k!} \, \mathrm{d}\cos x \\
&= -\frac{P(x)^k}{k!} \cos x \Big|_0^\pi + \int_0^\pi \cos x \, \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{P(x)^k}{k!}\right) \mathrm{d}x \\
&= 0 + \int_0^\pi \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{P(x)^k}{k!}\right) \mathrm{d}\operatorname{sen} x \\
&= \operatorname{sen} x \, \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{P(x)^k}{k!}\right)\Big|_0^\pi - \int_0^\pi \operatorname{sen} x \, \frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(\frac{P(x)^k}{k!}\right) \mathrm{d}x \\
&= \int_0^\pi \frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(\frac{P(x)^k}{k!}\right) \mathrm{d}\cos x \\
&= \cos x \, \frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(\frac{P(x)^k}{k!}\right)\Big|_0^\pi + \int_0^\pi \cos x \, \frac{\mathrm{d}^3}{\mathrm{d}x^3}\left(\frac{P(x)^k}{k!}\right) \mathrm{d}x \\
&= \ldots
\end{aligned}$$

Observemos que $\operatorname{sen}(0) = \operatorname{sen}(\pi) = 0$, $\cos(0) = 1$, $\cos(\pi) = -1$ *y, por lo visto anteriormente:*

$$\frac{\mathrm{d}^j}{\mathrm{d}x^j}\left(\frac{P(x)^k}{k!}\right)$$

toma valores enteros en $x = 0$ y $x = \pi$. Por otro lado, el proceso anterior se acaba cuando $j = 2k$, ya que al derivar $2k + 1$ veces un polinomio de grado $2k$ obtenemos cero.

Resumiendo: "I_k es un entero y, como es estrictamente mayor que cero, resulta que $I_k \geq 1$". Esto produce la contradicción.

El número Pi

El número Pi es digno de admiración
tres coma uno cuatro uno
todas sus cifras siguientes también son iniciales
cinco nueve dos, porque nunca se termina.
No permite abarcarlo con la mirada seis cinco tres cinco
con un cálculo ocho nueve
con la imaginación siete nueve
o en broma tres dos tres, es decir, por comparación
cuatro seis con cualquier otra cosa
dos seis cuatro tres en el mundo.
La más larga serpiente después de varios metros se interrumpe.
Igualmente, aunque un poco más tarde, hacen las serpientes fabulosas.
El cortejo de cifras que forman el número Pi
no se detiene en el margen de un folio,

es capaz de prolongarse por la mesa, a través del aire,
a través del muro, de una hoja, del nido de un pájaro,
de las nubes, directamente al cielo
a través de la total hinchazón e inmensidad del cielo.
¡Oh qué corta es la cola del cometa, como la de un ratón!
¡Qué frágil el rayo de la estrella que se encorva en cualquier espacio!
Pero aquí dos tres quince trescientos noventa
mi número de teléfono la talla de tu camisa
año mil novecientos setenta y tres sexto piso
número de habitantes sesenta y cinco décimos
la medida de la cadera dos dedos la charada y el código
en la que mi ruiseñor vuela y canta
y pide un comportamiento tranquilo
también transcurren la tierra y el cielo
pero no el número Pi, este no,
él es todavía un buen cinco
no es un ocho cualquiera
ni el último siete
metiendo prisa, oh, metiendo prisa a la perezosa eternidad
para la permanencia.

Wislawa Szymborska

(Premio Nobel de Literatura 1996)

5.5. Irracionalidad de $\zeta(2)$ y $\zeta(3)$

Recordemos la identidad de Euler (capítulo 4):

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Observemos que:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \sum_{n=1}^{\infty} \left(\int_0^1 x^{n-1}\,\mathrm{d}x \right) \left(\int_0^1 y^{n-1}\,\mathrm{d}y \right) = \int_0^1 \int_0^1 \sum_{n=1}^{\infty} (xy)^{n-1}\,\mathrm{d}x\,\mathrm{d}y$$
$$= \int_0^1 \int_0^1 \frac{1}{1-xy}\,\mathrm{d}x\,\mathrm{d}y;$$

si α es un entero positivo:

$$\int_0^1 \int_0^1 \frac{x^\alpha y^\alpha}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \sum_{n=1}^{\infty} \int_0^1 \int_0^1 x^{\alpha+n-1}\,y^{\alpha+n-1}\,\mathrm{d}x\,\mathrm{d}y$$
$$= \sum_{n=1}^{\infty} \frac{1}{(n+\alpha)^2} = \zeta(2) - \sum_{n=1}^{\alpha} \frac{1}{n^2}$$

y si $\alpha < \beta$ son dos enteros positivos distintos:

$$\int_0^1 \int_0^1 \frac{x^\alpha y^\beta}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \sum_{n=1}^{\infty} \frac{1}{n+\alpha}\,\frac{1}{n+\beta} = \frac{1}{\beta-\alpha}\sum_{k=\alpha}^{\beta}\frac{1}{k}.$$

Resulta fácil ver que si $P_n(x,y) = \sum_{\substack{\alpha\le n\\ \beta\le n}} p_{\alpha,\beta}x^\alpha y^\beta$ es un polinomio de coeficientes enteros en dos variables, x, y, de grado menor o igual que n en cada una, entonces:

$$\int_0^1 \int_0^1 \frac{P_n(x,y)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = A_n\zeta(2) + \frac{B_n}{C_n}\,, \quad m.c.d.(B_n, C_n) = 1$$

donde A_n, B_n y C_n son enteros, verificándose además la desigualdad: $C_n \le m.c.m.(1,2,\ldots,n)^2$.

También que $P_n(x,y) = (1-y)^n\,\dfrac{1}{n!}\,\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}\{x^n(1-x)^n\}$ es un polinomio de coeficientes enteros.

Integrando por partes n veces en la variable x obtenemos la desigualdad:

$$\begin{aligned} 0 < \left|\int_0^1\int_0^1 \frac{P_n(x,y)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y\right| &= \left|\int_0^1\int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n}{(1-xy)^{n+1}}\,\mathrm{d}x\,\mathrm{d}y\right| \\ &\le \max_{0\le x,y\le 1}\left[\frac{x(1-x)y(1-y)}{1-xy}\right]^n \cdot \int_0^1\int_0^1 \frac{\mathrm{d}x\,\mathrm{d}y}{1-xy} \\ &\le C\left(\frac{\sqrt{5}-1}{2}\right)^{5n} \end{aligned}$$

donde C es una constante fija e independiente de n.

Finalmente el teorema de Chebychev sobre los números primos para concluir que:

$$\lim_{n\to\infty} C_n\left|A_n\zeta(2) + \frac{B_n}{C_n}\right| \le C \lim_{n\to\infty} m.c.m.(1,2,\ldots,n)^2\left(\frac{\sqrt{5}-1}{2}\right)^{5n} = 0.$$

Esto implica que $\zeta(2) = \dfrac{\pi^2}{6}$ es irracional.

El caso de $\zeta(3)$ es muy parecido: En primer lugar tenemos la representación integral siguiente:

$$\zeta(3) = -\frac{1}{2}\int_0^1\int_0^1 \frac{\log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y\,.$$

Consideremos la integral

$$\int_0^1\int_0^1 \frac{x^{\alpha+\gamma}y^{\alpha+\gamma}}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \sum_{n=1}^{\infty}\frac{1}{(\alpha+\gamma+n)^2}\,.$$

Tomando derivadas respecto de γ y evaluando en $\gamma = 0$ obtenemos

$$\int_0^1 \int_0^1 \frac{x^\alpha y^\alpha \log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = -2\sum_{n=1}^{\infty} \frac{1}{(\alpha+n)^3} = -2\Big\{\zeta(3) - \sum_{n=1}^{\infty}\frac{1}{n^3}\Big\}$$

Análogamente, si $\alpha > \beta$:

$$\int_0^1 \int_0^1 \frac{x^{\alpha+\gamma} y^{\beta+\gamma}}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \frac{1}{\alpha-\beta}\sum_{n=1}^{\infty}\Big\{\frac{1}{n+\beta+\gamma} - \frac{1}{n+\alpha+\gamma}\Big\}$$

luego, derivando respecto a γ y evaluando en $\gamma = 0$ tenemos

$$\int_0^1 \int_0^1 \frac{x^\alpha y^\beta \log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \frac{-1}{\alpha-\beta}\sum_{n=\beta+1}^{\infty}\frac{1}{n^2}\,.$$

Es decir, si $Q(x,y)$ es un polinomio de coeficientes enteros, de grado n en cada variable separadamente, entonces

$$\int_0^1 \int_0^1 \frac{Q(x,y)\log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = A_n\zeta(3) + B_n$$

donde A_n es un entero y B_n es un racional cuyo denominador de un divisor de d_n^3, $d_n = m.c.m.\{1,\ldots,n\}$.

Escogiendo $P_n(x,y) = P_n(x)\,P_n(y)$

$$I_n = \int_0^1 \int_0^1 \frac{P_n(x,y)\log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \int_0^1\int_0^1\int_0^1 \frac{P_n(x)P_n(y)}{1-(1-xy)u}\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}u$$
$$= \int_0^1\int_0^1\int_0^1 \frac{x^n y^n u^n (1-x)^n P_n(y)}{(1-(1-xy)u)^{n+1}}\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}u$$

después de integrar por partes, n veces, respecto de la variable x.

El cambio de variables

$$u = \frac{1-w}{1-(1-xy)w}\,, \qquad \mathrm{d}u = \frac{-xy}{(1-(1-xy)w)^2}\,\mathrm{d}w$$

nos permite escribir

$$I_n = \int_0^1\int_0^1\int_0^1 \frac{(1-x)^n(1-w)^n P_n(y)}{1-(1-xy)w}\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}w\,.$$

Integramos por partes, de nuevo n veces, pero ahora respecto a la variable y:

$$\begin{aligned} I_n &= \int_0^1\int_0^1\int_0^1 \frac{x^n(a-x)^n y^n(1-y)^n w^n(1-w)^n}{\big[1-(1-xy)w\big]^{n+1}}\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}w \\ &\le \Big[\max\Big(\frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w}\Big)\Big]^n \cdot \int_0^1\int_0^1\int_0^1 \frac{1}{1-(1-xy)w}\,\mathrm{d}x\mathrm{d}y\mathrm{d}w \\ &= C\big(\sqrt{2}-1\big)^{4n}. \end{aligned}$$

La irracionalidad de $\zeta(3)$ es una consecuencia de que $(\sqrt{2}-1)^{4n}e^3 < 1$ y del teorema de Chebychev.

Ejercicio 10. *Un número real x puede ser escrito de la forma siguiente:*

$$x = [x] + (x) = [x] + \frac{1}{\frac{1}{(x)}}$$

llamando $a_0 = [x]$, $a_1 = \big[\frac{1}{(x)}\big] \ge 1$, tenemos que:

$$x = a_0 + \frac{1}{a_1 + \big(\frac{1}{(x)}\big)}.$$

Este procedimiento puede ser iterado:

$$a_2 = \left[\frac{1}{\big(\frac{1}{(x)}\big)}\right], \dots$$

para obtener el desarrollo en fracción continua:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \dots}}} \qquad \text{que se abrevia como } [a_0; a_1, a_2, \dots].$$

1. *Hallar los desarrollos en fracción continua de los racionales $\frac{3}{5}$, $\frac{21}{17}$ y $\frac{113}{24}$.*

2. *La razón áurea $\Phi = \dfrac{\sqrt{5}+1}{2}$ verifica la ecuación $\Phi^2 = \Phi + 1$, que puede escribirse de la manera siguiente:*

$$\Phi = 1 + \frac{1}{\Phi} = 1 + \frac{1}{1+\frac{1}{\Phi}} = \cdots = [1; 1, 1, \dots].$$

   Hallar las fracciones continuas de los números $\sqrt{2}$, $\sqrt{3}$ y $\sqrt{7}$.

3. *¿Qué números reales tienen fracciones continuas finitas? ¿A quién corresponden los desarrollos periódicos?*

4. *Hallar los tres primeros cocientes parciales, a_j, $j = 0, 1, 2$, de las fracciones continuas de e y de π.*

5.6. El continuo y sus enigmas

Un resultado muy importante de la Teoría de Conjuntos, obtenido por Cantor, es el siguiente:

Teorema. *Los números reales no son un conjunto numerable.*

Demostración. *(Reducción al absurdo) Supongamos lo contrario, entonces todos los reales del intervalo* $[0,1)$ *pueden ponerse en una sucesión:*

$$[0,1) = \{x_1, x_2, x_3, \dots, x_n, \dots\}.$$

Usando ahora los desarrollos decimales (en base 10*, por ejemplo) podemos escribir:*

$$\begin{aligned} x_1 &= 0, x_1^1\, x_1^2\, x_1^3\, x_1^4 \dots\, x_1^n \dots \\ x_2 &= 0, x_2^1\, x_2^2\, x_2^3\, x_2^4 \dots\, x_2^n \dots \\ x_3 &= 0, x_3^1\, x_3^2\, x_3^3\, x_3^4 \dots\, x_3^n \dots \\ x_4 &= 0, x_4^1\, x_4^2\, x_4^3\, x_4^4 \dots\, x_4^n \dots \\ \vdots &\qquad \dots\dots \end{aligned}$$

Sea $y = 0{,}y^1y^2y^3y^4 \dots y^n \dots$ *el número del intervalo* $[0,1)$ *cuyas cifras han sido elegidas de manera que:*

$$y^1 \neq x_1^1,\ y^1 \neq 9; \quad y^2 \neq x_2^2,\ y^2 \neq 9; \quad \dots; \quad y^n \neq x_n^n,\ y^n \neq 9; \quad \dots$$

La unicidad de los desarrollos decimales implica que $y \neq x_j$*, para todo* j*, por cuanto* $y^j \neq x_j^j$*. Pero eso contradice la hipótesis de partida acerca de que todos los elementos de* $[0,1)$ *estaban en la fila* $\{x_j\}$*.* ■

Los conjuntos infinitos que pueden ponerse en correspondencia biyectiva con los naturales (o que son equinumerables o equipotentes con los naturales) son los numerables, o los que pueden ponerse en fila. Diremos que su cardinal es $\aleph_0$ *("alef subcero"). La prueba de Cantor muestra que el cardinal de* $\mathbb{R}$ *(al que llamaremos* $\mathcal{C}$*, o continuo), es distinto de* $\aleph_0$*. Podríamos decir que es mayor, por cuanto* $\mathbb{N} \subset \mathbb{R}$ *y* $card\,\mathbb{N} = \aleph_0$*. Un instrumento básico para comparar cardinales es el siguiente.*

Lema. *(Cantor–Schröder–Bernstein). Sean* X*,* Y *dos conjuntos tales que existen dos aplicaciones inyectivas* $\varphi : X \longrightarrow Y$ *y* $\psi : Y \longrightarrow X$*. Entonces hay una biyección* $\Phi : X \longrightarrow Y$*, es decir, los conjuntos* X *e* Y *son biyectables, equipotentes o equinumerables.*

Este lema garantiza pues que la definición

$$card(X) \leq card(Y) \ :\equiv:\ X \text{ es inyectable en } Y,$$

es consistente con la implicación

$$\Big(\big((card(X) \leq card(Y)\big) \wedge \big((card(Y) \leq card(X)\big)\Big) \Longrightarrow \big(card(X) = card(Y)\big).$$

Demostración. *Dado un $y_1 \in Y$ vamos a construir una familia $y_1, x_1, y_2, x_2, \ldots$ de elementos, alternando entre Y y X, de la siguiente manera:*

- $\boxed{1}$ *Puede existir o no un $x_1 \in X$ tal que $\varphi(x_1) = y_1$. Si existe es único (porque φ es inyectiva). Elijamos, si podemos, x_1 como la preimagen de y_1.*
- $\boxed{2}$ *Supongamos que hemos obtenido x_1 en $\boxed{1}$. Elegimos y_2 como el único, si existe, elemento de Y tal que $\psi(y_2) = x_1$ (ψ es inyectiva); y_2 puede no existir.*
- $\boxed{3}$ *Si hemos obtenido y_2 en $\boxed{2}$, construyo, si puedo, $x_2 \in X$ como en $\boxed{1}$, a partir de $y_2 \in Y$.*

Si seguimos este proceso pueden ocurrir tres cosas:

a) *Paramos en X, i.e., obtenemos algún $x_n \in X$ y paramos porque $\nexists y \in Y$ con $\psi(y) = x_n$ (ψ no es necesariamente sobreyectiva).*
b) *Paramos en Y, i.e., obtenemos algún $y_m \in Y$ y paramos porque $\nexists x \in X$ con $\varphi(x) = y_m$ (φ no es necesariamente sobreyectiva).*
c) *No paramos.*

Así, para cada $y \in Y$ tenemos un proceso bien definido que nos plantea 3 posibles casos, dando lugar a una partición de Y en 3 conjuntos disjuntos:

$$\begin{aligned} Y_X &= \{y \in Y \mid \textit{paramos en } X\} \\ Y_Y &= \{y \in Y \mid \textit{paramos en } Y\} \\ Y_\infty &= \{y \in Y \mid \textit{no paramos}\}. \end{aligned}$$

El mismo proceso se puede montar para X, obteniendo una partición de X en 3 conjuntos disjuntos:

$$\begin{aligned} X_X &= \{x \in X \mid \textit{paramos en } X\} \\ X_Y &= \{x \in X \mid \textit{paramos en } Y\} \\ X_\infty &= \{x \in X \mid \textit{no paramos}\}. \end{aligned}$$

Es fácil ver que las siguientes aplicaciones son biyectivas:

$$\begin{aligned} \psi : Y_Y &\longrightarrow X_Y \\ \varphi : X_X &\longrightarrow Y_X; \quad \varphi^{-1} : Y_X \longrightarrow X_X \\ \psi : Y_\infty &\longrightarrow X_\infty. \end{aligned}$$

Se tiene así una biyección $F : Y \longrightarrow X$ definida como sigue

$$F(y) = \begin{cases} \psi(y) & \textit{si } y \in Y_Y \\ \varphi^{-1}(y) & \textit{si } y \in Y_X \\ \psi(y) & \textit{si } y \in Y_\infty. \end{cases}$$

■

Ejemplo 2: *Sean* $X = (0,1) \subset \mathbb{R}$ *e* $Y = (0,1] \subset \mathbb{R}$, *y tomemos las siguientes aplicaciones inyectivas:*

$$\begin{array}{rcl} \varphi : X & \longrightarrow & Y \\ x & \longmapsto & \varphi(x) = x \end{array} \qquad \begin{array}{rcl} \psi : Y & \longrightarrow & X \\ y & \longmapsto & \psi(y) = \dfrac{1}{2}\, y\,. \end{array}$$

Obsérvese que $\mathrm{Im}(\varphi) = (0,1)$ *e* $\mathrm{Im}(\psi) = (0,1/2)$. *Si aplicamos el algoritmo descrito en la demostración del lema de Cantor–Schröeder–Bernstein, se obtienen las siguientes particiones de* X *e* Y*:*

$$\begin{array}{ll} X = X_X \cup X_Y \cup X_\infty & Y = Y_X \cup Y_Y \cup Y_\infty \\ \textit{donde:} & \textit{donde:} \\ X_X = \displaystyle\bigcup_{n=0}^{\infty} \left(\frac{1}{2^{n+1}}, \frac{1}{2^n}\right) & Y_X = \displaystyle\bigcup_{n=0}^{\infty} \left(\frac{1}{2^{n+1}}, \frac{1}{2^n}\right) \\ X_Y = \left\{\dfrac{1}{2^{n+1}}\right\}_{n=0}^{\infty} & Y_Y = \left\{\dfrac{1}{2^n}\right\}_{n=0}^{\infty} \\ X_\infty = \emptyset & Y_\infty = \emptyset\,, \end{array}$$

y las siguientes aplicaciones biyectivas:

$$\begin{array}{rcl} \psi : Y_Y & \longrightarrow & X_Y \\ y & \longmapsto & \psi(y) = \dfrac{1}{2}\, y \end{array} \qquad \begin{array}{rcl} \varphi^{-1} : Y_X & \longrightarrow & X_X \\ y & \longmapsto & \varphi^{-1}(y) = y. \end{array}$$

De esta manera, se obtiene la siguiente biyección $F : Y \longrightarrow X$*:*

$$F(y) = \begin{cases} \dfrac{1}{2}\, y & \textit{si } y \in Y_Y \\ y & \textit{si } y \in Y_X. \end{cases}$$

Es un buen ejercicio para el lector comprobar que todas las afirmaciones realizadas son ciertas.

La función $y = \tan x$ *es una biyección del intervalo* $(-\pi/2, \pi/2)$ *con la recta real* $\mathbb{R} = (-\infty, +\infty)$. *Luego ambos tienen el mismo cardinal,* $\mathcal{C}$. *La transformación* $y = (2a/\pi)x$ *es una biyección entre* $(-\pi/2, \pi/2)$ *y* $(-a, a)$.

Por otra lado la traslación $y = x - (a+b)/2$ *lleva el intervalo* (a,b) *en el intervalo* $(-(b-a)/2, (b-a)/2)$. *Combinando estas transformaciones, podemos concluir que todo intervalo abierto* (a,b), $a < b$, *es equipotente (o equinumerable) con la recta real* $\mathbb{R}$, *y su cardinal es el continuo* $\mathcal{C}$.

Ejercicio 11. *Probar que* $y = \dfrac{x}{1-|x|}$ *es una biyección entre* $(-1,1)$ *y* $\mathbb{R}$.

Dado el intervalo cerrado $[a,b]$, $a<b$, la traslación $y=x-a$ lo pone en correspondencia biyectiva con $[0,b-a]$. A su vez, la homotecia

$$y=\frac{x}{b-a}$$

es una biyección de $[0,b-a]$ con $[0,1]$. La inclusión

$$\begin{array}{rcl}[0,1] & \longrightarrow & \mathbb{R}\\ t & \longmapsto & t\end{array}$$

es una inyección de $[0,1]$ en $\mathbb{R}$.

Por otro lado sabemos que $\mathbb{R}$ y $(0,1)$ son equipotentes, luego existe una inyección $\varphi:\mathbb{R}\longrightarrow(0,1)\subset[0,1]$. Por el lema de Cantor–Schröder–Bernstein, $\mathbb{R}$ y $[a,b]$ son equipotentes. Un razonamiento similar sirve para los intervalos semiabiertos $[a,b)$ y $(a,b]$.

Corolario. *Todos los intervalos de $\mathbb{R}$ no triviales (distintos de un punto) son equipotentes a $\mathbb{R}$; es decir, siempre que $a<b$ se tiene:*

$$card\big([a,b]\big)=card\big((a,b)\big)=card\big([a,b)\big)=card\big((a,b]\big)=card\big(\mathbb{R}\big).$$

Como $\mathbb{R}=\mathbb{Q}\cup I$ y sabemos que la unión de dos conjuntos numerables es numerable, podemos concluir que el conjunto I, de los números irracionales, no es numerable. Eso no implica, automáticamente, que su cardinal sea el continuo. Pero sí lo es por la proposición siguiente.

Proposición. *I es equipotente a $\mathbb{R}$.*

Demostración 1. *Sea $\mathbb{P}^{1/2}=\big\{\sqrt{p}\mid p \text{ número primo}\big\}$. Tenemos que:*

$$\mathbb{R}=\Big(\mathbb{Q}\cup\mathbb{P}^{1/2}\Big)\cup\Big(\mathbb{R}-\Big(\mathbb{Q}\cup\mathbb{P}^{1/2}\Big)\Big).$$

Observemos que $\mathbb{P}^{1/2}$ y $\mathbb{Q}\cup\mathbb{P}^{1/2}$ son ambos numerables y, por tanto, existe una biyección: $\Phi:\mathbb{Q}\cup\mathbb{P}^{1/2}\longrightarrow\mathbb{P}^{1/2}$. Entonces la función ψ definida por la fórmula:

$$\begin{cases}\psi(x) = \Phi(x) & \text{si } x\in\mathbb{Q}\cup\mathbb{P}^{1/2}\\ \psi(x) = x & \text{si } x\in\mathbb{R}-\big(\mathbb{Q}\cup\mathbb{P}^{1/2}\big)\end{cases}$$

es una biyección entre $\mathbb{R}$ y

$$\mathbb{P}^{1/2}\cup\Big(\mathbb{R}-\Big(\mathbb{Q}\cup\mathbb{P}^{1/2}\Big)\Big)=\mathbb{R}-\mathbb{Q}=I.$$

■

Demostración 2. *Por el lema de Cantor-Schröder-Bernstein, basta verificar que es inyectiva la siguiente función* $f : \mathbb{R} \to I$

$$f(x) = \begin{cases} x + x/|x| & si\ x \in I \\ x/\sqrt{3} & si\ \sqrt{3} > |x| \in \mathbb{Q} \\ \sqrt{2}/x & si\ \sqrt{3} < |x| \in \mathbb{Q} \end{cases}$$

porque: cada una de esas fórmulas da una función inyectiva, $|f(x)| > 1$ *si y solo si* $x \in I$*, y no puede ser* $x/\sqrt{3} = \sqrt{2}/y$*, es decir* $xy = \sqrt{6}$ *para dos racionales* x*,* y*.* ■

Ejercicio 12. *Dar una demostración de esta última proposición, esencialmente distinta a las dos mostradas.*

Proposición. *El producto cartesiano* $[0,1) \times [0,1)$ *es equipotente a* $[0,1)$*.*

Demostración. *Usaremos los desarrollos decimales (en base* 10*). Dado un punto* $(x, y) \in [0,1) \times [0,1)$ *consideremos los desarrollos decimales*

$$\begin{aligned} x &= 0{,}x_1x_2x_3\ldots \\ y &= 0{,}y_1y_2y_3\ldots \end{aligned}$$

Con ellos le asignamos el punto $z = 0{,}x_1y_1x_2y_2x_3y_3\ldots \in [0,1)$*. Por otro lado la inclusión* $x \mapsto (x, 0)$ *es una inyección de* $[0,1)$ *en* $[0,1) \times [0,1)$*. El lema de Cantor–Schröder–Bernstein nos permite concluir la faena.* ■

Ejercicio 13. *a) Demostrar que si* $a < b$ *y* $c < d$ *entonces todos los cuadrados* $(a,b)\times(c,d)$*,* $[a,b)\times(c,d)$*,* $[a,b)\times[c,d)$*, . . . ,* $[a,b]\times[c,d]$ *son biyectables con* $\mathbb{R}$*.*

b) Probar que $\mathbb{R}^k$ *y* $\mathbb{R}$ *son conjuntos equipotentes para todo* $k = 1, 2, 3, \ldots$*. Explicar qué ocurre en el caso:*

$$\mathbb{R}^{\mathbb{N}} = \mathbb{R} \times \mathbb{R} \times \cdots = \{(x_n)_{n=1}^{\infty} \mid x_n \in \mathbb{R}\}.$$

Para un conjunto finito, A*, con* n *elementos (*$card(A) = n$*), sabemos que* $\mathcal{P}(A) = \{$ *subconjuntos de* $A\}$ *tiene cardinal* 2^n*:*

$$card(\mathcal{P}(A)) = 2^n > card(A).$$

Esta relación sigue siendo válida también en el caso de conjuntos infinitos. Por ejemplo: $card(\mathcal{P}(\mathbb{N})) = card(\mathbb{R}) = \mathcal{C}$*. Dado un subconjunto de* $\mathbb{N}$*, que podemos suponer ordenado* $E = \{n_1 < n_2 < n_3 < \ldots\}$*, la función*

$$\varphi(E) = 0{,}0\cdots\overset{n_1}{1}0\cdots\overset{n_2}{1}0\cdots\overset{n_3}{1}0\cdots$$

le asigna un número real del intervalo $[0,1)$ *cuyo desarrollo "decimal" en base* 3 *tiene el dígito* 1 *en las posiciones* n_k *del conjunto* E *y el* 0 *en las restantes. Es fácil ver que* φ *es biyectiva.*

Teorema. *No existe una biyección entre X y $\mathcal{P}(X)$, de otra manera*

$$card(X) < card(\mathcal{P}(X)).$$

Demostración. *(Por reducción al absurdo). Supongamos que existe una tal biyección $\Phi : X \longrightarrow \mathcal{P}(X)$. En particular, para cada $x \in X$, su imagen, $\Phi(x)$ es un subconjunto de X que puede contener a x, o puede no contenerlo. Sea $E = \{x \in X \mid x \notin \Phi(x)\} \subset X$, y por tanto $E \in \mathcal{P}(X)$. Como Φ es una biyección, existirá un único $e \in X$ tal que $\Phi(e) = E$. Tenemos dos posibilidades:*

$$a)\, e \in \Phi(e) \quad y \quad b)\, e \notin \Phi(e).$$

Ahora bien: a) no puede ser, por cuanto $\phi(e) = E = \{x \in X \mid x \notin \Phi(x)\}$. Luego $e \notin \Phi(e)$, pero esto resulta también imposible por la definición de E, ya que si $e \notin \Phi(e)$ entonces e debería pertenecer a $E = \Phi(e)$. ■

Corolario. $\mathcal{C} = card(\mathbb{R}) < card(\mathcal{P}(\mathbb{R})) < card(\mathcal{P}(\mathcal{P}(\mathbb{R})) < \ldots$

Luego tenemos un procedimiento para generar conjuntos de cardinalidad arbitrariamente grande. No obstante, la pregunta que cada vez parece más relevante es la siguiente: ¿Existe un conjunto cuyo cardinal esté estrictamente comprendido entre $\aleph_0$ y $\mathcal{C}$? ¿Es $\mathcal{C} = \aleph_1$?

Conocida como la hipótesis del continuo, fue abordada por Cantor y recogida en la famosa lista de problemas que elaboró D. Hilbert para el Congreso Internacional de Matemáticas celebrado en París en el año 1900. La solución se debe a K. Gödel y P. Cohen: resulta que la hipótesis del continuo es independiente de los otros axiomas de la Teoría de Conjuntos (axiomas de Zermelo–Fraenkel que discutiremos en el capítulo 8). Es decir, podemos adoptarla como un nuevo axioma de nuestra teoría sin peligro de que el sistema así ampliado sea inconsistente, dé lugar a contradicciones, sin que lo fuera el de partida.

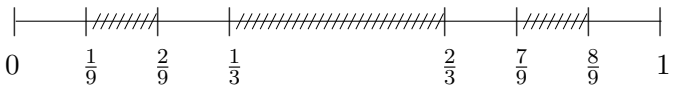
Pero también podríamos, si eso fuese conveniente, introducir como axioma su negación. La hipótesis del continuo generalizada afirma que entre $card(X)$ y $card(\mathcal{P}(X))$ no existe un cardinal intermedio. La demostración de Gödel y Cohen prueba también la independencia del axioma generalizado respecto al sistema de Zermelo–Fraenkel.

En particular, este resultado hace ociosa la búsqueda de subconjuntos de $\mathbb{R}$ con un cardinal comprendido estrictamente entre $\aleph_0$ y $\mathcal{C}$. Empero, los esfuerzos realizados por Cantor, y otros muchos, dieron lugar a construcciones que luego resultaron ser útiles para resolver otros problemas. Un ejemplo notable es el llamado conjunto de Cantor.

El conjunto de Cantor. *En su construcción se comienza dividiendo el intervalo unidad,* $[0,1)$*, en tres partes iguales:*

$$[0,1) = \left[0,\tfrac{1}{3}\right) \cup \left[\tfrac{1}{3},\tfrac{2}{3}\right) \cup \left[\tfrac{2}{3},1\right),$$

y eliminamos el trozo de en medio, $[\frac{1}{3},\frac{2}{3})$*.*



Luego se repite el proceso con los dos intervalos restantes:

$$\begin{aligned}\left[0,\tfrac{1}{3}\right) &= \left[0,\tfrac{1}{9}\right) \cup \left[\tfrac{1}{9},\tfrac{2}{9}\right) \cup \left[\tfrac{2}{9},\tfrac{1}{3}\right)\\ \left[\tfrac{2}{3},1\right) &= \left[\tfrac{2}{3},\tfrac{7}{9}\right) \cup \left[\tfrac{7}{9},\tfrac{8}{9}\right) \cup \left[\tfrac{8}{9},1\right),\end{aligned}$$

para eliminar los de en medio: $[\frac{1}{9},\frac{2}{9})$*,* $[\frac{7}{9},\frac{8}{9})$*; y así sucesivamente. El conjunto de Cantor es lo que queda del intervalo* $[0,1)$ *después de repetir el proceso anterior una cantidad numerable de veces.*

Otra descripción del conjunto de Cantor se consigue al escribir, en base 3*, el desarrollo decimal de los números del intervalo* $[0,1)$*. Obtenemos expresiones* $0{,}x_1x_2x_3\ldots$*, donde los dígitos son ahora* 0*,* 1 *o* 2*. En la primera etapa de la construcción del conjunto de Cantor eliminamos el intervalo central,* $[1/3,2/3)$*, que consta precisamente de los números cuya primera cifra decimal es* 1*.*

En la segunda etapa los intervalos suprimidos, $[1/9,2/9)$ *y* $[7/9,8/9)$*, son, respectivamente, los números cuyo desarrollo empieza como* $0{,}01\ldots$ *o* $0{,}21\ldots$ *Es decir, al quitar ambos intervalos nos aseguramos que* 1 *no aparezca entre las dos primeras cifras decimales del conjunto. Y así sucesivamente: el conjunto de Cantor está constituido por los elementos,* $0{,}x_1x_2x_3\ldots$*, del intervalo* $[0,1)$ *en cuyo desarrollo en base* 3 *no aparece la cifra* 1*.*

Si en lugar de base 3 *tomamos ahora base* 2*, entonces todo número real* $y \in [0,1)$*, admite un único desarrollo de la forma* $y = 0{,}y_1y_2y_3\ldots$ *donde los dígitos* $y_j \in \{0,1\}$*, y la igualdad significa* $y = \sum_{j=1}^{\infty} y_j/2^j$*.*

Lema. *Existe una biyección entre el conjunto de Cantor,* C*, y el intervalo real* $[0,1)$*. Es decir, el cardinal de* C *es el continuo.*

Demostración. *Sea*

$$x = 0{,}x_1x_2x_3\ldots$$

el desarrollo en base 3 *de un elemento del conjunto de Cantor. Como* $x_j \neq 1$ *para todo* j*, resulta que* $y_j = x_j/2$ *es uno de los dígitos* 0 *o* 1*. Considerado en base* 2*, el desarrollo* $y = 0{,}y_1y_2y_3\ldots$ *es un número del intervalo* $[0,1)$*, y la función* $y = \phi(x)$ *así construida es una biyección:* $\phi : C \longrightarrow [0,1)$*.* ■

El conjunto de Cantor tiene otras muchas propiedades notables. Por ejemplo, es autosemejante: si cortamos un trozo y lo ampliamos suficientemente, reproduciremos el conjunto. Es también un fractal, es decir un conjunto de dimensión fraccionaria. Otra propiedad importante es que tiene medida nula.

Definición. *Un subconjunto $A \subset \mathbb{R}$ tiene medida nula si para todo $\varepsilon > 0$ existe una colección numerable de intervalos $\{I_n\}$, $I_n = (a_n, b_n)$, tales que:*

$$A \subset \bigcup I_n \quad y \quad \sum_{n=1}^{\infty} |b_n - a_n| < \varepsilon.$$

Metafóricamente podemos describir un conjunto de medida nula en $\mathbb{R}$ como uno que puede ser tapado con un trozo de cinta adhesiva tan pequeño como queramos. Dada una pieza de longitud $\varepsilon > 0$ podemos partirla en trozos $\widetilde{I}_n$ tales que $\sum \mu(\widetilde{I}_n) = \varepsilon$ de manera que trasladando estos trozos convenientemente a posiciones I_n cubrimos a todo el conjunto $A \subset \bigcup I_n$.

Un ejemplo de un conjunto de medida nula es el que solo tiene un punto, $\{q\}$, o un número finito de puntos, $\{q_1, \ldots, q_n\}$. Hay, sin embargo, muchos conjuntos infinitos con medida nula.

Lema. *Si $A = \{a_1, a_2, a_3, \ldots\}$ es numerable, entonces tiene medida nula.*

Demostración. *Dado $\varepsilon > 0$, consideremos los intervalos:*

$$\begin{aligned} I_1 &= \big(a_1 - \frac{\varepsilon}{2^2}, a_1 + \frac{\varepsilon}{2^2}\big) \\ I_2 &= \big(a_2 - \frac{\varepsilon}{2^3}, a_2 + \frac{\varepsilon}{2^3}\big) \\ &\vdots \quad \ldots\ldots \\ I_n &= \big(a_n - \frac{\varepsilon}{2^{n+1}}, a_n + \frac{\varepsilon}{2^{n+1}}\big) \\ &\vdots \quad \ldots\ldots \end{aligned}$$

Es claro que $A \subset \bigcup_{n=1}^{\infty} I_n$, mientras que $\sum_{n=1}^{\infty} \text{longitud}\,(I_n) = \sum_{n=1}^{\infty} \frac{2\varepsilon}{2^{n+1}} = \varepsilon$. ■

En particular, los racionales, aunque densos en $\mathbb{R}$, son un conjunto de medida nula por ser numerable. El conjunto de Cantor, sin embargo, nos da un conjunto de medida nula que no es numerable.

Lema. *El conjunto de Cantor tiene medida nula.*

Demostración. *Observemos que según la primera etapa de su construcción, C está contenido en la unión de dos intervalos de longitud $1/3$ cada uno. En el segundo paso obtenemos C contenido en la unión de 4 intervalos de longitud $1/3^2, \ldots$, en el paso n-ésimo C aparece contenido en la unión de 2^n intervalos de longitud $(1/3)^n$. Como $\lim_{n\to\infty}(2/3)^n = 0$, resulta que C es de medida nula.* ■

El hecho de que $\mathbb{Q}$ tenga medida nula en $\mathbb{R}$ tiene una interesante interpretación probabilística. Si elegimos un número "al azar" la probabilidad de que sea racional es cero. "Casi todos" los números son irracionales. No obstante, si alguien nos señala un número concreto, por ejemplo,

$$\pi^e, \quad \gamma = \lim_{n\to\infty}\Big(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log(n)\Big), \quad \zeta(5)=\sum_{n=1}^{\infty}\frac{1}{n^5}\,,$$

y nos pregunta si es racional o irracional, es posible que nos ponga en un aprieto, y no sepamos contestar. Es una situación paradójica que da que pensar: resulta relativamente fácil saber que casi todos los números reales son irracionales, pero puede ser un problema tremendo el decidir si un número concreto, por ejemplo 2^π, lo es o no lo es.

Ejercicio 14. *Demostrar que si $\{E_n\}$ es una familia numerable de conjuntos de medida nula su unión, $\bigcup_n E_n$, es también de medida nula.*

Indicación: dado $\varepsilon>0$ podemos gastar $\frac{\varepsilon}{2}$ encontrando una familia numerable de intervalos que cubren E_1 y cuya suma de longitudes sea menor o igual que $\frac{\varepsilon}{2}$; luego con $\frac{\varepsilon}{4}$ nos apañamos para cubrir I_2 y así sucesivamente. El cardinal total de intervalos usados en los pasos es numerable (unión numerable de numerables) y la suma de longitudes de todos ellos será menor o igual que $\varepsilon=\sum_{n=1}^{\infty}\frac{\varepsilon}{2^n}$.

Consideremos los desarrollos decimales en base 10 de los números del intervalo $[0,1)$:

$$x = 0{,}x_1x_2x_3\ldots \qquad x_j\in\{0,1,2,3,4,5,6,7,8,9\}.$$

Escojamos una cifra, por ejemplo 7, y tratemos de medir el subconjunto de los x tales que la cifra 7 no aparezca en su desarrollo decimal:

> *$x_1\neq 7 \iff x\notin\left[\frac{7}{10},\frac{8}{10}\right)$ luego hemos eliminado un intervalo de longitud $\frac{1}{10}$.*
>
> *En los 9 intervalos restantes $\left[\frac{k}{10},\frac{k+1}{10}\right)$, $k\neq 7$, la condición $x_2\neq 7$ exige quitar, en cada uno de ellos, un intervalo de longitud $\frac{1}{100}$. Precisamente: $x\notin\left[\frac{k}{10}+\frac{7}{100},\frac{k}{10}+\frac{8}{100}\right)$. En total 9 intervalos de longitud $\frac{1}{100}$.*
>
> *En cada uno de los $9^2=81$ intervalos restantes la condición $x_3\neq 7$ exige eliminar un intervalo de longitud $\frac{1}{1000}$.*

Y así sucesivamente: en cada paso del proceso nos vemos obligados a eliminar 9^{n-1} intervalos de longitud $\frac{1}{10^n}$. Si sumamos sus longitudes resulta que

$$\frac{1}{10}+\frac{9}{10^2}+\frac{9^2}{10^3}+\cdots=\frac{1}{10}\sum_{k=0}^{\infty}\left(\frac{9}{10}\right)^k=\frac{\frac{1}{10}}{1-\frac{9}{10}}=1,$$

lo que equivale a afirmar que el conjunto complementario $=\big\{x\in[0,1)\mid$ el desarrollo decimal de x no contiene el dígito $7\big\}$ es un conjunto de medida nula.

Como la cifra 7 *no tiene nada de especial y como la unión de* 10 *conjuntos de medida nula es también de medida nula, podemos afirmar lo siguiente:*

> *Los puntos del intervalo* $[0,1)$ *en cuyo desarrollo decimal falta alguno de los dígitos es un conjunto de medida nula. Dicho de otra manera: si con los ojos bien cerrados escogemos un número al "azar" en* $[0,1)$ *entonces, con probabilidad igual a* 1*, hallaremos todos los dígitos entre sus cifras decimales.*

Supongamos ahora que en vez de un solo dígito nos interesan dos de ellos y nos preguntamos por los desarrollos $x = 0{,}x_1x_2x_3x_4x_5x_6\ldots$ *tales que* $x_{2k-1}x_{2k} \neq 75$ *para todo* $k = 1, 2, 3, \ldots$

Veamos: $x_1x_2 \neq 75$ *elimina el siguiente intervalo de longitud* $\frac{1}{100}$*:*

$$\left[\frac{7}{10} + \frac{5}{100}, \frac{7}{10} + \frac{6}{100}\right).$$

La condición $x_3x_4 \neq 75$ *en cada uno de los* 99 *intervalos restantes* $\left[\frac{k}{10} + \frac{j}{100}, \frac{k}{10} + \frac{j+1}{100}\right)$*,* $k = 0, 1, 2, \ldots, 9$*,* $j = 0, 1, 2, \ldots, 9$*,* $(k, j) \neq (7, 5)$*, elimina un subintervalo de longitud* $\frac{1}{100^2}$*. Y así sucesivamente. En total la longitud de los intervalos eliminados es:*

$$\frac{1}{100} + \frac{99}{100^2} + \frac{99^2}{100^3} + \cdots = \frac{\frac{1}{100}}{1 - \frac{99}{100}} = 1.$$

Luego su complementario en $[0,1)$ *es de medida cero.*

Observemos de nuevo que la sucesión 75 *no tiene nada de particular y que el mismo razonamiento nos serviría para cualquier otro par de dígitos* (k, j)*. Como en total obtenemos* $10 \times 10 = 100$ *conjuntos de medida nula, su unión también lo será. Es decir: excepto por un conjunto de medida cero los números del intervalo* $[0,1)$ *contienen cualquiera de las* 100 *combinaciones de dígitos* mn *en posiciones sucesivas de su desarrollo decimal.*

Pero lo hecho para dos nos sirve también para tres, cuatro... Estamos pues en condiciones de ser más ambiciosos y con el mismo argumento probar que, para cada n*, existe un subconjunto* E_n *de medida nula,* $\mu(E_n) = 0$*, tal que si* $x \in [0,1) \setminus E_n$ *entonces el desarrollo decimal del número* x *contiene todas las* 10^n *sucesiones posibles de* n *dígitos.*

Ahora bien, sabemos que la unión de todos esos conjuntos $E = \bigcup E_n$ *tiene también medida nula. Luego su complementario* $[0,1) \setminus E$ *no puede ser numerable, ni por consiguiente vacío. Sea pues* α *un número en* $[0,1) \setminus E$*, entonces el desarrollo decimal de* α *contendrá cualquier sucesión finita de dígitos que podamos escribir: nuestro N.I.F.; el número de nuestro teléfono; los números premiados en la lotería; la fecha de nuestro nacimiento... ¡todo!*

La discusión anterior podríamos haberla hecho con otras bases de numeración. En particular el sistema binario está especialmente adaptado al funcionamiento de los ordenadores. Los dígitos son ahora 0 *y* 1 *y todo* $x \in [0,1)$ *tiene un único desarrollo*

$$x = 0{,}x_1x_2\ldots\,, \qquad x_j = 0 \text{ o } 1\,, \qquad x = \sum_{j=1}^{\infty} \frac{x_j}{2^j}.$$

Salvo por un conjunto E *de medida cero, todo* $x \in [0,1)$ *contiene cualquier sucesión finita de dígitos (*0 *y* 1*) colocados de forma consecutiva en su desarrollo decimal en base* 2*.*

Por lo tanto, si elegimos un número β *al azar en el intervalo* $[0,1)$*, con probabilidad igual a* 1*, tendremos que dada una sucesión cualquiera de dígitos, por ejemplo* 10011100110101100001001*0, aparecerá siempre en el número* $\beta = 0,\beta_1\beta_2\beta_3\ldots$ *aunque quizás tengamos que avanzar mucho, tal vez muchísimo, en su desarrollo decimal.*

Supongamos ahora un alfabeto, por ejemplo el castellano, que conste de letras, signos ortográficos, tales como $\boxed{\text{, . : ; ¿ ? ¡ ! ( )}}$ *..., y al que hemos añadido también un signo para los espacios en blanco. Escogiendo* n *suficientemente grande podemos asignar un número natural menor que* $N = 2^n$ *a cada signo. No importa cómo lo hagamos, por ejemplo* $(a = 0)$*,* $(b = 1)$*, ...,* $(z = 27)$*, (espacio en blanco* $= 28)$*,* $(, = 29)$*,* $(. = 30)$*, etcétera.*

Ahora escribimos en base dos estos números utilizando n *lugares:*

$$\begin{array}{cc} a = 0 = 0\ldots000000 & b = 1 = 0\ldots000001 \\ c = 2 = 0\ldots000010 & \cdots \\ \cdots & z = 27 = 0\ldots0011011 \\ \cdots & \cdots \end{array}$$

Este sistema nos permite codificar cualquier texto escrito en nuestro idioma como una sucesión de ceros y unos. Por ejemplo usando $n = 6$ *nos da un total de* 64 *posibilidades, que son más que suficientes para numerar todas las letras y signos del castellano, tenemos que "En un lugar de la Mancha ..." empezaría así:*

000100001110011100010110011100011100001011010110000011000000001001*1*

Todo el Quijote sería pues una sucesión, enorme pero finita, de ceros y unos que, según hemos demostrado, encontraríamos en el desarrollo decimal de β*. Podemos pues escribir un programa de descodificación de* β*, haciendo que el ordenador vaya transcribiendo cada bloque de siete dígitos consecutivos en su signo ortográfico correspondiente. Al principio seguramente encontraremos textos ininteligibles pero, ¡si esperamos suficiente tiempo!, habrá un momento en el que el ordenador empezará a escribir aquello de "En un lugar de la Mancha ..." y seguirá el Quijote completo.*

¡Magnífico! Ese número β, elegido al azar, es, con toda probabilidad, la biblioteca de Babel ensoñada por Jorge Luis Borges. ¡Toda la información está contenida en β, pero hay que tener una paciencia infinita, y un tiempo inmenso, para sacarla! ¡La información está allí pero no nos sirve de nada!

> *El universo (que otros llaman la Biblioteca) se compone de un número indefinido, y tal vez infinito, de galerías hexagonales, con vastos pozos de ventilación en el medio, cercados por barandas bajísimas...*
>
> *...Hace quinientos años, el jefe de un hexágono superior dio con un libro tan confuso como los otros, pero que tenía casi dos líneas homogéneas. Mostró su hallazgo a un descifrador ambulante, que le dijo que estaban redactadas en portugués; otros le dijeron que en yiddish. Antes de un siglo pudo establecerse el idioma: un dialecto samoyedo–lituano del guaraní, con inflexiones de árabe clásico. También se descifró el contenido: nociones de análisis combinatorio, ilustradas por ejemplos de variaciones con repetición ilimitada. Estos ejemplos permitieron que un bibliotecario de genio descubriera la ley fundamental de la Biblioteca. Este pensador observó que todos los libros, por diversos que sean, constan de elementos iguales: el espacio, el punto, la coma, las veintidós letras del alfabeto. También alegó un hecho que todos los viajeros han confirmado: No hay, en la vasta Biblioteca, dos libros idénticos. De esas premisas incontrovertibles dedujo que la Biblioteca es total y que sus anaqueles registran todas las posibles combinaciones de los veintitantos símbolos ortográficos o sea todo lo que es dable expresar: en todos los idiomas. Todo: la historia minuciosa del porvenir, las autobiografías de los arcángeles, el catálogo fiel de la Biblioteca, miles y miles de catálogos, la demostración de la falacia del catálogo verdadero, el evangelio gnóstico de Basílides, el comentario de ese evangelio, la relación verídica de tu muerte, la versión de cada libro a todas las lenguas, las interpolaciones de cada libro en todos los libros...*
>
> Jorge Luis Borges
>
> ("La biblioteca de Babel")

Volviendo a la Aritmética, los resultados anteriores tienen diversas prolongaciones en teorías sumamente interesantes. Por ejemplo, con la notación usual $x = [x] + (x)$ ="parte entera"+"parte fraccionaria", el desarrollo decimal (en base 10) admite la interpretación siguiente.

$$\begin{aligned}(x) &= 0{,}x_1x_2\ldots\\ x_1 &= \big[10(x)\big]\\ x_2 &= \big[10\big(10(x)\big)\big]\\ &\ldots\end{aligned}$$

Es decir la k–ésima cifra decimal x_k se obtiene de x por la siguiente regla:

1. *Se halla la parte fraccionaria y el resultado se multiplica por diez: $T\,x = 10(x)$.*
2. *Se itera el procedimiento anterior k veces y al resultado se le calcula la parte entera: $x_k = \big[T^k\,x\big]$.*

Si asociamos k con un tiempo discreto, el proceso anterior es un sistema dinámico que tiene características parecidas con otros relevantes en contextos muy distintos tales como algunos de la teoría cinética de los gases y de la mecánica estadística. Un resultado profundo de estas teorías dinámicas es el llamado teorema ergódico que aplicado a nuestro ejemplo permite concluir lo siguiente:

> *Para casi todos los números $x \in [0,1)$, $x = 0{,}x_1x_2x_3\ldots$, es decir si exceptuamos un subconjunto de medida cero, se verifica que:*
>
> $$\lim_{n\to\infty} \frac{card\{x_j \mid x_j = a,\ 1 \le j \le n\}}{n} = \frac{1}{10},$$
>
> *para todo dígito $a = 0, 1, 2, 3, \ldots, 9$.*

Es decir, si elegimos un número al azar en el intervalo $[0,1)$ entonces, con probabilidad igual a 1, tendrá un desarrollo decimal equilibrado: las frecuencias con las que aparecen cada uno de los 10 dígitos son iguales a $\frac{1}{10}$. Esos números se llaman normales en base 10. Es fácil señalar a uno de ellos, por ejemplo el racional $x = 0,\overbrace{0123456789}$. Un caso menos obvio es el número de Chanpernowne:

$$0{,}12345678910111213\ldots$$

obtenido disponiendo uno detrás de otro a los números naturales en base 10. Otro es el número de Copeland-Erdös:

$$0{,}23571113171923\ldots$$

cuyas cifras decimales siguen la sucesión de los números primos.

En realidad los resultados de E. Borel demuestran que, salvo un conjunto de medida cero, los números reales del intervalo $[0,1)$ presentan en su desarrollo cualquier patrón, o sucesión finita de k dígitos, que prescribamos con la frecuencia $\frac{1}{10^k}$ que es la que le corresponde por su tamaño. A veces se llama normales a estos números y se designan a los anteriores como simplemente normales que es una condición menos restrictiva como muestra el número racional antes señalado $0,\overbrace{0123456789}$, que es simplemente normal pero no es normal en base 10.

Las nociones anteriores y los correspondientes teoremas de Borel son ciertos en cualquier base de numeración. Un resultado reciente obtenido por D. Bailey y R. Crandall afirma que la suma de la serie

$$\frac{1}{a \times b^a} + \frac{1}{a^2 \times b^{a^2}} + \frac{1}{a^3 \times b^{a^3}} + \ldots$$

es un número normal en base $b \ge 2$ siempre que m.c.d.$(a,b) = 1$.

Resulta fácil demostrar que ser normal en una base b es equivalente a ser simplemente normal en todas sus potencias, b^k, $k = 1, 2, 3, \ldots$ También lo es

probar que el conjunto de los números del intervalo $[0,1)$ *que son normales en todas las bases, llamados absolutamente normales, es de medida total, es decir, su complementario tiene probabilidad cero.*

En el año 1917 *el matemático polaco W. Sierpinski consiguió una demostración constructiva del teorema de Borel que le permitió señalar, o nombrar, a un número real concreto que es absolutamente normal. Recientemente, Verónica Becher y Santiago Figueira, de la Universidad de Buenos Aires, han mejorado la construcción de Sierpinski demostrando que su número absolutamente normal es computable, en el sentido de la sección siguiente, pero el algoritmo que obtienen para calcular sus cifras decimales es de tipo exponencial.*

En estos momentos todavía nos pondrían en un gran compromiso al pedirnos decidir si un número dado es o no absolutamente normal. Surge una pregunta que aparece enroscada en el poema de la premio Nobel W. Szymborska:

$$\text{¿Es } \pi \text{ un número normal?}$$

A la que podemos añadir: ¿Lo son e, $\sqrt{2}$, $\log 2$*?*

5.7. Números computables

Diremos que un número es computable si existe un programa de ordenador para calcular sus cifras decimales. De manera más precisa, un número real es computable si existe una función recursiva $f : \mathbb{N} \to \mathbb{N}$ *tal que* $f(n)$ *sea su enésima cifra decimal. La noción de función recursiva es sencilla, pero vamos a obviarla en esta sección por motivos de espacio, quedándonos con la idea intuitiva de programa de ordenador.*

Ejemplos de números computables son $1/3$, $\sqrt{2}$, π *y* e*. También todos los números racionales. Sin embargo hay muchos números, la mayoría, que no son computables porque, como nos muestra el siguiente teorema, los computables forman un conjunto de medida cero, por ser numerable.*

Teorema. *Los números computables forman un conjunto numerable.*

Demostración. *Cada programa de ordenador es un texto finito escrito en un alfabeto que contiene un número finito de símbolos o letras:* $\mathcal{A} = \{a_1, \ldots, a_N\}$.

$$\begin{array}{ll} \textit{Hay} & N \textit{ textos de una sola letra: } (a_1), \ldots, (a_N) \\ & N^2 \textit{ textos de dos letras: } (a_1a_1), (a_1a_2), \ldots, (a_Na_N) \\ & N^3 \textit{ textos de tres letras: } (a_1a_1a_1), (a_1a_1a_2), \ldots, (a_Na_Na_N) \\ & \qquad \cdots \\ & N^k \textit{ textos de } k \textit{ letras: } (a_{i_1}a_{i_2}\ldots a_{i_k}) \\ & \qquad \cdots \end{array}$$

La unión de todos ellos es por tanto un conjunto numerable.

Muchos de esos textos carecen de sentido y serán rechazados por el compilador. Entre los que sean aceptados hallaremos los programas que sirven para calcular las cifras decimales de los números computables. Podemos pues establecer una correspondencia biyectiva entre tales números y un subconjunto del conjunto numerable de textos, es decir: los números computables forman un conjunto numerable y, por tanto, de medida nula. ¡La mayoría de los números reales no son computables! ■

Pensemos en los textos (finitos) que podemos escribir en cualquier idioma conocido (arameo, hebreo, árabe, griego, latín, fortran, algol, java, lisp...) y que forman un conjunto numerable. La mayoría de ellos no tendrán que ver con los números, pero aquellos que nos sirvan para designar a un número real concreto formarán un subconjunto que también será numerable. Luego el conjunto de números reales que podemos nombrar en alguna lengua es siempre numerable. El resto, la mayoría, es innombrable. Están ahí, en la recta real, pero son auténticos parias a los que nunca podremos mencionar.

El concepto de número computable se debe a Alan Turing, quien lo introdujo en un artículo titulado "On computable number with an application to the Entscheidungsproblem" que publicó en el año 1936 *en los Proceedings of the London Mathematical Society. En estos tiempos estamos tan familiarizados con los ordenadores y sus lenguajes, algoritmos, programas que no es necesario hacer hincapié en un concepto tan natural como el de número computable. Pero ese no era el caso en el año* 1936*, por lo que Turing tuvo que concebir una máquina que pudiese realizar las operaciones lógicas requeridas en la definición de número computable.*

Una máquina de Turing Universal, que es una precursora ideal de un computador moderno, admite programas que consisten en sucesiones de bits en una de las dos posiciones 0 , 1*. Una vez que un programa ha sido reconocido por la máquina, esta empieza su proceso pudiendo ocurrir que en un número finito de pasos genere una respuesta. Pero también puede suceder lo contrario y que el proceso nunca se detenga. Es el famoso problema de "la parada" detectado por Turing, quien lo usó para dar otra demostración del teorema de incompletitud de Gödel (ver capítulo 8).*

Recientemente Gregory Chaitin ha profundizado en este flujo de ideas, algunas de las cuales tienen su origen en Leibniz, para introducir la noción de número algorítmicamente aleatorio *y de complejidad algorítmica. Sabemos que un programa consta de una sucesión finita de bits, pero puede ocurrir que un mismo cálculo u operación, el "output" del programa, pueda ser codificado de diversas maneras originando sucesiones distintas de ceros y unos. Podemos asignar a cada "output" el número mínimo de bits que son necesarios y suficientes para obtenerlo. Este número mide la complejidad del algoritmo o programa y nos permite introducir la noción de programa elegante, o eficiente, si minimiza la complejidad entre los que producen el mismo resultado.*

Siguiendo a Chaitin diremos que un número real $x = 0{,}x_1x_2x_3\ldots$ es algorítmicamente aleatorio si existe una constante $c(x)$ tal que para cada natural n, cualquier programa que calcule la enésima cifra decimal de x ha de tener por lo menos $n - c(x)$ bits.

Chaitin ha estudiado las propiedades de estos números algorítmicamente aleatorios y ha demostrado que son absolutamente normales, es decir, normales en todas las bases de numeración. Un ejemplo es el número de Chaitin de una máquina Universal de Turing

$$\Omega = \sum 2^{-\text{número de bits del programa } \mathcal{P}}$$

obtenido sumando, sobre todos los programas elegantes $\mathcal{P}$, la probabilidad de haberlos obtenido al azar en lanzamientos independientes de una moneda bien hecha, es decir, que tenga igual probabilidad, $\frac{1}{2}$, de obtener cara (bit= 0) o cruz (bit= 1). En otras palabras, dada una máquina Universal de Turing imaginemos contenidos en una gran caja a todos lo programas que se paran en un número finito de operaciones. Supongamos también codificados en forma de sucesiones finitas de los dos dígitos binarios, 0, 1, de manera eficiente o elegante. El número Ω describe la probabilidad de que, lanzando al azar una moneda, acabemos generando un programa de la caja en un número finito de tiradas. Ω es definible o nombrable, pero Chaitin ha demostrado que no es computable y, aunque sabemos que es absolutamente normal, solo conocemos un número finito de sus cifras decimales.

Ejercicios

1) *Sea $x \in \mathbb{R}$, $x > 0$. Demostrar que existe $q \in \mathbb{Q}$ tal que $0 < q < x$.*

2) *Demostrar que cada número real positivo tiene una única raíz cuadrada positiva.*

3) *Demostrar que en cada base de numeración b, los decimales que sean periódicos desde algún lugar en adelante, corresponden a los números racionales.*

4) *Demostrar que $\mathcal{P}(\mathbb{N})$ es equipotente con $\mathbb{R}$.*

Sugerencia: sean $f : [0,1) \longrightarrow \mathcal{P}(\mathbb{N})$, dada por $f(x) = \{a_j 10^j \mid j \geq 1\}$ si x tiene desarrollo decimal $0{,}a_1a_2\ldots$; y $g : \mathcal{P}(\mathbb{N}) \longrightarrow [0,1)$ dada por $g(X) = 0{,}a_1a_2\ldots$ siendo

$$a_j = \begin{cases} 0 & \text{si } j \notin X \\ 1 & \text{si } j \in X \end{cases} .$$

Demostrar que ambas, f y g, son inyectivas.

5) *Demostrar que el conjunto de todos los polinomios con coeficientes enteros es numerable. Deducir que el conjunto de todos los números reales que son raíces de polinomios es numerable. ¿Qué puede decirse del conjunto de todos los números reales que no son raíz de ningún polinomio?*

6) *Probar que el conjunto de todos los subconjuntos finitos de* $\mathbb{N}$ *es numerable. Deducir que el conjunto de los subconjuntos infinitos de* $\mathbb{N}$ *no es numerable.*

7) *¿Existe un conjunto* X *tal que* $\mathcal{P}(X)$ *sea infinito y numerable?*

8) *Demostrar que si* $\text{card}(A) \leq \text{card}(B)$ *entonces* $\text{card}(\mathcal{P}(A)) \leq \text{card}(\mathcal{P}(B))$. *Demostrar que si* A *y* B *son equipotentes, entonces también lo son* $\mathcal{P}(A)$ *y* $\mathcal{P}(B)$.

9) *Demostrar que el conjunto de las líneas rectas del plano es equipotente con* $\mathbb{R}$.

10) *Demostrar que el conjunto de todos las sucesiones infinitas de elementos de* $\mathbb{R}$ *es equipotente con* $\mathbb{R}$.

6

Los números complejos

El camino más corto entre dos verdades reales pasa por lo imaginario.

Jacques Hadamard

A pesar de su nombre, la construcción del cuerpo $\mathbb{C}$ de los números complejos a partir de los reales, $\mathbb{R}$, es mucho más sencilla que la de estos sobre los racionales. Como conjunto $\mathbb{C}$ es simplemente $\mathbb{R}\times\mathbb{R}$, el producto cartesiano de los reales por sí mismos. Es decir, un número complejo es un par ordenado de números reales. No obstante, para que $\mathbb{R}\times\mathbb{R}$ adquiera la categoría de cuerpo de números es menester saber sumarlos y multiplicarlos apropiadamente.

Definición. *Sean (a_j, b_j), $j = 1, 2$, elementos de $\mathbb{R}\times\mathbb{R}$. Se definen las operaciones siguientes:*

1. *Suma:* $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$;
2. *Producto:* $(a_1, b_1) \times (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.

Ejercicio 1. *Demostrar las propiedades siguientes de la suma y el producto de números complejos.*

1. *Asociativa (suma y producto).*
2. *Conmutativa (suma y producto).*
3. *Distributiva del producto respecto de la suma.*
4. *Existencia de elemento neutro para la suma:* $(0, 0)$.
5. *Existencia de elemento neutro para el producto:* $(1, 0)$.
6. *Elemento opuesto para la suma:* $(a, b) + (-a, -b) = (0, 0)$.
7. *Elemento inverso para el producto. Si* $(a, b) \neq (0, 0)$, *entonces:*

$$(a, b) \times \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0).$$

Estas propiedades se resumen en la frase siguiente: el conjunto $\mathbb{C}$, dotado de la suma y el producto antes definidos, es un cuerpo.

Observemos que la aplicación $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$, definida por

$$x \longmapsto \varphi(x) = (x, 0),$$

conserva la suma y el producto:

$$\varphi(x + y) = \varphi(x) + \varphi(y)\,, \qquad \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Luego nos permite identificar a los números reales, $\mathbb{R}$, con un subcuerpo de los complejos:

$$0 = (0, 0)\,, \quad 1 = (1, 0)\,, \quad -1 = (-1, 0)\,, \quad \textit{etcétera.}$$

Observemos que

$$(0, 1)^2 = (0, 1) \times (0, 1) = (-1, 0) = -1,$$

es decir, el número complejo $(0, 1)$, que se designará por el símbolo i (la unidad imaginaria), verifica la ecuación $i^2 = -1$: "es una raíz cuadrada de -1", la otra es $-i = (0, -1)$.

Tomando como base de $\mathbb{R} \times \mathbb{R}$ los vectores $1 = (1, 0)$, $i = (0, 1)$, encontramos la expresión típica de un número complejo, $z = x + iy$, $x, y \in \mathbb{R}$, donde:

$$x = \mathrm{Re}(z) = \textit{ parte real}$$
$$y = \mathrm{Im}(z) = \textit{ parte imaginaria.}$$

6.1. Representación polar

En $\mathbb{C}$ tenemos las coordenadas polares. Todo número, $z = x + iy$, queda determinado por su módulo, $r = |z| = \sqrt{x^2 + y^2}$, o distancia del punto (x, y) al origen $(0, 0)$ de $\mathbb{R} \times \mathbb{R}$, y por su argumento, el ángulo θ que el vector (x, y) determina con el eje OX: $x = r \cos\theta$, $y = r \operatorname{sen}\theta$, es decir:

$$z = x + iy \implies z = r(\cos\theta + i \operatorname{sen}\theta), \quad (r = \sqrt{x^2 + y^2}).$$

El origen, $(0, 0)$, queda fuera de esta discusión.

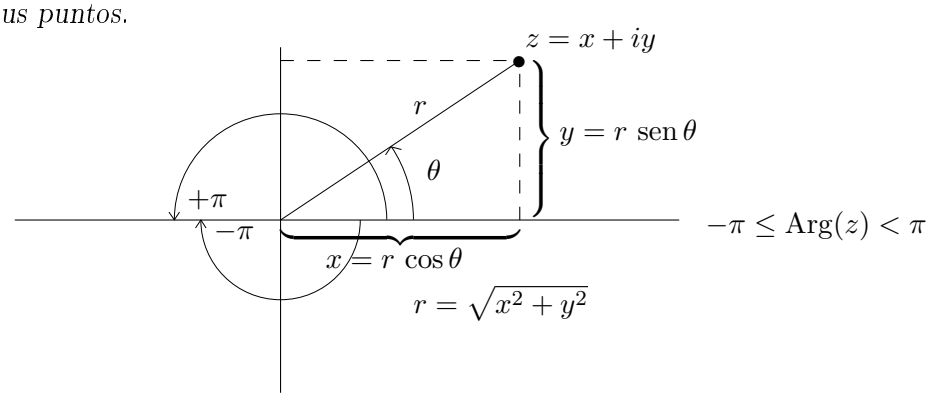
No obstante, las coordenadas x, y, no determinan unívocamente el ángulo θ, puesto que $\cos(\theta + 2k\pi) = \cos\theta$ y $\operatorname{sen}(\theta + 2k\pi) = \operatorname{sen}\theta$, para cualquier entero k. Es decir, a un número complejo, z, le podemos asociar una familia numerable de ángulos, o argumentos, de manera que dos cualesquiera de ellos difieran entre sí en un múltiplo entero de 2π.

Una manera de describir esta situación es la siguiente: en $\mathbb{R}$ *establecemos la relación*

$$x \sim y \Longleftrightarrow \exists k \in \mathbb{Z},\ x - y = 2k\pi.$$

Es fácil ver que $\sim$ *satisface las propiedades reflexiva, simétrica y transitiva. Tenemos, por lo tanto, una relación de equivalencia que divide a* $\mathbb{R}$ *en clases disjuntas de equivalencia:* $[\theta]$. *Pues bien el argumento del número complejo* z *será una de estas clases, y las coordenadas polares asocian a cada* $z \neq 0$ *un módulo,* $|z| > 0$, *y un argumento,* $[\theta]$, *de manera unívoca.*

A veces, no obstante, es conveniente hacer una elección adecuada de representantes del argumento para los números complejos de una región del plano $\mathbb{C}$. *Una estrategia usual consiste en fijar un intervalo de longitud* 2π, $[a, a + 2\pi)$, *y exigir que el representante del argumento pertenezca a él:* $a \leq \theta < a + 2\pi$. *Un ejemplo es* $[-\pi, \pi)$, $a = -\pi$, *que suele llamarse argumento principal de* z, $\operatorname{Arg}(z)$. *Obsérvese que* $\operatorname{Arg}(z)$ *es una función continua en el plano* $\mathbb{C}$ *menos el eje real negativo:* $\mathbb{C}\backslash(-\infty, 0]$. *Precisamente en* $(-\infty, 0]$ *se da un salto de* 2π *en* $\operatorname{Arg}(z)$, *que presenta una discontinuidad en todos sus puntos.*



La representación polar resulta especialmente adecuada para analizar el producto. Dados

$$z = r(\cos\theta + i\operatorname{sen}\theta), \quad \omega = s(\cos\varphi + i\operatorname{sen}\varphi),$$

tenemos que:

$$\begin{aligned} z \cdot \omega &= rs\big((\cos\theta\cos\varphi - \operatorname{sen}\theta\operatorname{sen}\varphi) + i(\cos\theta\operatorname{sen}\varphi + \operatorname{sen}\theta\cos\varphi)\big) \\ &= rs\big[\cos(\theta + \varphi) + i\operatorname{sen}(\theta + \varphi)\big]. \end{aligned}$$

Es decir, el módulo del producto es el producto de los módulos ($|z \cdot \omega| = |z| \cdot |\omega|$), *mientras que el argumento es la suma de los correspondientes argumentos.*

La regla anterior se traduce en la siguiente fórmula para las potencias de un número complejo: si $z = |z|\,(\cos\theta + i\operatorname{sen}\theta)$, *entonces:*

$$z^n = |z|^n\,\big(\cos(n\theta) + i\operatorname{sen}(n\theta)\big).$$

6.2. Raíces

Supongamos que queremos resolver la ecuación $z^n = \omega$, *siendo*

$$\omega = |\,\omega|(\cos\theta + i\,\mathrm{sen}\,\theta).$$

Si $z = |z|\,(\cos\varphi + i\,\mathrm{sen}\,\varphi)$, *tendremos que*

$$z^n = |z|^n\,\big(\cos(n\varphi) + i\,\mathrm{sen}(n\varphi)\big) = |\,\omega|(\cos\theta + i\,\mathrm{sen}\,\theta)$$

da lugar a las igualdades:

* $|z| = |\,\omega|^{1/n}$, *raíz enésima positiva del número real positivo* $|\,\omega|$.

** $n\,\varphi = \theta + 2k\pi$, $k \in \mathbb{Z}$; *equivalentemente:*

$$\varphi = \frac{\theta}{n} + \frac{2k\pi}{n}, \quad k \in \mathbb{Z}.$$

Ahora bien, los infinitos ángulos $\theta/n + 2k\pi/n$ *se distribuyen en* n *clases de equivalencia respecto a la relación* $\sim$ *que definía los argumentos. Sea* $k = cn + r$, $0 \le r \le n-1$, *el resultado de la división de* k *por* n. *Entonces:*

$$\frac{\theta}{n} + \frac{2k\pi}{n} = \frac{\theta}{n} + 2\pi c + \frac{2r\pi}{n} \sim \frac{\theta}{n} + \frac{2r\pi}{n}.$$

Luego los ángulos:

$$\theta_r = \frac{\theta}{n} + \frac{2r\pi}{n}, \quad r = 0, 1, 2, \ldots, n-1$$

son representantes de los argumentos de las n *raíces enésimas del número* ω*:*

$$\left\{\begin{array}{rcl} z_1 & = & |\,\omega|^{1/n}\Big(\cos\Big(\dfrac{\theta}{n}\Big) + i\,\mathrm{sen}\,\Big(\dfrac{\theta}{n}\Big)\Big) \\ z_2 & = & |\,\omega|^{1/n}\Big(\cos\Big(\dfrac{\theta}{n} + \dfrac{2\pi}{n}\Big) + i\,\mathrm{sen}\,\Big(\dfrac{\theta}{n} + \dfrac{2\pi}{n}\Big)\Big) \\ \vdots & \vdots & \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z_n & = & |\,\omega|^{1/n}\Big(\cos\Big(\dfrac{\theta}{n} + \dfrac{2(n-1)\pi}{n}\Big) + i\,\mathrm{sen}\,\Big(\dfrac{\theta}{n} + \dfrac{2(n-1)\pi}{n}\Big)\Big) \end{array}\right.$$

Obsérvese que los ángulos $\theta/n + 2r\pi/n$, $0 \le r \le n-1$ *están simétricamente distribuidos en la circunferencia unidad (circunferencia goniométrica).*

***Ejemplos: a) Raíces cuadradas de* i:** *Se tiene que* $|i| = 1$, *y* $\arg(i) = [\pi/2]$, *luego sus raíces cuadradas son:*

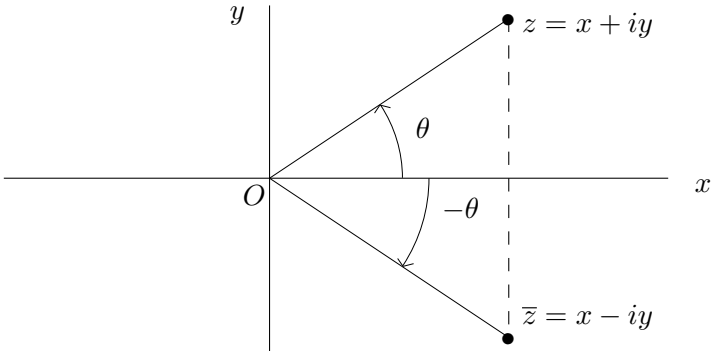
$$z_1 = \cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4} = \frac{\sqrt{2}}{2}\,(1+i)$$

$$z_2 = \cos\Big(\frac{\pi}{4} + \frac{2\pi}{2}\Big) + i\,\mathrm{sen}\,\Big(\frac{\pi}{4} + \frac{2\pi}{2}\Big) = -\frac{\sqrt{2}}{2}\,(1+i).$$

b) Raíces cúbicas de 2: *Tenemos que* $|2| = 2$, *y* $\arg(2) = [0]$, *de donde sus tres raíces cúbicas son:*

$$z_1 = 2^{1/3}\Big[\cos\frac{0}{3} + i\,\mathrm{sen}\,\frac{0}{3}\Big] = 2^{1/3}$$
$$z_2 = 2^{1/3}\Big[\cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}\Big] = 2^{1/3}\Big[-\frac{1}{2} + \frac{\sqrt{3}}{2}i\Big]$$
$$z_3 = 2^{1/3}\Big[\cos\frac{4\pi}{3} + i\,\mathrm{sen}\,\frac{4\pi}{3}\Big] = 2^{1/3}\Big[-\frac{1}{2} - \frac{\sqrt{3}}{2}i\Big]$$

Definición. *El conjugado del número* $z = x + iy$ *es* $\overline{z} = x - iy$. *Geométricamente,* $\overline{z}$ *se obtiene de* z *por medio de una reflexión en el eje real.*



En coordenadas polares,

$$|\overline{z}| = |z| = \sqrt{x^2 + y^2}\,,$$

mientras que

$$\arg(\overline{z}\,) = -\arg(z).$$

La operación de conjugar, $z \longmapsto \overline{z}$, *es involutiva, ya que:* $\overline{\overline{z}} = z$.

Ejercicios

1) *Demostrar las desigualdades:*

$$\big|\,|z| - |\,\omega|\big| \le |\,z - \omega\,| \le |z| + |\,\omega|.$$

2) *Calcular* $\arg(z)$ *en los casos:*

$$z = \frac{2}{1 - i\sqrt{3}}\;; \quad z = \big(\sqrt{3} - i\big)^6.$$

3) *Sea* $r > 0$ *una constante. Demostrar que la ecuación de la circunferencia de radio* r *centrada en un punto* ω *es:*

$$|z|^2 - 2\mathrm{Re}(z\overline{\omega}) + |\,\omega|^2 = r^2.$$

4) *Calcular las raíces de la ecuación* $z^4 + 16 = 0$.

5) *Deducir la identidad:*

$$1 + z + z^2 + \cdots + z^n \;=\; \frac{1 - z^{n+1}}{1 - z}$$

cuando z *es un número complejo,* $z \neq 1$. *Demostrar la identidad:*

$$\frac{1}{2} + \cos\theta + \cdots + \cos(n\theta) \;=\; \frac{\operatorname{sen}\big((n + 1/2)\theta\big)}{2\operatorname{sen}(\theta/2)}, \quad 0 < \theta < 2\pi.$$

6) *Calcular las raíces quintas de la unidad.*

7) *Demostrar que* z *es real si y solo si* $z = \overline{z}$.

8) *Dados dos números complejos* z, w, *demostrar las identidades siguientes:*

$$\begin{aligned} |z + w|^2 &= |z|^2 + 2\mathrm{Re}(z \cdot \overline{w}) + |w|^2; \\ |z - w|^2 &= |z|^2 - 2\mathrm{Re}(z \cdot \overline{w}) + |w|^2; \\ |z + w|^2 + |z - w|^2 &= 2(|z|^2 + |w|^2). \end{aligned}$$

Interpretar geométricamente la tercera de ellas.

9) *Demostrar por inducción que si* $z = z_1 + z_2 + \cdots + z_n$, $w = w_1 \cdot w_2 \cdots w_n$ *entonces:*

$$\overline{z} = \overline{z}_1 + \overline{z}_2 + \cdots + \overline{z}_n, \qquad \overline{w} = \overline{w}_1 \cdot \overline{w}_2 \cdots \overline{w}_n$$

6.3. Convergencia

Recordemos que el principal motivo para construir los números reales fue completar el conjunto $\mathbb{Q}$ *de los racionales, de manera que las sucesiones de Cauchy tuvieran siempre límite en* $\mathbb{R}$. *Al extender* $\mathbb{R}$ *al cuerpo complejo,* $\mathbb{C}$, *es importante no haber perdido ese carácter de completitud.*

Revisemos, en este contexto, los conceptos de límite de una sucesión y de sucesión de Cauchy.

Definición. *Dada una sucesión* $\{z_n\}$ *de números complejos, se dice que*

$$z = \lim_{n\to\infty} z_n$$

si para todo real $\varepsilon > 0$, *existe un natural,* $n = n(\varepsilon)$, *tal que* $|\, z - z_n \,| < \varepsilon$ *siempre que* $k \geq n$.

Definición. *Una sucesión,* $\{z_n\}$, *de números complejos es de Cauchy si para todo real* $\varepsilon > 0$, *existe un índice,* $n = n(\varepsilon)$, *tal que* $|\, z_k - z_j \,| < \varepsilon$ *siempre que* $\min\{k, j\} \geq n$.

Se trata de la extensión natural de la noción de sucesión de Cauchy de números reales. Sea $z_n = x_n + iy_n$, *tenemos que:*

$$\begin{aligned} \text{máx}\left\{|\,x_k - x_j\,|, |\,y_k - y_j\,|\right\} &\leq \sqrt{|\,x_k - x_j\,|^2 + |\,y_k - y_j\,|^2} \\ &\leq |\,x_k - x_j\,| + |\,y_k - y_j\,| \\ &\leq 2\ \text{máx}\left\{|\,x_k - x_j\,|, |\,y_k - y_j\,|\right\} \end{aligned}$$

Estas desigualdades nos permiten demostrar que la sucesión $\{x_n + iy_n\}$ *es de Cauchy en* $\mathbb{C}$, *si y solo si las dos sucesiones* $\{x_n\}$, $\{y_n\}$ *son de Cauchy en* $\mathbb{R}$. *Además, si* $x = \lim_{n\to\infty} x_n$ *e* $y = \lim_{n\to\infty} y_n$, *entonces*

$$\lim_{n\to\infty}(x_n + iy_n) = x + iy.$$

Luego el cuerpo de números $\mathbb{C}$ *es también completo: "toda sucesión de Cauchy en* $\mathbb{C}$ *tiene límite en* $\mathbb{C}$".

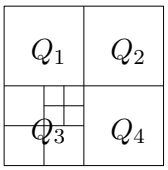
Una propiedad importante de compacidad es la siguiente que poseen las sucesiones acotadas en $\mathbb{C}$. *Es decir, sucesiones,* $\{z_n\}$, *tales que existe* $R > 0$ *verificando:*

$$|\,z_n\,| \leq R, \quad \forall n.$$

Proposición. *De toda sucesión acotada de números complejos,* $\{z_n\}$, *podemos extraer una subsucesión convergente.*

Demostración. *Observemos que la condición de estar acotada es necesaria, como muestra el ejemplo* $z_n = n$, *ya que no hay subsucesión convergente de* $\{n\}$.

La hipótesis de acotación nos permite suponer que hay un cuadrado, Q, *que contiene a la sucesión* $\{z_n\}$. *Empezamos eligiendo* $\omega_1 = z_1$. *A continuación dividimos el cuadrado* Q *en cuatro cuadrados de igual tamaño demediando sus lados:* $Q = Q_1 \cup Q_2 \cup Q_3 \cup Q_4$ *(ver la figura). Obsérvese que uno de ellos, al menos, ha de contener infinitos términos de la sucesión. Sea este* Q_j, *entonces elegimos* $\omega_2 = z_{\nu_2}$ *con el criterio de que* $\nu_2 > 1$ *y* $\omega_2 = z_{\nu_2} \in Q_j$.



Ahora volvemos a dividir Q_j *en cuatro cuadrados iguales,* $Q = Q_{j,1} \cup Q_{j,2} \cup Q_{j,3} \cup Q_{j,4}$, *y nos quedamos con uno de ellos,* $Q_{j,k}$, *que contenga infinitos términos de la sucesión* $\{z_n\}$. *Luego escogemos* $\omega_3 = z_{\nu_3} \in Q_{j,k}$ *de manera que* $\nu_3 > \nu_2 > 1$, *y así sucesivamente.*

Es claro que la sucesión $\{\omega_k\}$ *es una subsucesión de Cauchy de* $\{z_n\}$ *ya que*

$$|\,\omega_k - \omega_j\,| \leq \frac{\text{diámetro de } Q}{2^{\text{mín}\{k,j\}}},$$

es tan pequeño como queramos si $\text{mín}\{k, j\}$ *es suficientemente grande.* ■

6.4. Funciones complejas

Las funciones, $\omega = f(z)$, cuyo dominio es un subconjunto $\Omega \subset \mathbb{C}$ y cuyo rango es $\mathbb{C}$ se llaman, naturalmente, funciones complejas de la variable compleja z. Ejemplos: $f(z) = z$; $f(z) = z^2$; $f(z) = 2z + iz^2 - \sqrt{2}$.

En general, si tenemos una función real, f, de la variable real x, dada por una expresión que involucre sumas, productos, divisiones, potencias, ..., podremos "extenderla" a un dominio mayor, dentro de los números complejos. Los dos primeros ejemplos anteriores son extensiones, respectivamente, de las funciones $f(x) = x$ y $f(x) = x^2$ de $\mathbb{R}$ en $\mathbb{R}$.

Un caso particular, importante, es cuando la función f es una serie de potencias convergente; por ejemplo:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \ldots$$

es la función exponencial. Cualquiera que sea el número real x, resulta que la sucesión:

$$y_n = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$$

es de Cauchy. Su límite, e^x, es el valor de la función exponencial de x. Ahora bien, la sucesión de números complejos:

$$\omega_n = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots + \frac{z^n}{n!}$$

también es de Cauchy en $\mathbb{C}$, luego tendrá un límite al que llamaremos e^z:

$$e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots + \frac{z^n}{n!} + \ldots$$

Un análisis similar nos permite obtener el seno y el coseno complejos:

$$\operatorname{sen} z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \ldots$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \ldots$$

En particular, si tomamos $z = ix$ puramente imaginario (x real), obtenemos:

$$e^{ix} = 1 + \frac{ix}{1!} - \frac{x^2}{2!} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} - \frac{x^6}{6!} - \frac{ix^7}{7!} + \ldots,$$

que podremos también escribir como:

$$\begin{aligned} e^{ix} &= \Big(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \ldots\Big) + i\Big(\frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots\Big) \\ &= \cos(x) + i\operatorname{sen}(x), \end{aligned}$$

que es una famosa fórmula de Euler. Sustituyendo $x = \pi$ *obtenemos:*

$$e^{i\pi} + 1 = 0\,,$$

identidad de la que Euler se sentía orgulloso, y que relaciona a los cinco números más importantes de las Matemáticas.

El logaritmo complejo. *Entre los números reales calcular logaritmos, naturales o en base* e*, es la operación inversa de la exponencial:*

$$y = \log x \iff x = e^y.$$

Esto se debe a que la exponencial $t = e^s$ *es una biyección entre la recta real,* $-\infty < s < +\infty$*, y la semirrecta positiva,* $t > 0$*. Pero entre los complejos, la exponencial deja de ser inyectiva, ya que* $e^{z+2\pi ni} = e^z$*,* $\forall n \in \mathbb{Z}$*, por lo que tenemos que complicar ligeramente nuestra estrategia.*

Dado $z = x + iy$ *en coordenadas polares*

$$z = |z|\, e^{i\theta}\,, \quad |z| = \sqrt{x^2 + y^2}\,, \quad \theta \in \arg(z) = \left[\arctan\frac{y}{x}\right]$$

planteémonos resolver la ecuación: $z = e^w$*.*

Sea $w = u + iv$*, entonces*

$$e^w = e^u \cdot e^{iv} = e^u\{\cos v + i \operatorname{sen} v\}.$$

Luego si queremos obtener $z = e^w$ *resulta que* $e^u = |z|$ *y* $v \in \arg(z)$*.*

Es decir, la parte real u *de* $w = \log z$ *está unívocamente determinada y vale* $u = \log|z|$ *(siendo* $\log|z|$ *el logaritmo de los números reales), pero para la parte imaginaria tenemos una multiplicidad de elección, una por cada argumento del número complejo* z*.*

Fijado el número real a*, cada complejo* z *tiene un miembro de su argumento* $\arg_a(z)$ *que satisface:* $a \le \arg_a(z) < a + 2\pi$*.*

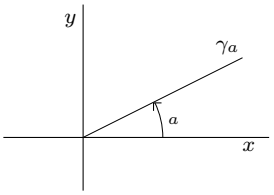
Esa elección se corresponde con una "rama" del logaritmo:

$$\log z = \log|z| + i\ \arg_a(z).$$

Si al plano $\mathbb{C}$ *le quitamos la semirrecta*

$$\gamma_a = \big\{r(\cos a, \operatorname{sen} a) \mid 0 \le r < \infty\big\},$$

la función $w = \log z$ *es continua en el resto* $(\mathbb{C} \setminus \gamma_a)$*, pero observemos que en los puntos de la semirrecta* γ_a *la parte imaginaria de* $\log z$ *tiene un salto de altura* 2π*.*

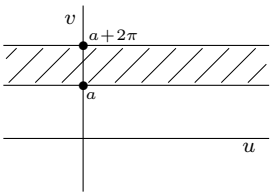


La imagen de $\mathbb{C} \setminus \gamma_a$ *por medio de la función*

$$\log z = \log|z| + i \arg_a(z)$$

es la franda horizontal

$$E_a = \{u + iv \mid a < v < a + 2\pi\}.$$



Recíprocamente: la exponencial, $z = e^w$*, es una aplicación biyectiva entre la franja* E_a *y el plano "cortado" por la semirrecta,* $C \setminus \gamma_a$*.*

Cuando γ_a *es el semieje real negativo y* $a = -\pi$*, se suele decir que tenemos la "rama principal" del logaritmo, que resulta especialmente apropiada cuando la acción transcurre fuera de ese semieje real negativo. En esta rama principal, el logaritmo de un número real positivo coincide satisfactoriamente con el logaritmo definido entre los reales.*

La función Gamma

Se trata de la función que extiende al dominio de los números complejos la noción de factorial de un número entero positivo: $n! = 1 \times 2 \times 3 \times \cdots \times n$*. Aunque la notación* $\Gamma(z)$ *se debe a Legendre, fue Euler quien pensó primero en esta función.*

Si $z = x + iz$ *es un número complejo de parte real positiva,* $x > 0$*, entonces la integral*

$$\Gamma(z) = \int_0^\infty t^{z-1}\, e^{-t}\, \mathrm{d}\, t \tag{6.1}$$

converge absolutamente ya que $|t^{z-1}| = t^{x-1}$*.*

Una sencilla integración por partes nos da la ecuación

$$\Gamma(z+1) = z\,\Gamma(z). \tag{6.2}$$

Habida cuenta de que $\Gamma(1) = \displaystyle\int_0^\infty e^{-t}\, \mathrm{d}\, t = 1$*, de (6.2) obtenemos la identidad*

$$\Gamma(n+1) = n!\,. \tag{6.3}$$

La fórmula (6.1) define pues a una función en el semiplano $\mathrm{Re}\, z > 0$*. Utilizando (6.2) obtenemos* $\Gamma(z) = \frac{\Gamma(z+1)}{z}$ *que nos da el valor de* Γ *cuando* $z \neq 0$ *y* $\mathrm{Re}(z) > -1$*. Iterando el proceso anterior conseguimos definir* Γ *en todos los complejos salvo en el conjunto* $\{0, -1, -2, -3, \ldots\}$*.*

La función Γ *desempeña un papel importante en muchas teorías y tiene propiedades analíticas muy interesantes. No es este el lugar adecuado para analizarlas en detalle pero sí podemos señalar algunas con el propósito de estimular la curiosidad del lector:*

a) $\Gamma(z) = \lim_{n\to\infty} \dfrac{n!\, n^z}{z(z+1)\cdots(z+n)}$

b) $\Gamma(1-z)\Gamma(z) = \dfrac{\pi}{\operatorname{sen}(\pi z)}$

c) $\Gamma(z) = \dfrac{e^{-\gamma z}}{z} \prod_{n=1}^{\infty} \left(1+\dfrac{z}{n}\right)^{-1} e^{\frac{z}{n}}$ *donde*

$$\gamma = \lim_{k\to\infty} \left(1 + \frac{1}{2} + \ldots + \frac{1}{k} - \log k\right) = 0{,}5772156649\ldots$$

es la constante de Euler–Mascheroni.

Ejercicio 2. *Calcular los valores siguientes de la función* Γ*:*

$$\Gamma\left(\tfrac{1}{2}\right), \quad \Gamma\left(\tfrac{-3}{2}\right), \quad \Gamma\left(\tfrac{3}{4}\right).$$

La función Zeta de Riemann: $\zeta(s)$

Es una de las funciones más interesantes de las Matemáticas y fue introducida también por L. Euler en el caso de argumento s real y luego extendida al dominio de los complejos por B. Riemann.

En el semiplano $s = \sigma + i\tau$, $\sigma > 1$, *tiene la siguiente definición:*

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

En capítulos anteriores analizamos la suma de los recíprocos de los cuadrados:

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

que es un caso particular de la identidad obtenida por Euler:

$$\zeta(2n) = (-1)^{n+1} \frac{\mathrm{B}_{2n}}{2\,(2n)!}\,(2\pi)^{2n}$$

donde los números racionales de Bernoulli B_k *están dados por la fórmula:*

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{\mathrm{B}_n}{n!}\, x^n,$$

válida para valores de x próximos a 0. En particular:

$$\mathrm{B}_0 = 1\,, \quad \mathrm{B}_1 = -\tfrac{1}{2}\,, \quad \mathrm{B}_2 = \tfrac{1}{6}\,, \quad \mathrm{B}_3 = 0\,, \quad \mathrm{B}_4 = -\tfrac{1}{30}\,,$$
$$\mathrm{B}_5 = 0\,, \quad \mathrm{B}_6 = \tfrac{1}{42}\,, \quad \mathrm{B}_7 = 0\,, \quad \mathrm{B}_8 = -\tfrac{1}{30}\,, \quad \mathrm{B}_9 = 0\,,\ldots$$

$\zeta(s)$ no está definida en $s = 1$, por ser la serie armónica divergente $\sum \frac{1}{n} = \infty$, y la naturaleza de los números $\zeta(2k+1)$, $k = 1, 2, 3 \ldots$, es todavía "terra incógnita", aunque desde el año 1978 sabemos con R. Apéry que $\zeta(3) = 1{,}20205690\ldots$ es un número irracional.

La conexión con los números primos fue descubierta también por Euler como se mostró en el capítulo 2, y se basa en la igualdad:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}$$

válida para todo número complejo $s = \sigma + i\tau$, $\sigma > 1$.

Otra fórmula interesante que hemos utilizado en capítulos anteriores es la siguiente

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

válida también cuando $\mathrm{Re}(s) > 1$ y donde aparece la función de Möbius $\mu(n) = (-1)^{p(n)}$ donde $p(n)$ es el número de primos todos distintos que dividen a n, pero siendo $\mu(n) = 0$ si n fuese divisible por el cuadrado de un número primo (ver §4.8, p. 162).

En el año 1859 B. Riemann publicó un trabajo muy notable titulado "Sobre el número de primos menores que una cantidad dada", en el que extendió la función $\zeta(s)$ a todo el dominio complejo, salvo el valor $s = 1$ donde no está definida. Demostró que ζ verifica la ecuación funcional

$$\zeta(s) = 2^s \pi^{s-1} \,\mathrm{sen}\left(\tfrac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

y relacionó sus propiedades con la distribución de los números primos.

Riemann desveló el papel que los ceros de la función ζ (los puntos donde se anula) desempeñan en la manera que tienen los primos de aparecer en la sucesión de los enteros positivos. Resulta relativamente fácil demostrar que la función ζ se anula en los puntos $s = -2, -4, -6, \ldots$ y que carece de ceros en el semiplano $\mathrm{Re}(s) > 1$. Pero Riemann observó que la acción relevante transcurre en la llamada banda crítica $0 < \mathrm{Re}(s) < 1$ y conjeturó que los infinitos ceros de ζ dentro de esa banda se encuentran ubicados, precisamente, en la línea vertical $\mathrm{Re}(s) = \frac{1}{2}$. Existen muchas teorías y resultados en las matemáticas que dependen de, o están estrechamente relacionados con, esa Hipótesis de Riemann, por lo que se trata, quizás, del problema abierto más famoso de las Matemáticas, que ya formó parte de la lista de preguntas que Hilbert formuló en el Congreso Internacional celebrado en París en el año 1900:

¿Dónde están los ceros de la función ζ?

Recientemente la fundación CLAY lo ha incluido entre los siete problemas del milenio y ofrece un millón de dólares por su solución.

Ejercicios

1) *Demostrar las fórmulas:*

$$\begin{aligned}\cos(z+w) &= \cos z \cos w - \operatorname{sen} z \operatorname{sen} w\\ \operatorname{sen}(z+w) &= \operatorname{sen} z \cos w + \cos z \operatorname{sen} w.\end{aligned}$$

2) *Sean z_1 y z_2 números complejos tales que $\operatorname{Re}(z_j) > 0$, $j = 1, 2$. Si $\log z$ designa a la rama principal del logaritmo demostrar que*

$$\log(z_1 \cdot z_2) = \log z_1 + \log z_2.$$

3) *Sea $z_0 \in \mathbb{C}$ y $r > 0$ un número real positivo. Describir geométricamente el conjunto de puntos*

$$|z - z_0| - |z + z_0| = 2r.$$

4) *Describir el lugar geométrico $\{z \in \mathbb{C} \mid z^2 + \overline{z}^{\,2} = 2\}$.*

5) *Estudiar las funciones de la variable real x: $\operatorname{sen}(ix)$, $\cos(ix)$, $\tan(ix)$.*

6) *Demostrar que cuando $x > 1$ es real tenemos la igualdad*

$$\zeta(x) = \frac{1}{\Gamma(x)} \int_0^\infty \frac{u^{x-1}}{e^u - 1} \mathrm{d}\, u.$$

7) *Estudiar las identidades:*

$$\zeta(2) = 3 \sum_{k=1}^{\infty} \frac{1}{k^2 \binom{2k}{k}}; \quad \zeta(3) = \frac{5}{2} \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3 \binom{2k}{k}}; \quad \zeta(4) = \frac{36}{17} \sum_{k=1}^{\infty} \frac{1}{k^4 \binom{2k}{k}}; \ldots$$

8) *Comprobar que:*

$$\sum_{n=2}^{\infty} \big(\zeta(n) - 1\big) = 1 \qquad \sum_{n=1}^{\infty} \big(\zeta(2n) - 1\big) = \frac{3}{4}$$

$$\sum_{k=2}^{\infty} \frac{(-1)^k \zeta(k)}{k} = \gamma = \text{ constante de Euler–Mascheroni.}$$

De joven enfrentose al gran problema que Riemann formuló con perspicacia. La Hipótesis quiso hacer teorema: quimeras en la edad de la arrogancia. Varias veces creyó subir la cima, disponiendo los ceros con audacia. Mas la Zeta el favor siempre escatima: todo lema crucial cae en desgracia. Aunque pronto su mente ya aprendía la lección de errores tan funestos, y lo intenta otra vez con más porfía. Sueña ceros en fila bien dispuestos: ¡qué prueba tan perfecta, qué alegría!, ¡qué control de los primos y compuestos!

Pero siempre despertaba hallando un fallo, una abertura en el engarce de las ideas por la que toda la construcción se venía abajo.

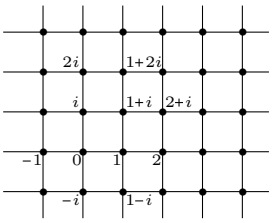
Pasó el tiempo y aquel joven arrogante era ya un anciano. Un atardecer, mientras descendía la ladera de una montaña menor, frente al mar encendido por el sol poniente, tuvo la visión de la Zeta formando una superficie bellísima, suave y ondulada en muchas partes, agreste en otras como una ola a punto de romper, pero con sus esquivos ceros perfectamente alineados (¿perfectamente?). Sentose en silencio bajo una encina y permaneció durante muchas horas observando a una distribución tan bella reflejarse en el mar.

6.5. Aritmética en $\mathbb{C}$

Entre los números complejos podemos señalar algunos subconjuntos que tienen propiedades similares a los números enteros y que han sido muy útiles para entender cuestiones aritméticas del anillo $\mathbb{Z}$. Uno de los más notables fue descrito por Gauss:

$$\mathbb{Z}[i] = \{a + b\,i \mid a, b \in \mathbb{Z}\},$$

cuyos elementos están representados en el plano complejo por los puntos de coordenadas enteras, constituyendo el retículo unidad:



El conjunto $\mathbb{Z}[i]$ es cerrado para la suma y el producto, verificándose todas las propiedades que caracterizan a la estructura que hemos llamado anillo conmutativo. Hay cuatro elementos inversibles (o unidades del anillo), a saber: 1, -1, i, $-i$.

La norma de un entero de Gauss es el número natural obtenido al multiplicarlo por su conjugado:

$$\mathrm{N}[a + bi] = (a + bi)(a - bi) = a^2 + b^2.$$

Ejercicio 3. *a) Comprobar que la norma es multiplicativa:*

$$\mathrm{N}[\alpha \cdot \beta] = \mathrm{N}[\alpha] \cdot \mathrm{N}[\beta],$$

para $\alpha = a + bi$, $\beta = c + di$ enteros arbitrarios en $\mathbb{Z}[i]$.
b) Demostrar que $\mathrm{N}[\alpha] = 1$ si y solo si α es una unidad: $\alpha = 1, -1, i, -i$.

En $\mathbb{Z}[i]$ tenemos también la relación de divisibilidad. Diremos que $\alpha = a + bi$ es un divisor de $\beta = c + di$ si existe $\gamma = e + fi$ tal que $\alpha = \beta \cdot \gamma$.

Todo entero de Gauss α es divisible siempre por las unidades 1, -1, i, $-i$ y por sus asociados α, $-\alpha$, $i\alpha$, $-i\alpha$. En el caso de que estos sean sus únicos divisores diremos que α es primo. Naturalmente, en caso contrario lo llamaremos compuesto.

Si $\mathrm{N}[\alpha] = a^2 + b^2 = p$ es un número natural primo en $\mathbb{Z}$, entonces α tiene que ser primo en $\mathbb{Z}[i]$ ya que la descomposición $\alpha = \beta \cdot \gamma$ implicaría $\mathrm{N}[\alpha] = \mathrm{N}[\beta] \cdot \mathrm{N}[\gamma]$, y esto solo es posible si uno de los dos, $\mathrm{N}[\beta]$ o $\mathrm{N}[\gamma]$, es igual a 1 y, por lo tanto, β o γ es una unidad.

Ejemplos:

1. *$\mathrm{N}[1+i] = 1^2+1^2 = 2$, luego $1+i$, y sus asociados, $1-i$, $-1+i$, $-1-i$, son primos.*
2. *$\mathrm{N}[2+i] = 4+1 = 5$, $\mathrm{N}[2+3i] = 4+9 = 13$, luego $2+i$, $2+3i$ y sus correspondientes asociados son primos en $\mathbb{Z}[i]$.*
3. *Observemos que 5, aunque primo en $\mathbb{Z}$, no lo es en $\mathbb{Z}[i]$ por cuanto $5 = (2+i)(2-i)$. Tampoco lo es 13 o 17. Sin embargo 3 sí es primo en $\mathbb{Z}[i]$ ya que $3 = \alpha \cdot \beta$ implicaría $\mathrm{N}[\alpha] = 3$ (o $\mathrm{N}[\beta] = 3$) y la ecuación $a^2 + b^2 = 3$ carece de solución en enteros a y b.*

El anillo $\mathbb{Z}[i]$ posee también un algoritmo de la división (es un anillo euclídeo) basado en la observación siguiente:

Lema. *Dados dos enteros de Gauss α y $\beta \neq 0$, existe otro entero γ tal que*

$$\mathrm{N}[\alpha - \beta \cdot \gamma] \leq \tfrac{1}{2}\,\mathrm{N}[\beta] < \mathrm{N}[\beta].$$

Demostración. *Sean $\alpha = a + bi$, $\beta = c + di$ y calculemos*

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i = R + Si.$$

Sean x, y números enteros situados a distancia menor o igual que $\frac{1}{2}$, respectivamente, de los números racionales R y S:

$$|x - R| \leq \tfrac{1}{2}\,, \qquad\qquad |y - S| \leq \tfrac{1}{2}.$$

Entonces:

$$a + bi = (c+di)(x+yi) + (c+di)\big(R - x + (S-y)i\big).$$

Observemos que $\gamma = (c+di)\big(R - x + (S-y)i\big) = (a+bi) - (c+di)(x+yi)$ es un entero de Gauss tal que:

$$\begin{aligned}\mathrm{N}[\gamma] = \mathrm{N}[c+di]\,\mathrm{N}[R-x+(S-y)i] &\leq (c^2+d^2)\left((R-x)^2 + (S-y)^2\right)\\ &\leq \frac{1}{2}\,(c^2+d^2) = \frac{1}{2}\,\mathrm{N}[\beta].\end{aligned}$$

■

El algoritmo de la división implica que todo entero de Gauss se descompone de manera única (salvo unidades) en producto de primos:

A *Dado $\alpha \in \mathbb{Z}[i]$ consideremos el conjunto $\mathcal{D}(\alpha)$ de sus divisores y quitémosle las unidades. Si un elemento $\pi \in \mathcal{D}(\alpha)\backslash\{1,-1,i,-1\}$ es de norma mínima, entonces π es primo pues, en caso contrario, sería un producto $\pi = \beta \cdot \gamma$ ($\mathrm{N}[\beta] \neq 1$, $\mathrm{N}[\gamma] \neq 1$) con β y γ en $\mathcal{D}(\alpha) \setminus \{1,-1,i,-1\}$ cuyas normas son estrictamente menores que la de π, en contra de la hipótesis de que π era de norma mínima.*

Por lo tanto, todo entero de Gauss α es divisible por un primo π_1: $\alpha = \pi_1 \cdot \alpha_1$, $\mathrm{N}[\alpha_1] < \mathrm{N}[\alpha]$; y el proceso se repite hasta que, en un número finito de pasos, obtenemos α como producto de números primos.

B *Dados dos enteros α y β consideremos el conjunto $I = \{\mu\alpha + \nu\beta \mid \mu, \nu \in \mathbb{Z}[i]\}$ y sea $\delta \neq 0$ un elemento de I de norma mínima. Tenemos que $I = \{\sigma \cdot \delta \mid \sigma \in \mathbb{Z}[i]\}$. En efecto, dado $\gamma \in I$ el algoritmo de Euclides para γ y δ nos da:*

$$\gamma = \tau\delta + \rho\,, \qquad \mathrm{N}[\rho] \leq \tfrac{1}{2}\mathrm{N}[\delta]$$

pero esto solo es posible si $\rho = 0$ ya que, en caso contrario tendríamos un elemento $\rho = \gamma - \tau\delta \in I$ de norma estrictamente menor que δ.

Es fácil ver que δ es un divisor de α y β, y que todo divisor común a ambos, α y β, lo es también de δ. Se trata pues del máximo común divisor $\delta = m.c.d.(\alpha, \beta)$ (que está definido salvo producto con una de las unidades).

El algoritmo de Euclides permite, como en $\mathbb{Z}$, establecer una estrategia para el calcular el $m.c.d.(\alpha, \beta)$ por medio de divisiones sucesivas: el último resto, antes de cero, es el máximo común divisor.

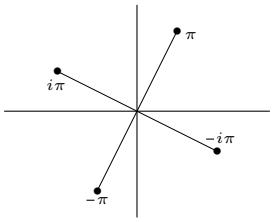
Tenemos también la identidad de Bézout: dados α y β enteros de Gauss, existen dos enteros μ y ν tales que $m.c.d.(\alpha, \beta) = \mu\alpha + \nu\beta$.

Si el máximo común divisor es una unidad diremos que α y β son primos entre sí. Estamos ahora en condiciones de probar el lema clave:

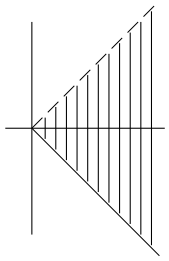
Lema. *Si $\pi \mid \alpha\beta$ y π es primo con α entonces π divide a β.*

Demostración. *Si π no es un divisor de α entonces $1 = m.c.d.(\pi, \alpha)$. Luego existen μ, $\nu \in \mathbb{Z}[i]$ tales que $1 = \mu\pi + \nu\alpha$ y, por tanto, $\beta = \mu\beta\pi + \nu\alpha\beta$. Es decir $\pi \mid \beta$.* ■

Dado un primo π sus asociados, $-\pi$, $i\pi$, $-i\pi$, que son también primos, están situados sobre la circunferencia centrada en el origen de radio $\sqrt{\mathrm{N}[\pi]}$, formando los vértices de un cuadrado.



Uno solo de los cuatro pertenecerá al cuadrante rayado en la figura:



$$C^+ = \{x + iy \mid x > 0,\ -x \leq y < x\}$$

Con abuso de lenguaje podemos llamar "positivos" a los primos situados en C^+. Estamos en condiciones de formular el Teorema Fundamental de la Aritmética en $\mathbb{Z}[i]$:

> *Todo entero de Gauss es una unidad o se descompone, de manera única, en el producto de una unidad por primos positivos elevados a exponentes naturales positivos:*
>
> $$\alpha = i^k \cdot \pi_1^{a_1} \cdot \cdots \cdot \pi_s^{a_s}.$$

Pero, ¿quiénes son los primos de Gauss? He aquí la lista completa:

1) $1 + i$ *y sus asociados* $1 - i$, $-1 + i$, $-1 - i$.

2) *Los primos de* $\mathbb{Z}$ *que son congruentes con* 3 *módulo* 4 *y sus asociados:*

$$3,\ 7,\ 11,\ 19,\ 23,\ \ldots$$

3) *Los factores en* $\mathbb{Z}[i]$ *en que se descomponen los primos de* $\mathbb{Z}$ *que son congruentes con* 1 *módulo* 4 *(y sus asociados):*

$$5 = (2+i)(2-i), \qquad 13 = (2+3i)(2-3i), \qquad 17 = (4+i)(4-i), \quad \ldots$$

Veamos: el punto 1) ya lo hemos analizado antes. En cuanto a 2) observemos que si $p \equiv 3\ mod(4)$ y $p = \alpha \cdot \beta$ en $\mathbb{Z}[i]$ resultaría que

$$p^2 = \mathrm{N}[p] = \mathrm{N}[\alpha]\mathrm{N}[\beta] = (a^2 + b^2)(c^2 + d^2)\,,$$

siendo $\alpha = a + bi$, $\beta = c + di$. Luego si α y β no son unidades habríamos de tener $p = a^2 + b^2 = c^2 + d^2$, lo que es imposible si $p \equiv 3\ mod(4)$.

Para completar el análisis tenemos que mostrar que si $p \equiv 1\ mod(4)$ es primo en $\mathbb{Z}$ entonces la ecuación $p = a^2 + b^2$ tiene solución (única salvo cambios de signos $\pm a$, $\pm b$).

Pero por ser $p \equiv 1\ mod(4)$ la ecuación $x^2 \equiv -1\ mod(p)$ tiene solución, como vimos en el capítulo 3. Es decir, existe un entero x tal que p es un divisor de $x^2+1=(x+i)(x-i)$.

Si p fuese primo en $\mathbb{Z}[i]$ tendría que ser un divisor de uno de los dos números $x+i$ o $x-i$, y eso no es posible. Luego $p=\alpha\cdot\beta$, con $\alpha=a+bi$, $\beta=c+di$ para ciertos enteros a, b, c, d. Ahora es ya un ejercicio fácil comprobar que $\beta=c+di=\overline{\alpha}=a-bi$ y que $a^2+b^2=p$.

Hay propiedades de los números enteros ordinarios que resultan mucho más fáciles de entender, y demostrar, cuando los analizamos en $\mathbb{Z}[i]$. Un ejemplo notable es la función

$$r(n)=card\big\{(a,b)\in\mathbb{Z}^2 \mid a^2+b^2=n\big\}$$

que cuenta el número de puntos del retículo unidad que están situados sobre la circunferencia de radio $\sqrt{n}$ centrada en el origen.

Ejercicio 4. *Usar el Teorema Fundamental de la Aritmética en $\mathbb{Z}[i]$ para demostrar el resultado siguiente:*

Sea

$$n=2^{\nu}\prod_{p_j\equiv 1(4)}p_j^{a_j}\prod_{q_k\equiv 3(4)}p_k^{b_k}$$

la descomposición en factores primos de n en $\mathbb{Z}$. Entonces:

1) *Si algún exponente b_k es impar resulta que $r(n)=0$.*
2) *Si todos los b_k, exponentes de los primos $\equiv 3\ mod(4)$, son pares, entonces:*

$$r(n)=4\prod_j(1+a_j).$$

Ejemplos:

$r(2)=4\,,\quad 2=(\pm1)^2+(\pm1)^2$
$r(3)=0$
$r(4)=4\,,\quad 4=(\pm2)^2+0^2=0^2+(\pm2)^2$
$r(5)=8\,,\quad 5=(\pm2)^2+(\pm1)^2=(\pm1)^2+(\pm2)^2$
$r(6)=0\,,\quad r(7)=0\ldots,\quad r(65)=16\,,\ldots$

Sea $\omega=e^{\frac{2\pi i}{3}}$ una de las raíces cúbicas de la unidad. El conjunto

$$\big\{a+b\,\omega \mid a\,,b\in\mathbb{Z}\big\}=\mathbb{Z}[\omega]$$

es cerrado para la multiplicación (porque $\omega^2=-1-\omega$) y constituye otro ejemplo notable de anillo de enteros en el que también se verifica el Teorema Fundamental de la Aritmética.

Este anillo resulta ser útil para entender que la ecuación de Fermat $x^3 + y^3 = z^3$, $x \cdot y \cdot z \neq 0$, *carece de soluciones en* $\mathbb{Z}$. *La demostración se hace viendo que tampoco tiene solución en* $\mathbb{Z}[\omega]$, *lo que es algo más fuerte pero* $\mathbb{Z}[\omega]$ *nos permite herramientas de las que carecemos en* $\mathbb{Z}$ *para implementar el método del descenso inventado por Fermat.*

No todos los anillos de enteros que podemos definir en $\mathbb{C}$ *verifican el Teorema Fundamental de la Aritmética. Por ejemplo en* $A = \left\{a + b\sqrt{-5} \mid a\,, b \in \mathbb{Z}\right\}$ *tenemos que:*

$$6 = 2 \times 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

y no es difícil comprobar que 2, 3, $1 + \sqrt{-5}$ *y* $1 - \sqrt{-5}$ *son elementos irreducibles de* A.

6.6. Cuaterniones

El conjunto de los complejos culmina la construcción de los cuerpos de números en un sentido muy preciso que estudiaremos en el capítulo 9: $\mathbb{C}$ *es algebraicamente cerrado, lo que significa que contiene las raíces de todos los polinomios; o, lo que es equivalente, podemos resolver todas las ecuaciones polinómicas dentro de* $\mathbb{C}$.

No obstante, podemos preguntarnos si de la misma manera que hemos obtenido $\mathbb{C}$ *dotando de una multiplicación a los puntos (o vectores) del plano* $\mathbb{R}\times\mathbb{R}$, *cabría obtener un cuerpo de números más grande si hacemos lo propio con* $\mathbb{R}^3$ *o, en general, con* $\mathbb{R}^n$.

Dada una base del espacio $\mathbb{R}^n$, *por ejemplo la base canónica*

$$\left.\begin{array}{l} e_1 = (1,0,0,0,\ldots,0) \\ e_2 = (0,1,0,0,\ldots,0) \\ e_3 = (0,0,1,0,\ldots,0) \\ \vdots \\ e_n = (0,0,0,0,\ldots,1) \end{array}\right\}$$

definir un producto que cumpla las leyes asociativa y distributiva respecto a la suma, equivale a definir el producto de elementos de la base con esas restricciones. Sean

$$e_j \cdot e_k = \sum_\ell \Gamma_{j,k}^\ell e_\ell$$

donde los coeficientes de estructura $\Gamma_{j,k}^\ell$ *son números reales.*

Que se verifique la propiedad asociativa equivale a que cualesquiera que sean los elementos de la base e_i, e_j, e_k *se verifique la identidad*

$$(e_i e_j)e_k = e_i(e_j e_k)$$

lo que impone una serie de restricciones a los coeficientes de estructura:

$$(e_i e_j)e_k = \big(\sum_\ell \Gamma^\ell_{i,j} e_\ell\big)e_k = \sum_\ell \Gamma^\ell_{i,j} e_\ell e_k = \sum_\ell \Gamma^\ell_{i,j} \sum_m \Gamma^m_{\ell,k} e_m$$
$$e_i(e_j e_k) = e_i\big(\sum_\ell \Gamma^\ell_{j,k} e_\ell\big) = \sum_\ell \Gamma^\ell_{j,k} e_i e_\ell = \sum_\ell \Gamma^\ell_{j,k} \sum_m \Gamma^m_{i,\ell} e_m$$

i.e.

$$\boxed{\sum_\ell \sum_m \Gamma^\ell_{i,j}\,\Gamma^m_{\ell,k} = \sum_\ell \sum_m \Gamma^\ell_{j,k}\,\Gamma^m_{i,\ell} \qquad \forall i,j,k.}$$

Esta ecuación admite soluciones que producen sistemas hipercomplejos. Sin embargo, si imponemos que la multiplicación sea también conmutativa y sin divisores de cero entonces la dimensión tiene que ser dos y, si además, queremos resolver la ecuación $x^2+1=0$, entonces recuperamos los números complejos de siempre.

El caso particular $n=4$ es especialmente interesante dando lugar a los cuaterniones de Hamilton que tienen la expresión

$$a + bi + cj + dk\,, \qquad a,b,c,d \in \mathbb{R}$$

con las siguientes reglas de multiplicar:

$$\left.\begin{array}{c} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik \end{array}\right\} (*)$$

Es decir se trata de los vectores de $\mathbb{R}^4$ donde hemos señalado como eje real el correspondiente a $(1,0,0,0)=1$ y tres imaginarios $i=(0,1,0,0)$, $j=(0,0,1,0)$, $k=(0,0,0,1)$. La multiplicación $(*)$ es asociativa y podemos dividir (excepto por 0), pero carece de conmutatividad.

Los cuaterniones fueron descubiertos por el matemático irlandés William Hamilton a mediados del siglo XIX *y son muy útiles en varias teorías de la Geometría y de la Física.*

Siguiendo a Hamilton, Arthur Cayley descubrió los octoniones también llamados números de Cayley:

$$x_0 + x_1 i_i + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6 + x_7 i_7$$

donde los x_j son números reales y cada una de las ternas

$$(i_1,i_2,i_4)\ \ (i_2,i_3,i_5)\ \ (i_3,i_4,i_6)\ \ (i_4,i_5,i_7)\ \ (i_5,i_6,i_1)\ \ (i_6,i_7,i_2)\ \ (i_7,i_1,i_3)$$

se multiplican como los números de Hamilton (i,j,k). Así la multiplicación de octoniones viene dada por la siguiente tabla:

$\cdot$	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
1	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	i_1	-1	i_4	i_7	$-i_2$	i_6	$-i_5$	$-i_3$
i_2	i_2	$-i_4$	-1	i_5	i_1	$-i_3$	i_7	$-i_6$
i_3	i_3	$-i_7$	$-i_5$	-1	i_6	i_2	$-i_4$	i_1
i_4	i_4	i_2	$-i_1$	$-i_6$	-1	i_7	i_3	$-i_5$
i_5	i_5	$-i_6$	i_3	$-i_2$	$-i_7$	-1	i_1	i_4
i_6	i_6	i_5	$-i_7$	i_4	$-i_3$	$-i_1$	-1	i_2
i_7	i_7	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$	-1

Pero la multiplicación de números de Cayley no es asociativa, aunque sí permite dividir por números distintos de 0.

A mediados del siglo XX*, J. F. Adams demostró que solo en dimensiones* $n = 1, 2, 4$ *y* 8 *podemos dotar al espacio* $\mathbb{R}^n$ *de un producto que origine un álgebra de división, es decir, en la que siempre podemos dividir por un elemento distinto de* 0*. Pero si queremos que la multiplicación sea también conmutativa, entonces* n *tiene que ser* 1 *o* 2 *y recuperamos, respectivamente, nuestros números reales o complejos.*

— 7 —

El orden y los ordinales

> *...El uno, por ejemplo, iba antes del dos aunque la U era una de las últimas letras del abecedario. Además, desayunábamos antes de comer y comíamos antes de cenar, cuando en una progresión alfabética se debería comenzar el día con la cena para continuar con la comida y acabar la jornada con un buen desayuno. Esta falta de acuerdo permanente entre el mundo enciclopédico y la existencia real constituyó una de las preocupaciones más fuertes de mi infancia.*
>
> Juan José Millás
>
> *(El orden alfabético)*

7.1. Con un poco de orden, aunque sea parcial

Según el diccionario de la Real Academia Española de la Lengua, la palabra "orden" deriva del latín "ordo-ordonis", y significa "colocación de las cosas en el lugar que les corresponde". Sigamos la pista:

Colocación:	*acción o efecto de colocar o colocarse.*
Colocar:	*poner a una persona o cosa en su debido lugar.*
Cambiemos de táctica	
Desorden:	*confusión y alteración del concierto propio de una cosa.*
Concierto:	*buen orden y disposición de las cosas.*
Confusión:	*caos, falta de orden, de concierto y de claridad.*
Caos:	*del latín "chaos" y este del griego "$\chi\alpha\varnothing\varsigma$".* *1. Estado de confusión en que se hallaban las cosas al momento de su creación, antes de que Dios las colocase en el orden que después tuvieron.* *2. Figuradamente: confusión, desorden.*

En vez de investigar el tipo de sustancia que ingirieron los señores académicos para lograr tan imaginativas definiciones, será más prudente que analicemos el concepto matemático, mucho más austero, de relación de orden.

Una relación binaria, $\mathcal{R}$, en un conjunto X, para la que usaremos la notación "$a\,\mathcal{R}\,b$" y diremos que "a está relacionado con b", nos determina un subconjunto del producto cartesiano $X \times X$.

Designaremos tal subconjunto con la misma letra que la relación binaria, $\mathcal{R}$, y diremos que el par ordenado (a, b) pertenece a $\mathcal{R}$ si $a\,\mathcal{R}\,b$. Recíprocamente, todo subconjunto $\mathcal{R}$ de $X \times X$, determina una relación: $a\,\mathcal{R}\,b$ si $(a, b) \in \mathcal{R}$. Es decir, tenemos la siguiente definición:

Definición. *Una relación binaria en el conjunto X es un subconjunto, $\mathcal{R}$, del producto cartesiano $X \times X$. Escribiremos $x\,\mathcal{R}\,y$ si y solo si $(x, y) \in \mathcal{R}$.*

Definición. *Un orden es una relación que cumple las propiedades:*

i) Reflexiva. $x\,\mathcal{R}\,x$, $\forall x \in X$.

ii) Antisimétrica. $(x\,\mathcal{R}\,y) \wedge (y\,\mathcal{R}\,x) \Rightarrow x = y$.

iii) Transitiva. $(x\,\mathcal{R}\,y) \wedge (y\,\mathcal{R}\,z) \Rightarrow (x\,\mathcal{R}\,z)$.

Abreviaremos la expresión "la relación $\mathcal{R}$ definida en el conjunto X es de orden", diciendo que $(X; \mathcal{R})$ es un conjunto ordenado.

Ejemplos de órdenes.

1. *El orden "$\leq$" en los naturales, $\mathbb{N}$; los enteros, $\mathbb{Z}$; los racionales, $\mathbb{Q}$; y los reales, $\mathbb{R}$.*
2. *La inclusión "$\subset$" en $\mathcal{P}(X)$ (partes de X).*
3. *La relación de divisibilidad en $\mathbb{N}$.*
4. *En $\mathbb{Z} \times \mathbb{Z}$ la relación $\mathcal{R}$ dada por:*

$$(a, b)\,\mathcal{R}\,(c, d) \quad \text{si y solo si} \quad (a \leq c) \wedge (b \leq d).$$

5. *El orden lexicográfico, o alfabético, en el conjunto de las palabras de un idioma.*
6. *En el conjunto de las funciones $f : [0, 1] \longrightarrow \mathbb{R}$ definimos $f \leq g$ si y solo si $f(x) \leq g(x)$ para todo $x \in [0, 1]$.*

Ejercicio 1. *Comprobar que los ejemplos anteriores verifican las tres propiedades exigidas a todo orden.*

Ejercicio 2. *Dado un conjunto ordenado, $(X; \mathcal{R})$, sea $x\,\mathcal{R}^{-1}y$ si y solo si $y\,\mathcal{R}\,x$. Demostrar que $(X; \mathcal{R}^{-1})$ es también un conjunto ordenado (con el orden inverso $\mathcal{R}^{-1}$).*

Cuando un orden $\mathcal{R}$ verifica que dos elementos cualesquiera de X son siempre comparables (ora $x\,\mathcal{R}\,y$, ya $y\,\mathcal{R}\,x$), se dice que tenemos un orden total o lineal. Por contraposición, un orden parcial es aquel en el que existen elementos que no son comparables.

En un conjunto ordenado $(X;\mathcal{R})$, una cadena es un subconjunto totalmente ordenado por $\mathcal{R}$.

Definición. *Sea $(X;\mathcal{R})$ un conjunto ordenado.*

1. *$c \in X$ es una cota superior de $A \subset X$ si $x\,\mathcal{R}\,c\ \forall x \in A$.*
2. *$c \in X$ es una cota inferior de $A \subset X$ si $c\,\mathcal{R}\,x\ \forall x \in A$.*
3. *$s \in X$ es un extremo superior o supremo de $A \subset X$ si s es una cota superior de A, y no existe otra cota superior c que verifique $c\,\mathcal{R}\,s$.*
4. *$i \in X$ es un extremo inferior o ínfimo de $A \subset X$ si i es una cota inferior de A, y no existe otra cota inferior c que verifique $i\,\mathcal{R}\,c$.*
5. *Diremos que $\overline{a}$ es el máximo de $A \subset X$ si $\overline{a} \in A$ y $x\,\mathcal{R}\,\overline{a}\ \forall x \in A$.*
6. *Diremos que $\underline{a}$ es el mínimo de $A \subset X$ si $\underline{a} \in A$ y $\underline{a}\,\mathcal{R}\,x\ \forall x \in A$.*
7. *El elemento $m \in X$ es maximal si no existe $y \neq m$ tal que $m\,\mathcal{R}\,y$.*
8. *El elemento $m \in X$ es minimal si no existe $y \neq m$ tal que $y\,\mathcal{R}\,m$.*

Obsérvese que las definiciones anteriores no garantizan la existencia de elementos con esas propiedades. Eso dependerá del conjunto ordenado que tengamos. En el caso de que el orden sea total, cada conjunto tendrá, a lo sumo, un extremo superior y un extremo inferior. La unicidad del máximo y del mínimo, en el caso de que existan, está garantizada por sus propias definiciones.

Ejercicio 3. *En $(\mathbb{R};\leq)$ hallar el máximo, mínimo, supremo e ínfimo de los conjuntos siguientes:*

$$(0,1);\ [0,1);\ (0,1];\ [0,1];\ \{2^{-n}\}_{n=1,2,3,\ldots};\ \mathbb{Q}\cap[-\pi,\pi].$$

Ejercicio 4. *Sea el conjunto cuyos elementos son los conjuntos*

$$I_m = \{\dot{m}\} = \{k\cdot m\}_{k\in\mathbb{Z}}\,,\quad m = 2,3,4,\ldots,$$

es decir: $X = \{I_2, I_3, I_4, I_5, I_6, \ldots\}$. Definamos la relación $I_m\,\mathcal{R}\,I_k$ si y solo si $I_m \subset I_k$. Determinar los elementos maximales.

Dados dos conjuntos ordenados $(X;\mathcal{R})$, $(Y;\mathcal{S})$ diremos que una función $f : X \longrightarrow Y$ es creciente, o que preserva el orden, si

$$(x_1\,\mathcal{R}\,x_2) \implies \big(f(x_1)\,\mathcal{S}\,f(x_2)\big).$$

Diremos que es estrictamente creciente si además es inyectiva:

$$\big[(x_1 \neq x_2) \wedge (x_1\,\mathcal{R}\,x_2)\big] \implies \big[\big(f(x_1)\neq f(x_2)\big) \wedge \big(f(x_1)\,\mathcal{S}\,f(x_2)\big)\big].$$

Definición. *Dos conjuntos ordenados,* $(X;\mathcal{R})$, $(Y;\mathcal{S})$, *son equivalentes si existe una aplicación biyectiva que preserva el orden:*

$$f : X \longrightarrow Y \quad \text{biyectiva tal que si } x_1\,\mathcal{R}\,x_2 \text{ entonces } f(x_1)\,\mathcal{S}\,f(x_2).$$

En este caso también diremos que $(X;\mathcal{R})$ *y* $(Y;\mathcal{S})$ *tienen el mismo tipo.*

Ejemplo 1: *Sean los conjuntos* $\mathbb{N}$ *y* $P = \{0, 2, 4, 6, \ldots, 2n, \ldots\}$ *con la relación* $\leq$. *La aplicación* $f(x) = 2x$ *realiza la equivalencia.*

Ejercicio 5. *¿Son equivalentes* $(\mathbb{N};\leq)$ *y* $(\mathbb{Q};\leq)$*?*

Proposición. *Todo conjunto numerable totalmente ordenado,* $(A;\mathcal{R})$, *es equivalente a un subconjunto de los racionales con el orden* $\leq$ *inducido de* $\mathbb{Q}$.

Demostración. *Sea* $a_1, a_2, a_3, \ldots$ *una enumeración de los elementos de* A. *Definiremos la función* $f : A \longrightarrow \mathbb{Q}$ *de manera inductiva:*

i) $f(a_1) = 0$.

ii) Supongamos elegidos los racionales $f(a_1), \ldots, f(a_n)$. *Obtendremos el siguiente,* $f(a_{n+1})$, *de este modo:*

Si a_{n+1} *es posterior en el orden* $\mathcal{R}$ *a todos los elementos* $a_1, \ldots, a_n$, *entonces basta hacer* $f(a_{n+1})$ *racional y mayor que todos los números* $f(a_1), \ldots, f(a_n)$.

Si a_{n+1} *es anterior en el orden* $\mathcal{R}$ *a todos los* $a_1, \ldots, a_n$, *escogemos* $f(a_{n+1})$ *entre los racionales menores que* $f(a_1), \ldots, f(a_n)$.

Finalmente, si no se dan ninguna de las dos situaciones anteriores, al ordenar el conjunto $\{a_1, \ldots, a_n\}$ *por el orden* $\mathcal{R}$, a_{n+1} *estará comprendido entre dos de ellos. Es decir:* $a_\ell\,\mathcal{R}\,a_{n+1}$, $a_{n+1}\,\mathcal{R}\,a_m$, *de manera que* $\forall j$: $(a_j\,\mathcal{R}\,a_\ell) \vee (a_m\,\mathcal{R}\,a_j)$.

En este caso hacemos $f(a_{n+1})$ *racional y comprendido entre* $f(a_\ell)$ *y* $f(a_m)$ *(por ejemplo:* $f(a_{n+1}) = (f(a_\ell) + f(a_m))/2$*).*

La demostración se concluye observando que $f : A \longrightarrow f(A) \subset \mathbb{Q}$ *es biyectiva y preserva el orden:* $x\,\mathcal{R}\,y \Rightarrow f(x) \leq f(y)$. ■

Ejercicio 6. *Demostrar las propiedades siguientes:*

a) *Si* $(X;\mathcal{R})$, $(Y;\mathcal{S})$ *son equivalentes y* $\mathcal{R}$ *es un orden total, entonces* $\mathcal{S}$ *es también total.*

b) *Si existe* $\min(X)$ *entonces también existe* $\min(Y)$, *para cualesquiera par de órdenes equivalentes* $(X;\mathcal{R})$, $(Y;\mathcal{S})$.

c) *Probar la propiedad análoga a b) para los máximos.*

d) *Si* f *es la aplicación biyectiva que realiza la equivalencia de los órdenes* $(X;\mathcal{R})$, $(Y;\mathcal{S})$, *entonces* f *lleva elementos maximales en elementos maximales.*

7.2. Algunos órdenes buenos

Entre los órdenes los hay de una importancia especial: "Diremos que $(X; \mathcal{R})$ *es un buen orden, o que el conjunto* X *está bien ordenado, si todo subconjunto no vacío* $A \subset X$ *tiene un mínimo".*

Esto implica que el orden es total, ya que dados dos elementos distintos, x *e* y*, la existencia de un mínimo del conjunto* $\{x, y\}$ *fuerza que uno de ellos sea anterior al otro,* y*, por lo tanto, que estén relacionados.*

Ejemplo 2: *El conjunto* $\mathbb{N}$ *está bien ordenado por la relación* $\leq$*. No ocurre lo mismo con* $(\mathbb{Z}; \leq)$*,* $(\mathbb{Q}; \leq)$ *y* $(\mathbb{R}; \leq)$*, ¿por qué?*

En un conjunto bien ordenado todo elemento distinto del máximo, si este existe, tiene un siguiente, a saber:

$$s(x) = \min \{y \in X \,;\, y \neq x,\, x \,\mathcal{R}\, y\}\,.$$

Pero no existe, en general, el precedente, como muestra el ejemplo:

$$X = \left\{1 - \frac{1}{2}, 1 - \frac{1}{3}, 1 - \frac{1}{4}, \ldots, 1 - \frac{1}{n}, \ldots, 1\right\}$$

con la relación de orden $\leq$*. Se trata de una relación de orden en la que* $s(1 - 1/n) = 1 - 1/(n+1)$*. Pero no hay precedente para* 1*.*

Ejercicio 7. *Demostrar que el orden* $\leq$ *en el conjunto* X *antes definido es del mismo tipo que el orden* $\mathcal{R}$ *en el conjunto* $\mathbb{N} \cup \{\mathbb{N}\}$ *dado por:*

i) si x*,* y *son elementos de* $\mathbb{N}$ *entonces* $x \,\mathcal{R}\, y$ *si y solo si* $x \leq y$*;*

ii) $\forall x \in \mathbb{N}$ *se verifica que* $x \,\mathcal{R}\, \{\mathbb{N}\}$*.*

Ejercicio 8. *Demostrar que si* $(X; \mathcal{R})$ *está bien ordenado, entonces cualquier otro conjunto ordenado,* $(Y; \mathcal{S})$*, y del mismo tipo que* $(X; \mathcal{R})$*, estará asimismo bien ordenado.*

Los números ordinales están asociados precisamente a los tipos de orden de los conjuntos bien ordenados. De igual manera que los cardinales lo están a la relación de equipotencia de conjuntos.

En un conjunto bien ordenado, $(X; \mathcal{R})$*, cada elemento* $a \in X$ *da lugar a un intervalo inicial:*

$$I_X(a) = \{\, x \in X \,;\, x \,\mathcal{R}\, a,\ x \neq a \,\}.$$

En el caso en que $a = m = \min(X)$*, entonces* $I_X(a) = \emptyset$*; pero si* $a \neq m$*, entonces* $m \in I_X(a)$*, y en particular,* $I_X(a) \neq \emptyset$*.*

Ejemplo 3: *En nuestro conjunto bien ordenado favorito,* $(\mathbb{N}; \leq)$*, tenemos que:*

$$I_{\mathbb{N}}(n) = \{0, 1, 2, 3, 4, \ldots, n-1\}.$$

Ejercicio 9. *a) Demostrar que todo conjunto numerable admite un buen orden.*

b) Si $(X;\mathcal{R})$ está bien ordenado, entonces la relación $\mathcal{R}$ induce un buen orden sobre cada intervalo inicial

$$I_X(a) = \{x \in X \mid x\,\mathcal{R}\,a, x \neq a\}.$$

Teorema. ***(Principio de inducción transfinita)*** *Sea $(X;\mathcal{R})$ un conjunto bien ordenado y supongamos que para todo $x \in X$ tenemos una proposición $\varphi(x)$ de manera que $\forall y$ la hipótesis de que $\varphi(x)$ es cierta $\forall x \in I_X(y)$ implica que $\varphi(y)$ es también cierta. Entonces $\varphi(x)$ es cierta para todo $x \in X$.*

Demostración. *Supongamos que el teorema sea falso y sea $F \neq \emptyset$ el conjunto de elementos de X tal que $\varphi(x)$ es falsa. Por ser $(X;\mathcal{R})$ un buen orden podemos considerar $x_0 = \min F$. Ahora bien, $I_X(x_0) \subset X \setminus F$ luego $\varphi(x)$ es cierta $\forall x \in I_X(x_0)$ y la hipótesis de inducción implica que $\varphi(x_0)$ es cierta lo que contradice que $x_0 \in F$.* ■

Proposición. *Una función estrictamente creciente f, del conjunto bien ordenado $(X;\mathcal{R})$ en sí mismo, verifica que $x\,\mathcal{R}\,f(x)$ para todo $x \in X$.*

Demostración. *Consideremos $Z = \{x \in X \mid x \leq f(x)\}$; queremos probar que $Z = X$. Sea x tal que $I_X(x) \subset Z$. Dado $y \in I_X(x)$ resulta que $y \leq f(y) < f(x)$. Luego $y < f(x)$ para todo $y \in I_X(x)$, es decir $f(x) \in X \setminus I_X(x)$ pero como $x = \min\big(X \setminus I_X(x)\big)$ resulta que $x \leq f(x)$. Por lo tanto $x \in Z$ y el principio de inducción transfinita nos permite concluir que $Z = X$.* ■

Corolario. *Si dos conjuntos bien ordenados $(X;\mathcal{R})$ y $(Y;\mathcal{S})$ son isomorfos, o del mismo tipo, el isomorfismo $f : X \longrightarrow Y$ es único.*

Proposición. *El conjunto bien ordenado $(X;\mathcal{R})$ no es equivalente a ninguno de sus intervalos iniciales.*

Demostración. *(Reducción al absurdo). Supongamos que existe una biyección*

$$f : (X;\mathcal{R}) \longrightarrow (I_X(a);\mathcal{R})$$

que preserva el orden. Tendremos que $f(a)\,\mathcal{R}\,a$, $f(a) \neq a$, por lo que el conjunto

$$\{x \in X \mid f(x)\,\mathcal{R}\,x, f(x) \neq x\}$$

será distinto del vacío. Sea z su mínimo. Tenemos que $f(f(z))\,\mathcal{R}\,f(z)$, lo cual contradice la definición de z, a menos que $f(f(z)) = f(z)$. Pero esto tampoco puede ser, ya que f es biyectiva, y como $f(z) \neq z$, no puede ocurrir que $f(f(z)) = f(z)$. ■

Corolario. *Dos intervalos iniciales distintos no pueden ser isomorfos en un conjunto bien ordenado.*

Si $a \mathcal{R} b$, $a \neq b$, entonces $I_X(a)$ es también un intervalo inicial de $(I_X(b); \mathcal{R})$ y por la proposición anterior, no puede ser isomorfo a $I_X(b)$.

Teorema. *Dados dos conjuntos bien ordenados, $(X; \mathcal{R})$, $(Y; \mathcal{S})$, o son isomorfos, o uno es isomorfo a un intervalo inicial del otro.*

Demostración. *Usaremos el símbolo "$\sim$" para designar la isomorfía de conjuntos ordenados.*

Sean $x_0 = \min X$, $y_0 = \min Y$. Tenemos que $I_X(x_0) = I_Y(y_0) = \emptyset$ son trivialmente isomorfos. Sea

$$Z = \{x \in X \mid \exists y \in Y, I_X(x) \sim I_Y(y)\}.$$

Por la observación anterior, $x_0 \in Z$, y así $Z \neq \emptyset$. Además, si $x \in Z$, entonces existe un único $y \in Y$ realizando el isomorfismo de los intervalos correspondientes. Tenemos pues definida una función $y = f(x)$ cuyo dominio es Z:

$$\forall x \in Z,\ \exists ! \, y = f(x),\ I_X(x) \sim I_Y(f(x)).$$

Es fácil ver que f no solo es inyectiva, sino que también preserva el orden.

Demostraremos que el conjunto Z es todo X o un intervalo inicial de X. Dado $x \in Z$ y $x' \mathcal{R} x$, queremos concluir que $x' \in Z$.

Sabemos que $I_X(x) \sim I_Y(f(x))$. Sea φ la función biyectiva que realiza el isomorfismo anterior.

Como $x' \mathcal{R} x$, $I_X(x')$ es un intervalo inicial de $I_X(x)$ y, por lo tanto, la aplicación φ debe transportarlo a un intervalo inicial de $I_Y(f(x))$, que será, por consiguiente, un intervalo inicial del conjunto ordenado $(Y; \mathcal{S})$. Pero eso significa que $x' \in Z$ y, por tanto, Z es un intervalo inicial de X, o todo X.

Análogamente, el conjunto $f(Z)$ es un intervalo inicial de Y, o todo Y, puesto que:

$$f(Z) = \{y \mid \exists x, y = f(x), I_Y(y) \sim I_X(x)\}.$$

Además, la condición $x' \mathcal{R} x$ implica que $I_Y(f(x'))$ es un intervalo inicial de $I_Y(f(x))$ y, por tanto, $f(x') \mathcal{S} f(x)$. Es decir $Z \sim f(Z)$.

Para terminar la demostración, supongamos que $Z \neq X$ y $f(Z) \neq Y$. Luego existen dos elementos $a \in X$, $b \in Y$, tales que $Z = I_X(a)$, $f(Z) = I_Y(b)$. Pero entonces $I_X(a) \sim I_Y(b)$, luego $a \in Z$, y eso es imposible por cuanto $a \notin I_X(a) = Z$. ■

Una consecuencia de este resultado es que los cardinales de dos conjuntos bien ordenados son siempre comparables.

Corolario. *Dados dos conjuntos bien ordenados, $(X; \mathcal{R})$, $(Y; \mathcal{S})$, sus cardinales son comparables. Es decir, una de las tres posibilidades siguientes tiene que darse:*

- *$\mathrm{card}(X) = \mathrm{card}(Y)$, que, por ahora, es simplemente una manera de decir que X e Y son biyectables;*

- *$card(X) < card(Y)$, cuando exista una aplicación inyectiva de X en Y, pero no de Y en X;*
- *$card(Y) < card(X)$, si existe una inyección de Y en X, pero no de X en Y.*

Cabe la pregunta: dados dos conjuntos arbitrarios, X, Y, ¿son sus cardinales comparables? En otras palabras, dados dos conjuntos arbitrarios, X e Y: ¿existirá siempre una aplicación inyectiva de X en Y, de Y en X, o ambas?

Por lo que sabemos, la respuesta es que sí en el caso de que ambos admitan una buena ordenación. ¿Es posible dotar a un conjunto arbitrario de un buen orden? La hipótesis afirmativa es el "principio de buena ordenación". ¿Es creíble? A su favor podemos aducir que todos los conjuntos finitos, o numerables, admiten un buen orden: el inducido por los naturales. En su contra está el hecho de que nadie haya podido encontrar un buen orden para el conjunto de los números reales: ¿pueden ordenarse bien los reales? La respuesta, como en las novelas de intriga, se encuentra en el siguiente párrafo.

7.3. Libertad de elección

> *Finalmente llega a Isidora, ciudad donde los palacios tienen escaleras de caracol incrustadas de caracoles marinos, donde se fabrican según las reglas del arte, largavistas y violines, donde cuando el forastero está indeciso entre dos mujeres encuentra siempre una tercera ...*
>
> Italo Calvino
>
> *(Las ciudades invisibles)*

Disponemos de varias expresiones equivalentes del llamado axioma de elección (A.E.):

1ª Versión. *Dada una familia, $\{X_i\}_{i\in I}$, de conjuntos no vacíos ($X_i \neq \emptyset$, $\forall i \in I$), existe una función de elección:*

$$s : \{X_i\}_{i\in I} \longrightarrow \bigcup X_i$$

de manera que $s(X_i) \in X_i$, $\forall i \in I$.

2ª Versión. *Dado un conjunto, $X \neq \emptyset$, existe una función:*

$$s : \mathcal{P}(X) - \{\emptyset\} \longrightarrow X$$

de manera que $s(A) \in A$, $\forall A \subset X$, $A \neq \emptyset$.

3ª Versión. *Si $\{X_i\}_i \in I$ es una familia de conjuntos no vacíos, entonces su producto cartesiano, $\prod X_i$, es distinto del vacío.*

La equivalencia de estas tres versiones es casi evidente. También parece fácil aceptarlas como postulados válidos. Por ello no deja de ser sorprendente que el axioma de elección (A.E.) sea equivalente al principio de buena ordenación (P.B.O.).

Antes de entrar de lleno en el análisis de esta inquietante equivalencia, conviene constatar que hay otra proposición, llamada el lema de Zorn, cuyo enunciado es algo más complicado que A.E. y P.B.O., pero que, sin embargo, es equivalente a ellos y desempeña también un papel destacado en esta historia.

Definición. *Diremos que un conjunto parcialmente ordenado, $(X; \mathcal{R})$, es inductivo si toda cadena (subconjunto totalmente ordenado), tiene una cota superior.*

Lema de Zorn. *(L.Z.) Todo conjunto inductivo tiene un elemento maximal.*

El lema de Zorn es un instrumento poderoso de demostración en muchas situaciones en las que es preciso considerar familias infinitas de conjuntos. Un ejemplo notable es la prueba de que todo espacio vectorial tiene siempre una base, es decir, un conjunto de generadores linealmente independiente. Tal propiedad se demuestra con facilidad en el caso de dimensión finita. Sin embargo, cuando el espacio vectorial, V, tiene infinitas dimensiones hay que echar mano del L.Z. Pero en las matemáticas existen muchos casos interesantes de espacios vectoriales de infinitas dimensiones. Un ejemplo es el de todas las funciones continuas del intervalo $[0,1]$ en $\mathbb{R}$; otro es el propio $\mathbb{R}$ considerado como espacio vectorial sobre el cuerpo $\mathbb{Q}$.

Proposición. *Todo espacio vectorial tiene una base.*

Demostración. *En el espacio vectorial V (sobre un cuerpo K, tal como $\mathbb{Q}$, $\mathbb{R}$ o los complejos $\mathbb{C}$), consideremos el conjunto $\mathcal{F}$ de todos los subconjuntos linealmente independientes.*

Recordemos que la independencia lineal de $A \subset V$ significa que si tenemos $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$, $\lambda_j \in K$, $x_j \in A$, $\forall j = 1, \ldots, n$, entonces, necesariamente, se verifica que $\lambda_1 = \cdots = \lambda_n = 0$.

El conjunto $\mathcal{F}$ está ordenado a través de la relación de inclusión de conjuntos. Sea $\mathcal{C} = \{A_i\}_{i \in I}$ una cadena de $\mathcal{F}$, entonces $A = \bigcup A_i$ es una cota superior de $\mathcal{C}$:

Tenemos que $A_i \subset A$, $\forall i \in I$, siendo A el subconjunto menor de V que tiene esta propiedad. Luego solo resta comprobar que A es linealmente independiente para tener una cota superior de $\mathcal{C}$.

Sea $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$, donde cada x_j es un elemento de A. De la definición de $A = \bigcup A_i$, se deduce que cada x_j pertenece a un cierto A_{i_j}, pero por ser $\mathcal{C}$ una cadena, los $A_{i_1}, \ldots, A_{i_n}$ están totalmente ordenados por la inclusión.

Luego hay uno de ellos, digamos A_{i_k}, que contiene a todos los demás. Resulta, por lo tanto, que $\{x_1, \ldots, x_n\} \subset A_{i_k}$, y la independencia lineal de A_{i_k} implica que $\lambda_1 = \cdots = \lambda_n = 0$, que es lo que queríamos demostrar.

Toda cadena tiene pues una cota superior, y el lema de Zorn nos asegura la existencia de un elemento maximal, B. Queremos demostrar que B es una base de V.

Supongamos lo contrario: existirá entonces un elemento, x, que no es combinación lineal de los elementos de B. Pero, en este caso, el conjunto $B_1 = B \cup \{x\}$ seguirá siendo linealmente independiente y como $B \subset B_1$, $B \neq B_1$, se contradice el carácter maximal de B. Eso nos permite concluir la demostración. ■

Hay otros muchos resultados matemáticos importantes que son consecuencia del lema de Zorn. Un ejemplo notable es el teorema de Hahn–Banach del Análisis Funcional; otro es el teorema de Tijonov de la Topología Conjuntista. Pero un aspecto destacable de las demostraciones basadas en el L.Z. es que no son "constructivas". Es decir, nos aseguran la existencia de algo (en nuestro ejemplo una base del espacio), pero no nos abastecen con un método para obtenerlo o construirlo.

Es un hecho notable que el L.Z. sea equivalente al A.E. y al P.B.O. De manera que si aceptamos alguno de ellos como válido, tenemos que aceptar, necesariamente, a los otros dos.

Principio de buena ordenación $\Longrightarrow$ Axioma de elección

Dado X según el P.B.O. hay un buen orden $\mathcal{R}$ en X. Eso nos permite definir la función de elección siguiente: Dado $A \subset X$, $A \neq \emptyset$,

$$S(A) = \text{mín}(A).$$

Lema de Zorn $\Longrightarrow$ Principio de buena ordenación

Dado X consideremos la familia $\mathcal{F}$ de las parejas $(A; \mathcal{R})$, donde $A \subset X$ es no vacío y $\mathcal{R}$ es un buen orden en A.

Diremos que $(A; \mathcal{R}) \leq (B; \mathcal{S})$, *si* $A \subset B$, $\mathcal{S}$ *restringido a* A *coincide con* $\mathcal{R}$, *y todos los elementos de* $B - A$ *son posteriores en* $\mathcal{S}$ *a todos los miembros de* A.

Sea $\mathcal{C} = \{(A_i; \mathcal{R}_i)\}_{i \in I}$ *una cadena de* $\mathcal{F}$. *Es fácil ver que* $(A; \mathcal{R})$ *es una cota superior de* $\mathcal{C}$, *donde:*

$$\begin{cases} A = \bigcup A_i \\ a \mathcal{R} b \text{ si } a \mathcal{R}_i b \text{ para } i \in I. \end{cases}$$

Por el lema de Zorn existe un elemento maximal $(M; \mathcal{R})$. *La demostración se acaba observando que* $M = X$.

Supongamos lo contrario: sea $x \in X \setminus M$ *y consideremos* $\overline{M} = M \cup \{x\}$ *con el orden* $\overline{\mathcal{R}}$ *dado por:*

$$\begin{cases} \text{si } a, b \in M \text{ entonces } a \overline{\mathcal{R}} b \text{ si y solo si } a \mathcal{R} b; \\ \text{si } a \in M \text{ entonces } a \overline{\mathcal{R}} x. \end{cases}$$

Resulta entonces que $\overline{\mathcal{R}}$ *es un buen orden en* $\overline{M}$, *por lo que* $(M; \mathcal{R}) \leq (\overline{M}; \overline{\mathcal{R}})$ *contradice el carácter maximal de* $(M; \mathcal{R})$.

Para acabar la anunciada equivalencia, nos resta demostrar que A.E. $\Rightarrow$ *L.Z. Esta es quizá la más onerosa de las tres implicaciones y nos apoyaremos en el lema siguiente.*

Lema clave. *Sea* $\mathcal{F}$ *una colección no vacía de subconjuntos de un conjunto no vacío* X. *En* $\mathcal{F}$ *tenemos el orden de la inclusión, para el que supondremos que la unión de toda cadena* $\mathcal{C}$ *de* $\mathcal{F}$ *está también en* $\mathcal{F}$. *Supongamos además que* $\varphi : \mathcal{F} \longrightarrow \mathcal{F}$ *es una función tal que* $A \subset \varphi(A)$ *y que* $\varphi(A) \setminus A$ *contiene, a lo más, un único elemento, cualquiera que sea* $A \in \mathcal{F}$. *Entonces, existe* $A \in \mathcal{F}$ *tal que* $\varphi(A) = A$.

Dejemos la demostración del lema clave para después. Con su ayuda estamos en condiciones de ver que A.E. $\Rightarrow$ *L.Z.*

Axioma de elección $\Longrightarrow$ *Lema de Zorn*

Sea $(X; \mathcal{R})$ *un conjunto inductivo y sea* $\mathcal{F}$ *la colección de todas las cadenas de* X.

$\mathcal{F}$ *es no vacía, ya que cada elemento* $x \in X$ *da lugar a la cadena* $\{x\}$. *Observemos que la unión de una cadena de conjuntos totalmente ordenados está totalmente ordenada. El axioma de elección postula la existencia de una función* S *de elección, tal que* $S(A) \in A$, *para todo* $A \subset X$, $A \neq \emptyset$.

Para $E \in \mathcal{F}$ *sea* E^* *el conjunto de todos los elementos* $x \in X \setminus E$ *tales que* $E \cup \{x\} \in \mathcal{F}$.

Si $E^* \neq \emptyset$ hacemos $\varphi(E) = E \cup \{S(E^*)\}$. Si $E^* = \emptyset$, hacemos que $\varphi(E) = E$.

Estamos en las condiciones del lema clave y, por consiguiente, existe un subconjunto $E \in \mathcal{F}$ tal que $\varphi(E) = E$; es decir $E^* = \emptyset$. Pero eso quiere decir que E es una cadena maximal de elementos de X. Por ser $(X; \mathcal{R})$ inductivo, E tendrá una cota superior, x, que, necesariamente, es un elemento maximal en $(X; \mathcal{R})$, ya que, en caso contrario, habría un elemento $y \neq x$, tal que $x \mathcal{R} y$. Pero entonces el conjunto $\overline{E} = E \cup \{y\}$ sería una cadena estrictamente mayor, en contra del carácter maximal de E.

Demostración del lema clave. *Fijemos un elemento $A_0 \in \mathcal{F}$. Diremos que un subconjunto $\mathcal{G} \subset \mathcal{F}$ es una tribu, si goza de las propiedades siguientes:*

i) $A_0 \in \mathcal{G}$;

ii) *si* $\mathcal{C} = \{C_i\}_{i \in I}$ *es una cadena contenida en* $\mathcal{G}$, *entonces* $C = \bigcup C_i \in \mathcal{G}$;

iii) $A \in \mathcal{G} \Longrightarrow \varphi(A) \in \mathcal{G}$.

La colección de todos los elementos de $\mathcal{F}$ que contienen a A_0 es una tribu.

Sea $\mathcal{F}_0$ la intersección de todas las tribus. Es fácil ver que $\mathcal{F}_0$ es también una tribu, la más pequeña de todas. Vamos a demostrar que $\mathcal{F}_0$ es, además, una cadena de $\mathcal{F}$.

Diremos que un elemento $C \in \mathcal{F}_0$ es un cronopio si es comparable con cualquier otro elemento de $\mathcal{F}_0$: para todo $A \in \mathcal{F}_0$, o bien $A \subset C$, o bien $C \subset A$. Sea $\mathcal{K}$ la colección de todos los cronopios.

Dado $C \in \mathcal{K}$ consideremos el conjunto

$$\mathcal{F}_0(C) = \big\{A \in \mathcal{F}_0 \,:\, (A \subset C) \vee (\varphi(C) \subset A)\big\}.$$

Si $A \in \mathcal{F}_0(C)$ tenemos tres posibilidades, no necesariamente excluyentes:

1. $A \subset C$ *y* $A \neq C$;
2. $A = C$;
3. $\varphi(C) \subset A$.

En el primer caso, ($A \subset C$ y $A \neq C$), observemos que C no puede ser un subconjunto propio de $\varphi(A)$. Eso implicaría que $\varphi(A) - A$ tendría, al menos, dos elementos. Como C es un cronopio tenemos que $\varphi(A) \subset C$.

Si $A = C$, entonces $\varphi(A) = \varphi(C)$.

Finalmente, si $\varphi(C) \subset A$, entonces $\varphi(C) \subset \varphi(A)$.

Resumiendo lo anterior, hemos probado que si $A \in \mathcal{F}_0(C)$, entonces $\varphi(A)$ también está en $\mathcal{F}_0(C)$. Luego $\mathcal{F}_0(C)$ es una tribu, y como $\mathcal{F}_0$ es la más pequeña de todas las tribus, resulta que $\mathcal{F}_0(C) = \mathcal{F}_0$ para todo cronopio C.

En otras palabras, si $A \in \mathcal{F}_0$ y $C \in \mathcal{K}$ entonces, o bien $A \subset C$, o bien $\varphi(C) \subset A$. Pero esto implica que $\varphi(C) \in \mathcal{K}$ y $\mathcal{K}$ es una tribu contenida en $\mathcal{F}_0$, la menor de ellas, luego $\mathcal{K} = \mathcal{F}_0$ y $\mathcal{F}_0$ está totalmente ordenado, por ser un conjunto de cronopios, por lo que $\mathcal{F}_0$ es una cadena, como pretendíamos probar.

Sea A la unión de todos los elementos de $\mathcal{F}_0$. Por la propiedad ii) resulta que $A \in \mathcal{F}_0$, y por iii), $\varphi(A) \in \mathcal{F}_0$. Pero por ser A el mayor conjunto de $\mathcal{F}_0$ y $A \subset \varphi(A) \in \mathcal{F}_0$ se concluye que $A = \varphi(A)$. ■

El axioma de elección es usado muchas veces de manera implícita. Por ejemplo, para encontrar la inversa por la derecha a una aplicación sobreyectiva: dada una tal aplicación f de X en Y, podemos definir una función inyectiva g de Y en X escogiendo, para cada y de Y, un elemento x de X tal que $f(x) = y$, y eso garantiza que g sea inyectiva y verifique $f(g(y)) = y$, para todo y de Y. Sin embargo, ese procedimiento supone elegir un elemento en cada uno de los (infinitos) conjuntos $f^{-1}(y)$ lo que solo puede hacerse con el axioma de elección.

El que nadie haya podido encontrar un buen orden en $\mathbb{R}$ alimenta el escepticismo en torno al P.B.O. Aunque su equivalencia con el A.E., más claro y de mejor reputación, refuerza la actitud de aceptarlo sin más. Pero las cosas no son tan simples, como los ejemplos siguientes tratan de ilustrar.

El problema de la medida

La teoría de la medida trata de construir una función μ que asigne a cada subconjunto acotado de la recta real un número no–negativo (su medida), de manera que se satisfagan ciertas reglas que postulamos han de verificar las medidas:

1. *Positividad: $\mu(A) \geq 0$ para todo subconjunto acotado de $\mathbb{R}$.*
2. *Aditividad: Si $\{A_n\}$ es una sucesión de subconjuntos acotados de $\mathbb{R}$ disjuntos dos a dos, entonces:*
$$\mu\Big(\bigcup A_n\Big) = \sum_{n=1}^{\infty} \mu(A_n).$$
3. *Unidad de medida: $\mu([0,1)) = 1$.*
4. *Invarianza por traslaciones: Para todo conjunto acotado, A, y todo número real, x, se verifica que $\mu(x + A) = \mu(A)$, donde $x + A = \{x + y \mid y \in A\}$.*

Estas reglas o axiomas de la medida en $\mathbb{R}$ son muy naturales y reflejan las propiedades del acto de medir longitudes. Por ejemplo, combinándolas adecuadamente, obtenemos que $\mu([a,b)) = b-a$, para cualesquiera números reales $a < b$. Otra propiedad es que si $A \subset B$, entonces $\mu(A) \leq \mu(B)$. Creo que resulta sorprendente que el Axioma de Elección impida la existencia de una tal teoría de la medida.

Proposición. *Según el Axioma de Elección, existe un subconjunto acotado de $\mathbb{R}$ que no es medible.*

Demostración. *En el intervalo real $[0,1)$, definimos la siguiente relación:*

$$x \mathcal{R} y \iff x - y \text{ es racional.}$$

Es fácil ver que $\mathcal{R}$ es una relación de equivalencia, por lo que divide al intervalo $[0,1)$ en una unión disjunta de clases de equivalencia:

$$[0,1) = \bigcup_{i \in I} E_i.$$

El Axioma de Elección nos permite considerar un conjunto, $E = \{e_i\}_{i \in I}$, que tiene un único elemento en cada clase E_i:

$$E \cap E_i = \{e_i\}.$$

Sea $q_1, q_2, q_3, \ldots, q_n, \ldots$, una numeración del conjunto numerable de los racionales del intervalo $[-1,1)$. Tenemos que:

$$[0,1) \subset \bigcup_{n=1}^{\infty} (q_n + E) \subset [-1,2).$$

Obsérvese que cada $x \in [0,1)$ pertenece a una clase, digamos E_i, de manera que $x - e_i$ es un racional mayor que -1 y menor que 1. Por tanto

$$x \in q_n + E \text{ para algún } q_n \in [-1,1).$$

En el otro sentido, observemos que $E \subset [0,1)$, por lo que $q_n + E \subset [-1,2)$, de aquí que

$$\bigcup_{n=1}^{\infty} (q_n + E) \subset [-1,2).$$

Además, si $q_n \neq q_m$, entonces $(q_n + E) \cap (q_m + E) = \emptyset$.

Si el conjunto E fuera medible, su medida, $\mu(E)$, tendría dos posibilidades:

$$(\mu(E) = 0) \vee (\mu(E) > 0).$$

Veremos que ambas producen una contradicción.

En efecto:

i) *Si* $\mu(E) = 0$ *entonces*

$$1 = \mu([0,1)) \leq \mu\big(\bigcup(q_n + E)\big) = \sum \mu(q_n + E) = \sum \mu(E) = 0,$$

esto es, $1 \leq 0$ *(absurdo).*

ii) *Si* $\mu(E) > 0$, *entonces*

$$\infty = \sum \mu(q_n + E) = \mu\big(\bigcup(q_n + E)\big) \leq \mu([-1,2)) = 3,$$

de otra manera, $\infty \leq 3$ *(absurdo).* ■

Luego el A.E. nos impide tener una teoría de la medida para todos los subconjuntos acotados de $\mathbb{R}$. *No obstante, se sabe que tal teoría sí es compatible con el Axioma de Elección numerable. Esto es porque con solo ese axioma no existe el conjunto* E *antes descrito. Es decir, que según adoptemos uno u otro axioma variará también la clase de los subconjuntos de la recta real: "¡conjuntos que existen con A.E. dejan de hacerlo cuando nos restringimos al A.E. numerable!".*

El resultado siguiente, conocido como la Paradoja de Banach-Tarski, es quizá un giro de tuerca en esta historia fascinante. Se trata de lo siguiente:

Sea B_1 *la bola unidad del espacio euclídeo tridimensional* $\mathbb{R}^3$*:*

$$B_1 = \big\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 \leq 1\big\}.$$

El A.E. permite demostrar la existencia de una partición de B_1 *en un número finito de conjuntos disjuntos dos a dos:* $B_1 = A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1} \cup \cdots \cup A_{2n}$. *De tal manera que tanto los* $A_1, \ldots, A_n$, *como los* $A_{n+1}, \ldots, A_{2n}$, *después de trasladarlos y rotarlos, producen otra bola unidad:*

$$B_1 = A_1^* \cup \cdots \cup A_n^*$$
$$B_1 = A_{n+1}^* \cup \cdots \cup A_{2n}^*,$$

donde A_j^* *es el resultado de trasladar y rotar* A_j.

Lo paradójico del resultado no radica en la demostración, que es clara, nítida y diamantina (aunque basada en el A.E.), sino en la perplejidad de su conclusión. Obsérverse, no obstante, que no hay ninguna contradicción, por cuanto los trozos A_j *son conjuntos no medibles. Así es que no podemos inferir que*

$$\mu(B_1) = 2\,\mu(B_1)$$

a través de la cadena de identidades:

$$\begin{aligned}\mu(B_1) &= \sum_1^{2n}\mu(A_j) = \sum_1^{n}\mu(A_j) + \sum_{n+1}^{2n}\mu(A_j)\\ &= \sum_1^{n}\mu(A_j^*) + \sum_{n+1}^{2n}\mu(A_j^*) = \mu\big(\bigcup_{j=1}^{n}A_j^*\big) + \mu\big(\bigcup_{j=n+1}^{2n}A_j^*\big)\\ &= \mu(B_1) + \mu(B_1),\end{aligned}$$

ya que no existen las cantidades comprendidas entre $\mu(B_1)$ *y* $\mu(B_1)+\mu(B_1)$.

Por lo tanto no hay contradicción, sino tan solo la perplejidad basada en el uso del A.E. no numerable que, por estas y otras razones, la mayoría de los matemáticos procura evitar. Hay quien describe este resultado en términos bíblicos, por aquello de la multiplicación de los panes y los peces. Aunque hay que usar un cuchillo mágico, que divida en pedazos no medibles.

Pero concluyamos antes de que se nos pueda aplicar lo que el escritor Borges escribió del filósofo Descartes: "Yo creo que el rigor de Descartes era aparente o ficticio. Y eso se nota en el hecho de que parte de un pensamiento riguroso y al final llega a algo tan extraordinario como la fe católica. Parte del rigor y llega al Vaticano".

7.4. Los ordinales

Según Cantor los números ordinales son los tipos de orden de los conjuntos bien ordenados. Pero hay que tener cuidado porque la clase de los conjuntos bien ordenados no es un conjunto (tampoco lo es la de los que tienen el mismo tipo que un conjunto bien ordenado fijado de antemano) y nos encontraríamos con otra versión de la paradoja de Russell de seguir por ese camino. No obstante, John von Neumann tuvo la idea de definir los ordinales escogiendo adecuadamente un elemento en cada clase de equivalencia:

Definición. *Un conjunto* α *es un número ordinal (o simplemente un ordinal) si tiene las propiedades siguientes:*

$P_1(\alpha)$: *Si* $\beta \in \alpha$ *entonces* $\beta \subset \alpha$.

$P_2(\alpha)$: $\big[(\beta \in \alpha) \wedge (\gamma \in \alpha)\big] \implies \big[\beta = \gamma) \vee (\beta \in \gamma) \vee (\gamma \in \beta)\big]$.

$P_3(\alpha)$: *Si* $\emptyset \neq A \subset \alpha$, *entonces existe* $\gamma \in A$ *tal que* $\gamma \cap A = \emptyset$.

Observemos que si en $P_3(\alpha)$ *tomamos* $A = \alpha$, *se tiene, debido a* $P_1(\alpha)$:

$$\big[(\gamma \in \alpha) \wedge (\gamma \cap \alpha = \emptyset)\big] \Longrightarrow \gamma = \emptyset.$$

Luego todo ordinal α, *distinto del vacío, contiene al vacío como elemento.*

Ejercicio 10. *Demostrar que si α es un ordinal entonces el conjunto $\alpha \cup \{\alpha\}$ es también un ordinal (que será designado luego por $\alpha + 1$).*

Ejemplos: *El ordinal 0 es simplemente el conjunto vacío $\emptyset$:*

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{\emptyset\} = \{0\} \\ 2 &= \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\ 3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} \\ &\cdots\cdots \\ n+1 &= \{0, 1, 2, \ldots, n\} \end{aligned}$$

En otras palabras cada ordinal es el conjunto de los ordinales anteriores a él. También en el caso no finito:

$$\begin{aligned} \omega &= \mathbb{N} \\ \omega + 1 &= \{\mathbb{N}, \{\mathbb{N}\}\} = \{\omega, \{\omega\}\} \\ \omega + 2 &= \{\mathbb{N}, \{\mathbb{N}\}, \{\mathbb{N}, \{\mathbb{N}\}\}\} = \{\omega, \omega + 1\} \\ &\cdots\cdots \end{aligned}$$

Ejercicio 11. *Comprobar que cada conjunto α de la lista anterior satisface las tres propiedades $P_1(\alpha)$, $P_2(\alpha)$, $P_3(\alpha)$ que definen los ordinales.*

De esta guisa volvemos a encontrarnos con los números naturales en su versión ordinal 1 (uno) primero; 2 (dos) segundo; ... ; 1999 (mil novecientos noventa y nueve) milésimo noningentésimo nonagésimonono... Mención aparte merece el cero del que carecemos de una denominación propiamente ordinal. Solemos empezar a contar por uno, pero, en Matemáticas (y también en la cronología, como puso de manifiesto la polémica sobre el año de inicio del nuevo milenio) resulta a veces conveniente empezar contando por el cero. Entonces el cardinal del conjunto hay que obtenerlo sumando uno al último ordinal adjudicado a sus elementos. Carecer de un término apropiado para el ordinal cero es algo común a la mayoría de los idiomas. Hubo, no obstante, un español que hizo una propuesta al respecto. Se trata del afamado torero Rafael Guerra, "Guerrita", quien preguntado sobre el escalafón de su oficio respondió: "dempués de mí, naide, y dempués de naide, el Fuentes". "Naide" o quizás "naidero" podría muy bien ser el cero ordinal en castellano.

Proposición. *Si α es un ordinal y $\beta \in \alpha$ entonces β es también un ordinal.*

Demostración. *Por ser α ordinal la propiedad $P_1(\alpha)$ implica que $\beta \subset \alpha$: esto nos da automáticamente las propiedades $P_2(\beta)$ y $P_3(\beta)$.*

En cuanto a $P_1(\beta)$ *dado* $\gamma \in \beta$ *tenemos que demostrar que* $\gamma \subset \beta$, *es decir:*

$$\big(\delta \in \gamma\big) \implies \big(\delta \in \beta\big).$$

Ahora bien, tales δ *y* β *están en* α *por lo que tendremos una de las tres posibilidades siguientes:* $\delta \in \beta$, $\beta \in \delta$ *o* $\delta = \beta$. *Y la demostración se acaba probando que no pueden darse los casos* $\beta \in \delta$ *o* $\delta = \beta$.

i) Si $\beta \in \delta$ *entonces* $\beta \in \delta \in \gamma \in \beta$, *y la propiedad* $P_3(\alpha)$ *fallaría para el conjunto*

$$B = \big\{\beta, \delta, \gamma\big\} \neq \emptyset$$

ya que:

$$\delta \in \gamma \cap B \neq \emptyset$$
$$\beta \in \delta \cap B \neq \emptyset$$
$$\gamma \in \beta \cap B \neq \emptyset.$$

ii) Análogamente $\big(\beta = \delta\big) \implies \big(\beta \in \gamma \in \beta\big)$ *y* $P_3(\alpha)$ *fallaría para el conjunto*

$$B = \big\{\gamma, \beta\big\}.$$

■

Observemos que si α *es un ordinal y* β, γ *son dos de sus elementos entonces:*

$$\big(\gamma \subset \beta\big) \iff \big[(\gamma = \beta) \vee (\gamma \in \beta)\big].$$

Esto es debido a que por ser β, γ *elementos de* α *ha de verificarse una de las tres posibilidades siguientes:* $(\beta = \gamma) \vee (\gamma \in \beta) \vee (\beta \in \gamma)$. *Por lo que*

$$\big[(\gamma \subset \beta) \wedge (\beta \in \gamma)\big] \implies \big[(\gamma \subset \beta) \wedge (\beta \subset \gamma)\big] \implies \big[\beta = \gamma\big].$$

Luego la inclusión de conjuntos "$\subset$*" es un orden total en el número ordinal* α.

Proposición. *Dado un ordinal* α *la inclusión entre sus elementos es un buen orden.*

Demostración. *Basta con ver que todo subconjunto distinto del vacío tiene un elemento mínimo.*

Sea $\emptyset \neq B \subset \alpha$. *Por la propiedad* $P_3(\alpha)$ *existe* $\gamma \in B$ *tal que*

$$\gamma \cap B = \emptyset.$$

Tenemos que $\gamma = \min B$ *ya que dado* $\beta \in B$, *por la propiedad* $P_2(\beta)$, *ha de verificarse que* $(\beta = \gamma) \vee (\beta \in \gamma) \vee (\gamma \in \beta)$. *Pero* $(\beta \in \gamma) \implies \big[\beta \in \gamma \cap B = \emptyset\big]$ *luego* $\gamma \subset \beta$, $\forall \beta \in B$. ■

Notación: *Conviene designar por el símbolo "*$\leq$*" la relación "*$\subset$*" entre los elementos de un número ordinal. Entonces la relación* $\gamma \in \beta$ *puede ser descrita por "*$<$*", que es el símbolo de la desigualdad estricta. En lo sucesivo*

consideraremos siempre un número ordinal como un conjunto α que además de verificar los postulados $P_1(\alpha)$, $P_2(\alpha)$ y $P_3(\alpha)$, es un conjunto bien ordenado por la relación "$\leq$" entre sus elementos.

Proposición. *Dos números ordinales α y β del mismo tipo son iguales.*

Demostración. *Sea $f : \alpha \longrightarrow \beta$ un isomorfismo que preserva el orden. Tenemos que $f(0) = 0$. Sea*

$$\emptyset \neq Z = \big\{\gamma \in \alpha \mid f(\gamma) = \gamma\big\}.$$

Procederemos por inducción transfinita: Supongamos que $I_\alpha(\gamma) \subset Z$. Como f preserva el orden resulta que

$$f\big(I_\alpha(\gamma)\big) = I_\beta\big(f(\gamma)\big).$$

Como $f(\delta) = \delta$ para todo $\delta < \gamma$ resulta que

$$f(\gamma) = I_\beta\big(f(\gamma)\big) = f\big(I_\alpha(\gamma)\big) = \big\{\delta < \gamma\big\} = \gamma.$$

Es decir $\gamma \in Z$. Por el teorema de inducción transfinita $Z = \alpha$ y, por tanto, $\alpha = \beta$ y f es la identidad. ■

Dado un número ordinal α cualquier intervalo inicial suyo $I_\alpha(\beta)$ es un número ordinal (puesto que verifica los axiomas P_1, P_2 y P_3) que es del mismo tipo que β. Luego si $\beta \in \alpha$: $\beta = I_\alpha(\beta)$.

Consideremos ahora dos ordinales distintos α, β. Sabemos que uno de ellos es del mismo tipo que un intervalo inicial del otro, luego: dados dos ordinales α y β ora $\alpha \leq \beta$ ya $\beta \leq \alpha$. La relación "$\leq$" es un orden total en cualquier conjunto de ordinales. Pero, ¡cuidado!, no existe el conjunto de todos los números ordinales.

Si α es un ordinal y consideramos $\alpha + 1 = \alpha \cup \{\alpha\}$, entonces cualquier ordinal β tal que $\alpha < \beta$ verifica que $\alpha+1 \leq \beta$ y, por tanto, resulta conveniente llamar a $\alpha + 1$ el sucesor de α: "Todo ordinal tiene un sucesor".

Proposición. *La unión de un conjunto de ordinales es un ordinal.*

Demostración. *Sea Ω un conjunto de ordinales y consideremos su unión: $\theta = \bigcup_{\omega\in\Omega} \omega$. Queremos ver que θ satisface las propiedades $P_j(\theta)$, $j = 1, 2, 3$:*

$\underline{P_1(\theta)}$: si $\beta \in \theta$ entonces $\exists\omega \in \Omega$ tal que $\beta \in \omega$ luego $\beta \subset \omega$ y, por tanto, $\beta \subset \theta = \bigcup_{\omega\in\Omega} \omega$.

$\underline{P_2(\theta)}$: Si $\beta, \gamma \in \theta$ entonces $\exists\omega_1, \omega_2 \in \Omega$ tales que $(\beta \in \omega_1) \wedge (\gamma \in \omega_2)$. Ahora bien, los ordinales verifican que $\omega_1 \leq \omega_2$ o $\omega_2 \leq \omega_1$, es decir:

$$(\omega_1 = \omega_2) \wedge (\omega_1 \in \omega_2) \wedge (\omega_2 \in \omega_1).$$

Luego uno de los dos ω_j verifica que $\beta \in \omega_j$, $\gamma \in \omega_j$ y, por tanto: $(\beta = \gamma) \vee (\beta \in \gamma) \vee (\gamma \in \beta)$.

$\underline{P_3(\theta)}$: *Sea* $\emptyset \neq A \subset \theta$ *y sea* $\alpha \in A$. *Sabemos que* α *es un ordinal. Si* $\alpha \cap A = \emptyset$ *entonces tenemos probada la propiedad. En caso contrario sea* $\gamma = \min(\alpha \cap A)$ *cuya existencia está asegurada por la propiedad* $P_3(\alpha)$. *Tenemos que* $\gamma \cap A = \emptyset$, *lo que nos permite concluir la demostración.* ■

Teorema. *Todo conjunto bien ordenado* $(X; \mathcal{R})$ *es del mismo tipo que un ordinal* α.

Demostración. *El ordinal de* $(X; \mathcal{R})$ *es único ya que si* $(X; \mathcal{R})$ *fuese del mismo tipo que los ordinales* α *y* β, *estos tendrían que ser iguales, por ser ambos también del mismo tipo.*

Sea $\widetilde{I}(x) = \{y \in X \mid y \,\mathcal{R}\, x\} = I_X(x) \cup \{x\}$ *y consideremos el conjunto:*

$$Z = \{x \in X \mid \widetilde{I}(x) \text{ es del mismo tipo que un ordinal } \omega_x\}.$$

Sabemos que si $m = \min X$ *entonces* $\widetilde{I}(m) = \{m\}$ *es del mismo tipo que el ordinal* 1: *luego* $Z \neq \emptyset$. *Queremos probar que* $Z = X$ *usando inducción transfinita.*

Supongamos pues que $I_X(x) \subset Z$: *Dado* $y \in I_X(x)$ *existe un único isomorfismo*

$$f_y : \widetilde{I}(y) \longrightarrow \omega_y$$

de los conjuntos $\widetilde{I}(y)$ *y el ordinal* ω_y. *Si* $z \,\mathcal{R}\, y$ *entonces* $f_y/\widetilde{I}(z) = f_z$. *Consideremos el ordinal* $\omega = \bigcup_{y \in I_X(x)} \omega_y$ *y el isomorfismo*

$$f : I_X(x) \longrightarrow \omega$$

dado por $f(y) = f_y(y)$ *que podemos extender de la forma:*

$$\begin{aligned} \overline{f} : \widetilde{I}(x) &\longrightarrow \omega \cup \{\omega\} \\ \overline{f}(y) &= f(y)\,, \quad \forall y \in I_X(x) \\ \overline{f}(x) &= \{\omega\}. \end{aligned}$$

Esto prueba que $x \in Z$ *y, por inducción transfinita,* $X = Z$. *Finalmente* X *es isomorfo a* $\bigcup_x \omega_x$ *por el isomorfismo* $f(y) = f_y(y)$. ■

Aritmética ordinal

Entre los números ordinales podemos definir una suma y un producto de la manera siguiente:

La suma $\alpha + \beta$ *es el ordinal que corresponde al tipo del conjunto* $\big(\{0\} \times \alpha\big) \cup \big(\{1\} \times \beta\big)$ *con el orden:*

$$(m, \gamma) \leq (n, \delta) \quad \Longleftrightarrow \quad \big(m < n\big) \vee \big[\big(m = n\big) \wedge \big(\gamma \leq \delta\big)\big].$$

El producto $\alpha\,\beta$ *es el tipo correspondiente al producto cartesiano* $\beta \times \alpha$ *con el orden alfabético:*

$$(\beta_1, \alpha_1) \leq (\beta_2, \alpha_2) \quad \Longleftrightarrow \quad \big(\beta_1 < \beta_2\big) \vee \big[\big(\beta_1 = \beta_2\big) \wedge \big(\alpha_1 \leq \alpha_2\big)\big].$$

Ejercicios

1) *Demostrar que* $\alpha + 1 = \alpha \cup \{\alpha\}$.

2) *Sea* $\omega = \mathbb{N}$ *el tipo de orden del conjunto de los naturales con la relación "*$\leq$*". Demostrar que* $1 + \omega = \omega \neq \omega + 1$.

3) *Demostrar que el ordinal* $\omega\,2 = \omega + \omega$ *es distinto del* $2\,\omega = \omega$.

4) *Demostrar las implicaciones siguientes* $\forall\gamma$, α *y* β *ordinales:*

$$\begin{aligned} \big(\alpha < \beta\big) &\implies \big(\gamma + \alpha < \gamma + \beta\big) \\ \big(\alpha \leq \beta\big) &\implies \big(\alpha + \gamma \leq \beta + \gamma\big). \end{aligned}$$

5) *¿Es cierto que si* $\alpha > 0$ *se verifica que* $\gamma < \alpha + \gamma$*?*

6) *Probar que si* $\alpha \geq \beta$ *entonces existe un único ordinal* γ *tal que* $\alpha = \beta + \gamma$.

— 8 —

Los cardinales: construcción y deconstrucción

Porque parece mentira
la verdad nunca se sabe.

Daniel Sada

Que los conjuntos X, Y tienen la misma cardinalidad, $card(X) = card(Y)$, ha sido hasta ahora una manera de decir que son biyectables. Por el Principio de buena ordenación sabemos que un conjunto X siempre admite un buen orden $\mathcal{R}$ y que el par ordenado $(X; \mathcal{R})$ será del mismo tipo que un único ordinal α. Pero en general tendremos muchos órdenes en X que serán de tipos ordinales distintos. Es decir que un mismo conjunto (infinito) contado de una forma o de otra puede dar resultados (tipos de orden) bien distintos. Un ejemplo son los naturales $\mathbb{N}$. Contados con el orden $\leq$ sale el ordinal que hemos llamado ω. Pero en $\mathbb{N}$ tenemos también este otro orden:

i) Si a y b son distintos de 0 entonces

$$a \mathcal{R} b \iff a \leq b$$

ii) $a \mathcal{R} 0$ $\forall a \in \mathbb{N}$.

Resulta que el tipo de orden $(\mathbb{N}; \mathcal{R})$ es $\omega + 1 \neq \omega$.

Para arreglar este desaguisado necesitamos definir los cardinales.

Definición. $card(X) = \min \{\alpha : \alpha \text{ es un ordinal biyectable con } X\}$.

Observemos que si $\mathcal{R}$ es un buen orden en $\mathcal{P}(X)$ que corresponde al ordinal β entonces todo ordinal biyectable con X es $\leq \beta$ por lo que

$$\{\alpha : \alpha \text{ es un ordinal biyectable con } X\}$$

es un conjunto contenido en el conjunto $\{\alpha : \alpha \text{ es un ordinal} \leq \beta\}$, que está bien ordenado. Por lo que la existencia de $card(X)$ está asegurada. O, en otras palabras, la definición anterior es de curso legal.

De esta definición resulta claro que X es biyectable con $card(X)$ por lo que podemos seguir afirmando que dos conjuntos tienen la misma cardinalidad si y solo si son biyectables:

$$X \text{ biyectable con } Y \iff card(X) = card(Y).$$

Para todo ordinal α se verifica que $card(\alpha) \leq \alpha$. Por otro lado es un sencillo ejercicio comprobar que la identidad $\alpha = card(\alpha)$ es equivalente a cualquiera de las propiedades siguientes:

1. $\beta < card(\alpha)$ *para todo ordinal* $\beta < \alpha$;
2. $card(\beta) < card(\alpha)$ *para todo* $\beta < \alpha$;
3. $card(\beta) \neq card(\alpha)$ *para todo* $\beta < \alpha$.

Este ejercicio justifica la denominación de "ordinales iniciales" para los cardinales. Esto es, ordinales que son los menores de entre los de una cardinalidad dada.

Lema. *Sean X e Y dos conjuntos. Tenemos que $card(X) \leq card(Y)$ si y solo si existe una inyección $f : X \longrightarrow Y$.*

Demostración. *Si $card(X) = card(Y)$ no hay nada que probar.*

Sean $X \overset{\varphi}{\sim} card(X)$, $Y \overset{\psi}{\sim} card(Y)$ biyecciones. Por ser $card(X) \leq card(Y)$ entonces $card(X) \subset card(Y)$. Sea $\imath$ la inclusión. Tenemos que

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & card(X) \\ \downarrow & & \downarrow \imath \\ Y & \xleftarrow{\psi^{-1}} & card(Y) \end{array}$$

donde $\psi^{-1} \circ \imath \circ \varphi$ es inyectiva.

Recíprocamente si $f : X \longrightarrow Y$ es inyectiva

$$\begin{array}{ccc} X & \xleftarrow{\varphi^{-1}} & card(X) \\ f \downarrow & & \downarrow \\ Y & \xrightarrow{\psi} & card(Y) \end{array}$$

entonces $\psi \circ f \circ \varphi^{-1}$ es inyectiva pero eso implica que $card(X) \leq card(Y)$. ■

Luego si $X \subset Y$ entonces $card(X) \leq card(Y)$. Las propiedades que hemos demostrado de los números ordinales nos permiten resolver fácilmente el ejercicio siguiente:

Ejercicio 1. *Cada ordinal finito n es un cardinal y $\omega = \{\{0, 1, 2, \ldots\}; \leq\}$ es también un cardinal al que hemos denominado $\aleph_0$, alef subcero.*

En el orden $\leq$ nuestro primer cardinal infinito $\aleph_0$ tiene un siguiente al que podemos llamar $\aleph_1$. Si $\mathcal{C}$ es el cardinal de los números reales, el teorema de Cantor nos permite concluir que $\aleph_1 \leq \mathcal{C}$. Naturalmente surge la pregunta: ¿Es cierto que $\aleph_1 = \mathcal{C}$ o, por el contrario, hay cardinales intermedios?

Conocida como hipótesis del continuo fue uno de los problemas propuestos por Hilbert a comienzos del siglo XX *y resuelto, en trabajos independientes y complementarios, por K. Gödel y P. Cohen. Entre ambos mostraron que la hipótesis del continuo es independiente de los axiomas que habían sido introducidos para fundamentar la teoría de Conjuntos (axiomas de Zermelo–Fraenkel) y, por lo tanto, podemos aceptarla, o no, como un nuevo axioma con la seguridad de que si nuestra teoría ya era consistente, la adición de la hipótesis del continuo, o de su contraria, no iba a cambiar ese status. Pero esas nociones de consistencia, completitud e independencia las analizaremos más adelante.*

Retomando la pregunta del capítulo 1, y siguiendo a Von Neumann, el cardinal uno, o cardinal del conjunto egoísta, $\{yo\}$, $\{yo\ mismo\}$, $\{mi\ mamá\}$, $\{mi\ ombligo\}$, es por tanto

$$1 = card(\{\emptyset\}) = card(\{yo\}).$$

O, como bien se lee en el Eclesiastés: vanitas vanitatis, et omnia vanitas.

8.1. Antinomias

En el capítulo 1 vimos la incidencia que tuvieron las llamadas antinomias o paradojas de la "teoría ingenua" de conjuntos. La más famosa es quizás la formulada por B. Russell en torno al conjunto de todos los conjuntos ordinarios, o que no se tienen a sí mismos como miembros: dicho conjunto no puede ser ni ordinario ni extraordinario. Pero Russell llegó a este conciso enunciado al analizar la paradoja que había detectado el propio Cantor. Se trata de lo siguiente:

Como vimos en el capítulo 5, Cantor demostró que

$$card(X) < card\big(\mathcal{P}(X)\big)$$

cualquiera que sea el conjunto X. Consideremos ahora $\Omega =$ "conjunto de todos los conjuntos" y el conjunto $\mathcal{P}(\Omega)$. Cada elemento de $\mathcal{P}(\Omega)$ es un conjunto y, por tanto, miembro de Ω: $\mathcal{P}(\Omega) \subset \Omega$. Esta inclusión implica que $card(\mathcal{P}(\Omega)) \leq card(\Omega)$ en contradicción con el teorema de Cantor citado anteriormente.

Enseguida surgieron otras antinomias que venían a poner en entredicho el uso indiscriminado del término conjunto. He aquí una muestra:

Paradoja de Berry (1906): *"Sea x el menor número natural que no puede ser nombrado con menos de cien sílabas". Resulta que la expresión de Berry nombra con menos de cien sílabas a un número que no puede ser así nombrado.*

Paradoja de Grelling (1908): *Diremos que un adjetivo es "heterológico" si la propiedad que expresa no se aplica a sí mismo. Por el contrario un adjetivo será "autológico" si se refiere a sí mismo. Ejemplo: "bisilábico" es heterológico, mientras que "polisilábico" es autológico. Consideremos ahora el adjetivo "heterológico": si es heterológico no se aplica a sí mismo, luego no es heterológico. Pero si no es heterológico no se aplica a sí mismo y, por tanto, ¡es heterológico!*

Paradoja de Richard (1905): *Algunas frases del castellano definen propiedades de los números naturales. Por ejemplo: "el número n es suma de dos cuadrados". Si al alfabeto le añadimos todos los signos ortográficos más otro para el "espacio en blanco" obtendremos un conjunto finito y ordenado de símbolos con los que escribir cualquier frase. Los textos escritos con k caracteres forman un conjunto finito que podemos ordenar alfabéticamente. Esto nos permite dar un orden al conjunto de frases: primero las de solo un carácter, luego las de dos, etc. Si nos restringimos ahora a aquellas que describen propiedades de los números naturales obtendremos una fila $P_0, P_1, P_2, \ldots$ que nos permite la siguiente definición:*

El número n es richardiano si no satisface la propiedad P_n.

Consideremos ahora la frase "n es un número richardiano" que ocupará un lugar en nuestra fila, i.e.: $\exists\, m\ P_m =$"n es un número richardiano". ¿Es m richardiano?

Veamos: si m fuese richardiano entonces m verificaría la propiedad P_m y, por tanto, no podría ser richardiano; pero si m no fuese richardiano entonces no verificaría P_m y, por definición, habría de ser richardiano. Es decir, ¡estamos perdidos!

Estas paradojas tienen una estructura parecida a otra ya famosa entre los clásicos griegos: la paradoja del mentiroso o de Epiménides.

Epiménides proclamó lo siguiente: "Esta afirmación es falsa. ¿Es falsa?". Se produce el bucle: si es falsa entonces es cierta, etcétera. Una versión equivalente consiste en las dos frases: "La afirmación siguiente es falsa. La afirmación precedente es verdadera".

Las paradojas, sobre todo las de Cantor y Russell, pusieron en cuarentena la teoría "ingenua" de conjuntos que consideramos en el primer capítulo. Había pues que ser más cuidadosos en la formulación y tomar las precauciones oportunas para evitar estas definiciones circulares que originan antinomias. Entre otros el gran D. Hilbert propuso una hoja de ruta:

Me gustaría eliminar totalmente los problemas de los fundamentos de las Matemáticas. Con ese fin transformo toda proposición matemática en una fórmula concreta demostrable y rigurosamente deducible, poniendo las definiciones y conclusiones matemáticas en tal posición que resultan incontrovertibles y proporcionan además una imagen de la ciencia considerada en su conjunto. Creo que podré conseguir completamente este objetivo con mi teoría de la demostración, aunque será todavía necesario mucho trabajo para llevarla a su perfección definitiva.

La Matemática como cualquier otra ciencia no puede basarse únicamente en la lógica. Por el contrario, algo ha tenido que sernos dado previamente en la imaginación como condición previa para el empleo de las inferencias y operaciones lógicas; ciertos objetos concretos y preter–lógicos que, intuitivamente como cualquier vivencia inmediata, vemos que están ahí precediendo a todo discurso. Pero si deseamos que la inferencia lógica sea segura, es preciso que estos objetos puedan ser comprendidos en todas sus partes, y que su descripción, distinción, ordenación y posición consecutiva sean dadas inmediatamente, e intuitivamente al mismo tiempo que los objetos; como algo que no permite ni necesita ser reducido nuevamente a algo ulterior.

Este es el fundamento filosófico que considero que debe exigirse tanto para la Matemática como para cualquier otro pensar, comprender o comunicar científicos. En la Matemática los objetos que consideramos son los mismos signos concretos, cuya forma, una vez introducida, debe ser inmediatamente clara y reconocible.

D. Hilbert *(1927)*

8.2. Lenguaje formal y axiomas

Feliz vivía el ciempiés
hasta que la rana con humor
preguntole: por favor,
¿en qué orden mueves los pies?

Creole tal estupor
que desde entonces el ciempiés
de una zanja no puede emerger
por pensar cómo correr.

Mrs. E. Craster

En un lenguaje formal tenemos variables $x_1, x_2, \ldots$ *y constantes* $a_1, a_2, \ldots$ *Disponemos además de los símbolos lógicos* $\big(\neg$ *(negación),* $\wedge$ *(conjunción),* $\vee$ *(disyunción),* $\Rightarrow$ *(implicación))* *y de los cuantificadores* $\forall$ *(universal) y* $\exists$ *(existencial). Aunque, como ya vimos en el capítulo 1, varios de estos símbolos son redundantes porque pueden ser definidos a partir de los otros, como muestran los ejemplos:* $\alpha \vee \beta$ *es lo mismo que* $\neg\big((\neg\alpha) \wedge (\neg\beta)\big)$*;* $\exists x\, \alpha(x)$ *es idéntico a* $\neg\big(\forall x\, \neg\alpha(x)\big)$*.*

También tendremos un conjunto numerable (no vacío) de predicados α_j *(cada uno con número finito* $n(j)$ *de argumentos) y de funciones* f_j*. Las constantes y las variables individuales son términos del idioma. También lo son los valores* $f_j(t_1, \ldots, t_{n(j)})$ *donde los* t_k *son términos.*

Con estos elementos podemos escribir textos o sucesiones de símbolos, pero no todos ellos formarán parte de nuestro lenguaje, solo aquellos que se atengan a unas ciertas reglas y que llamaremos fórmulas (o fórmulas bien hechas) serán aceptadas por nuestro "compilador" de acuerdo con las siguientes instrucciones:

1) *Fórmulas atómicas* $\alpha_j(t_1, \ldots, t_{n(j)})$ *donde* α_j *es un predicado y los* t_k *son términos.*

2) *Si* $\mathcal{A}$ *y* $\mathcal{B}$ *son fórmulas y* x *es una variable entonces* $\neg\mathcal{A}$*,* $\big(\mathcal{A} \Rightarrow \mathcal{B}\big)$ *y* $\forall x\, \mathcal{A}$ *son fórmulas.*

Las fórmulas se originan aplicando un número finito de veces las instrucciones 1 y 2. En ellas aparecen las variables en dos situaciones distintas, a saber: libres y ligadas.

En la fórmula "$\forall x\ \alpha(x\,,\, y)$*" y es una variable libre mientras que* x *está ligada. En "*$\big(\exists x\, \alpha(x, z)\big) \Rightarrow \big((\forall y\, \beta(x, y)) \Rightarrow \gamma\big)$*" las dos primeras apariciones de* x *son ligadas, pero la tercera es libre. La "ligadura" está pues asociada a los*

cuantificadores. Recordemos que en el cálculo diferencial tenemos expresiones como

$$F(x) = \int_0^x f(x)\,\mathrm{d}\,x$$

donde la x de $\int_0^x$ es "libre" mientras que la x de $f(x)\,\mathrm{d}\,x$ está "ligada" y podemos sustituirla por otra variable eliminando entonces cualquier confusión:

$$F(x) = \int_0^x f(y)\,\mathrm{d}\,y.$$

Parece pues muy razonable hacer lo mismo en nuestro lenguaje formal exigiendo que en las fórmulas no aparezcan variables en las dos versiones, libre y ligada, al mismo tiempo.

En una teoría formal se escogen unas fórmulas, denominadas axiomas, y a partir de ellas, usando las reglas de inferencia, se obtienen los teoremas. Hay dos tipos de axiomas: unos son los axiomas lógicos comunes a todas las teorías que sintetizan las reglas básicas del pensamiento; otros son los axiomas propios de cada teoría particular.

Axiomas lógicos. *Si $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ designan fórmulas bien hechas entonces:*

1) $\mathcal{A} \Longrightarrow \big(\mathcal{B} \Longrightarrow \mathcal{A}\big)$

Ejemplo: "Si Cervantes escribió el Quijote entonces ora Cervantes escribió el Quijote ya los ángeles tienen alas".

2) $\big(\mathcal{A} \Longrightarrow (\mathcal{B} \Longrightarrow \mathcal{C})\big) \Longrightarrow \big((\mathcal{A} \Longrightarrow \mathcal{B}) \Longrightarrow (\mathcal{A} \Longrightarrow \mathcal{C})\big)$

Ejemplo: "Si es que de si que Cervantes escribió el Quijote resulta que si los demonios tienen cuernos entonces los ángeles tienen alas, tenemos que si de que Cervantes escribió el Quijote se sigue que los demonios tienen cuernos entonces de que Cervantes escribió el Quijote se deduce que los ángeles tienen alas".

3) $\big(\neg\mathcal{B} \Longrightarrow \neg\mathcal{A}\big) \Longrightarrow \big((\neg\mathcal{B} \Longrightarrow \mathcal{A}) \Longrightarrow \mathcal{B}\big)$.

Ejemplo: "Si de que los demonios no tengan cuernos se deriva que los ángeles no tienen alas, entonces, ora los demonios tienen cuernos ya los ángeles no tienen alas y los demonios no tienen cuernos".

4) $\forall\, x\, \mathcal{A}(x) \Longrightarrow \mathcal{A}(t)$.

Suponiendo que ninguna de las variables ligadas de $\mathcal{A}(x)$ coincida con alguna de las variables contenidas en t.

5) $\Big(\big(\forall\, x\, \mathcal{A}\big) \Longrightarrow \mathcal{B}\Big) \Longrightarrow \Big(\mathcal{A} \Longrightarrow \big(\forall\, x\, \mathcal{B}\big)\Big)$.

Donde $\mathcal{A}$ es una fórmula en la que la variable x no aparece libre.

Las reglas de inferencia son las siguientes:

a) *Modus ponens: Si $\mathcal{A}$ y $\mathcal{B}$ son fórmulas entonces:*

$$\big(\mathcal{A} \wedge (\mathcal{A} \Longrightarrow \mathcal{B})\big) \Longrightarrow \mathcal{B}.$$

b) *Sustitución: La regla de sustitución dice que de una fórmula que contiene variables se deriva otra fórmula sustituyendo variables libres por fórmulas de una manera uniforme. Es decir, que si una variable libre ha sido sustituida por una fórmula, la misma sustitución debe hacerse cada vez que la misma variable aparezca libremente en la fórmula original.*

8.3. El sistema de Zermelo–Fraenkel

Dijo Dios, sea la nada.
Y alzó su mano derecha
hasta ocultar la mirada
quedando la nada hecha.

A. Machado

En la teoría formal de conjuntos todos los objetos son conjuntos, por lo que esta palabra resulta superflua: "conjunto es todo lo que es, pero el de todos no es".

Las fórmulas básicas son: "$a \in b$" (que se lee a pertenece a b) y "$a = b$" (a es igual a b), donde $a, b \ldots, x, y, z, \ldots$ o cualquier otra variable representan conjuntos.

Fueron muchos los matemáticos que contribuyeron a formular un sistema de axiomas para la teoría de conjuntos llevando a cabo el programa de Hilbert. Cabe citar, entre otros, a Zermelo, Fraenkel, Skolen, Von Neumann, Bernays, Gödel y Mirimanoff. Los axiomas admiten diversas presentaciones, he aquí una de ellas:

0) Existencia: Existe un conjunto $x = x$.

1) Extensión: Si a y b son conjuntos tales que $x \in a$ si y solo si $x \in b$ entonces $a = b$.

2) Separación: Si a es un conjunto y $\mathcal{B}(x)$ un predicado entonces existe un conjunto b tal que $x \in b$ si y solo si $x \in a$ y $\mathcal{B}(x)$ es cierta: $b = \{x \in a \mid \mathcal{B}(x)\}$.

Los dos primeros axiomas deben entenderse también como una definición de los símbolos "$\in$" y "$=$", además de postular la existencia de conjuntos. También nos permite definir la inclusión $a \subset b$ si y solo si "$(x \in b) \Longrightarrow (x \in a)$".

El axioma de separación es en realidad un esquema de axiomas, uno por cada conjunto a y cada predicado $\mathcal{B}(x)$. Combinando los axiomas 0 y 2 obtenemos

Corolario. (Existencia del vacío) *Existe* $\emptyset = \{y \in X \mid y \neq y\}$.

Observemos que el axioma de separación no postula la existencia de objetos que verifican una propiedad, que era el axioma esquema de comprensión de Frege que nos llevaría a la paradoja de Russell.

La versión más modesta que adoptamos como axioma de separación necesita de un conjunto a en el que separar los elementos que tienen la propiedad prescrita. Eso elimina la paradoja de Russell.

Proposición. *No existe el conjunto de todos los conjuntos.*

Demostración. *Si existiese tal conjunto Ω entonces por el axioma de separación también existiría el conjunto $O = \{x \in \Omega \mid x \notin x\}$ que produce una contradicción ya que $\big(O \in O\big) \wedge \big(O \notin O\big)$. Luego Ω no existe.* ■

3) *Parejas: Si a y b son conjuntos existe un conjunto c tal que $x \in c$ si y solo si $(x = a) \vee (x = b)$: $c = \{a, b\}$.*
4) *Uniones: Si c es un conjunto, existe un conjunto a tal que $x \in a$ si y solo si $x \in b$ para algún miembro $b \in a$: $a = \bigcup_{b \in c} b$.*
5) *Potencias: Si a es un conjunto entonces existe otro conjunto $\mathcal{P}(a)$ tal que $b \in \mathcal{P}(a)$ si y solo si $b \subset a$.*
6) *Infinito: Existe un conjunto ω tal que $\emptyset \in \omega$ y si $x \in \omega$ entonces $x \cup \{x\} \in \omega$.*

   Con este axioma nos aseguramos la existencia de conjuntos con infinitos elementos y tiene sentido hallar modelos de los axiomas de Peano para los naturales $\mathbb{N}$.
7) *Elección: Si a es un conjunto cuyos elementos son conjuntos no vacíos, entonces existe una función f cuyo dominio es a y tal que $f(b) \in b$ para todo $b \in a$.*
8) *Reemplazo: Si a es un conjunto y $\mathcal{B}(x, y)$ es una fórmula en la que x , y son variables libres, de manera que $\forall\, x \in a\, \exists! y$ tal que $\mathcal{B}(x, y)$ es cierta, entonces existe un conjunto b cuyos miembros son los y determinados por $\mathcal{B}(x, y)$ cuando x varía en a.*
9) *Regularidad: Cada conjunto no vacío posee un elemento minimal para la relación $\in$:*

   Si $x \neq \emptyset$ entonces existe $y \in x$ tal que no existe $z \in x$ tal que $z \in y$:

$$\forall x \big(\exists y \mid y \in x\big) \implies \exists y \big((y \in x) \wedge (\neg \exists z (z \in x) \wedge (z \in y)\big).$$

Este axioma impide la existencia de cadenas infinitas $\cdots \in x_{n+1} \in x_n \in x_{n-1} \in \cdots \in x_0$.

Una consecuencia de este axioma, que dejamos como ejercicio al lector, son las siguientes proposiciones:

i) $\forall x \;\; x \notin x$.

ii) Para x, y *es falso que* $x \in y \in x$.

El axioma 7 de elección es el más controvertido y algunas de sus implicaciones fueron analizadas en el capítulo 7. El axioma de regularidad fue añadido posteriormente al sistema primitivo de E. Zermelo. Pero es quizás el axioma del infinito el que da lugar a la mayor fuente de problemas de consistencia. ¿Existen los enteros realmente? Es fácil probar la consistencia de los axiomas necesarios para la aritmética de cualquier conjunto finito de enteros. La dificultad aparece cuando consideramos el conjunto infinito de todos ellos. Se debe a A. Fraenkel la demostración de la independencia del axioma de elección respecto de los demás. Muchos autores consideran fundamental la contribución de Skolem sugiriendo que su nombre sea añadido a los de Zermelo y Fraenkel.

Este capítulo no puede hacer justicia a la riqueza de las ideas involucradas y tan solo pretende animar al lector a seguir aprendiendo las sutilezas de la Lógica Matemática, tan necesaria e interesante. No obstante, la mayoría de los axiomas son "verdades" tan evidentes que hacen recordar el magnífico relato de Julio Cortázar:

Nadie habrá dejado de observar que con frecuencia el suelo se pliega de manera tal que una parte sube en ángulo recto con el plano del suelo, y luego la parte siguiente se coloca paralela a este plano, para dar paso a una nueva perpendicular, conducta que se repite en espiral o en línea quebrada hasta alturas sumamente variables. Agachándose y poniendo la mano izquierda en una de las partes verticales, y la derecha en la horizontal correspondiente, se está en posesión momentánea de un peldaño o escalón ...

Para subir una escalera se comienza por levantar esa parte del cuerpo situada a la derecha abajo, envuelta casi siempre en cuero o gamuza, y que salvo excepciones cabe exactamente en el escalón. Puesta en el primer peldaño dicha parte, que para abreviar llamaremos pie, se recoge la parte equivalente de la izquierda (también llamada pie, pero que no ha de confundirse con el pie antes citado), y llevándola a la altura del pie, se la hace seguir hasta colocarla en el segundo peldaño, con lo cual en este descansará el pie, y en el primero descansará el pie. (Los primeros peldaños son siempre los más difíciles, hasta adquirir la coordinación necesaria. La coincidencia de nombre entre el pie y el pie hace difícil la explicación. Cuídese especialmente de no levantar al mismo tiempo el pie y el pie).

Llegado en esta forma al segundo peldaño, basta repetir alternadamente los movimientos hasta encontrarse con el final de la escalera.

Julio Cortázar

(Fragmento de "Instrucciones para subir una escalera")

8.4. Hilbert, Gödel, Turing: tocata y fuga

La teoría axiomática de conjuntos de Zermelo–Fraenkel consigue pues eliminar las paradojas lógicas de Russell y Cantor ya que los axiomas impiden que un conjunto pueda ser elemento de sí mismo y no cabe hablar de algo que no existe como es el conjunto de los conjuntos extraordinarios o el conjunto de todos los conjuntos. No obstante podemos desarrollar una teoría de clases cuyos elementos son conjuntos, que nos permita considerar, por ejemplo, la clase de todos los conjuntos, la de los espacios vectoriales o la de los grupos o anillos. Pero esto hay que hacerlo con cuidado, porque en caso contrario repetiríamos otra vez las paradojas al considerar la clase de todas las clases. Es decir, tenemos que someterlas a unos axiomas similares a los de Zermelo–Fraenkel pero dirigidos a estas clases propias.

Esta teoría fue desarrollada por Bertrand Russell y Alfred Whitehead en su obra Principia Mathematica, un conjunto de tres volúmenes publicados entre los años 1910 y 1913. Pero el plan diseñado por Hilbert para fundamentar las Matemáticas con unos cimientos sólidos era mucho más ambicioso, ya que pretendía con un número finito de axiomas (o esquemas de axiomas) derivar todo su edificio. En términos que se han hecho ahora populares, Hilbert, con su famosa frase "queremos saber, sabremos", pretendía conseguir una teoría del Todo para las matemáticas.

Recordemos que en una teoría formal tenemos las fórmulas, o fórmulas bien hechas aceptadas por nuestro "compilador" porque han sido obtenidas ajustándose a los criterios de formación de fórmulas. Tenemos también las reglas de inferencia y los axiomas que son un conjunto finito de fórmulas.

Una demostración $D = \{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n\}$ es una sucesión finita tal que cada fórmula $\mathcal{A}_j$ o bien es un axioma o bien se obtiene a partir de las anteriores utilizando las reglas de inferencia.

Una fórmula $\mathcal{A}$ es un teorema (lo que se designa con la notación $\vdash \mathcal{A}$) si aparece como el último elemento de una tal demostración.

Hilbert pretendía fundar las matemáticas sobre está noción estricta y austera de teoría y demostración. Acuñó también el término Metamatemática, en analogía con la Metafísica de Aristóteles, para designar el estudio desde fuera de los sistemas formales.

Una propiedad muy importante de un sistema de axiomas es que sea consistente. Es decir que no se dé el caso de una fórmula $\mathcal{A}$ tal que ella y su negación $\neg\mathcal{A}$ sean teoremas. Observemos que si ocurriese que $\vdash \mathcal{A}$ y $\vdash (\neg\mathcal{A})$ entonces cualquier fórmula $\mathcal{B}$ es un teorema y nuestra teoría sería banal:

$$\forall\mathcal{B} \quad \big(\mathcal{A} \wedge (\neg\mathcal{A})\big) \Longrightarrow \mathcal{B}$$

o, en otras palabras, la sucesión $\{\mathcal{A}, \neg\mathcal{A}, \mathcal{B}\}$ es una demostración de $\mathcal{B}$.

Otra propiedad importante de un sistema de axiomas es la de ser completo, lo que significa que si $\mathcal{A}$ es una fórmula bien hecha que no contiene ninguna variable libre entonces $\vdash \mathcal{A}$ o $\vdash (\neg\mathcal{A})$. Es decir que $\mathcal{A}$, su negación $\neg\mathcal{A}$ (o ambas) son teoremas demostrables en la teoría.

Que la propiedad de completitud solo atañe a fórmulas sin variables libres puede ilustrarse con un ejemplo: La fórmula $x + y = 7$ no es ni verdadera ni falsa, mientras que $\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z},\ \ x + y = 7$ es un teorema.

Es claro que consistencia y completitud apuntan en sentido contrario. La primera es imprescindible para que nuestra teoría merezca alguna consideración. La segunda es muy deseable si queremos que toda verdad sea demostrable. Pero la afirmación de que un sistema sea consistente o completo es un ejemplo de propiedad metamatemática cuyas leyes de demostración hay que precisar también con cuidado.

Hilbert lo hizo en la esperanza de que se pudiera probar que el sistema de Zermelo–Fraenkel, más o menos modificado, con el que podemos desarrollar la Aritmética, cumpla ambos requisitos. Otra propiedad metamatemática que cabe pedir también a un sistema axiomático es la independencia, que se trata de una aplicación del principio de Occam: ningún axioma, o parte de él, debe ser consecuencia de los demás. Resulta adecuado pedir la independencia ya que, en caso contrario, podríamos eliminar ese axioma, o la parte correspondiente, sin alterar para nada el conjunto de teoremas.

Un caso particular en el que es posible satisfacer las exigencias de Hilbert es el del cálculo de predicados, que es la teoría básica obtenida cuando no añadimos ninguno propio a los axiomas lógicos. Pero, ¿cómo demostrar algo así? La estrategia consiste en lo siguiente: si una teoría es inconsistente es decir si existe una fórmula $\mathcal{A}$ sin variables libres tal que $\vdash \mathcal{A}$ y $\vdash (\neg\mathcal{A})$, entonces todas esas fórmulas han de ser teoremas, es decir demostrables en la teoría. Ahora bien, esta afirmación tiene una recíproca obvia: si no toda fórmula es un teorema entonces la teoría es consistente. Basta pues con encontrar una fórmula sin variables libres que no pueda ser deducida de los axiomas.

Aunque ingeniosa, la idea es sin embargo muy sencilla y se basa en la noción de tautología que vimos en el capítulo primero cuando analizamos el cálculo de proposiciones. Los axiomas lógicos 1, 2 y 3 son ejemplos de tales tautologías, como también lo son todas las fórmulas bien hechas que se

puedan demostrar a partir de dichos tres axiomas. Eso no resulta sorprendente y la demostración la dejamos como ejercicio al lector.

Dada una fórmula $\mathcal{A}$ de nuestra teoría (cálculo de predicados) la transformamos en una expresión $\varphi(\mathcal{A})$ por el procedimiento de borrar en ella todos los cuantificadores y todos los términos, junto a las comas y a los paréntesis asociados. Por ejemplo:

$$\varphi\big(\forall x_1\, \alpha_j(x_1,\ldots,x_{n_j}) \implies \alpha_k(x_1,\ldots,x_{n_k})\big) = \big(\alpha_j \implies \alpha_k\big).$$

Tenemos que $\varphi\big(\neg\mathcal{A}\big) = \neg\varphi(\mathcal{A})$ y $\varphi(\mathcal{A} \implies \mathcal{B}) = \big(\varphi(\mathcal{A}) \implies \varphi(\mathcal{B})\big)$.

Es fácil ver que la imagen por φ de los cinco axiomas lógicos devienen tautologías del cálculo de proposiciones: Los tres primeros son evidentes. El cuarto se convierte en $\varphi(\mathcal{A}) \implies \varphi(\mathcal{A})$ y el quinto en $\big(\varphi(\mathcal{A}) \implies \varphi(\mathcal{B})\big) \implies \big(\varphi(\mathcal{A}) \implies \varphi(\mathcal{B})\big)$.

Por lo tanto todo teorema $\vdash \mathcal{C}$ del cálculo de predicados se convierte en una tautología $\varphi(\mathcal{C})$ del cálculo de proposiciones. Si aquél fuese inconsistente habría una fórmula bien hecha $\mathcal{B}$ tal que $\vdash \mathcal{B}$ y $\vdash (\neg\mathcal{B})$ pero, entonces, tendríamos que tanto $\varphi(\mathcal{B})$ como $\neg\varphi(\mathcal{B})$ son tautologías, y eso es absurdo.

El cálculo de predicados es también completo, lo que demostró Kurt Gödel en su tesis doctoral en torno al año 1930. Pero el programa de Hilbert requería algo más, porque la fundamentación de las Matemáticas involucra a una teoría más rica en axiomas como, por ejemplo, los que incorpora el sistema Zermelo–Fraenkel, con o sin el axioma de elección, recogidos por Russell y Whitehead en los Principia Mathematica. En el año 1931 K. Gödel dio a conocer su celebrado teorema de incompletitud: cualquier teoría que contenga al sistema de los Principia Mathematica es incompleta. En otras palabras, contiene una fórmula bien hecha $\mathcal{A}$, sin variables libres, que es indecidible, es decir tal que ni $\mathcal{A}$ ni $\neg\mathcal{A}$ son demostrables en la teoría.

Por lo tanto, aunque añadamos más y más axiomas al sistema original siempre se nos escapará alguna proposición que no podremos demostrar, ni tampoco hacerlo con su contraria. Por lo que respecta al programa formalista de lograr una "teoría del Todo para las Matemáticas", Gödel colgó el mismo cartel que puso Dante a la entrada del infierno: "Lasciate ogni speranza".

El artículo de K. Gödel se tituló "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I" y fue publicado en la revista Monatshefte für Mathematik und Physik. El enunciado que hemos presentado es una glosa, en román paladino, del original de Gödel que está formulado en los términos lógicos precisos. Es también conocido como el "primer teorema de incompletitud". El segundo teorema puede ser enunciado

así: "Cualquier teoría axiomática formal que incluya a la Aritmética, contiene una demostración de su consistencia si y solo si es inconsistente". En otras palabras, si la teoría es consistente entonces no podemos, dentro de ella, demostrar su propia consistencia.

Hay ciertas sutilezas técnicas en los teoremas de Gödel que hacen conveniente precisar lo que entendemos por una teoría y por una prueba de consistencia. Pero la descripción que hemos hecho es básicamente correcta. Las ideas involucradas son muy ingeniosas, la demostración no es excesivamente complicada y puede ser comprendida sin mucho esfuerzo. En la bibliografía recomendada se encuentran escritos y comentados todos los pasos. Digamos tan solo que Gödel consigue transcribir afirmaciones metamatemáticas en términos aritméticos con un mecanismo que ha dado en llamarse gödelización. Usando el Teorema Fundamental de la Aritmética asocia a cada fórmula de la teoría axiomática de partida (que contiene los axiomas de Zermelo–Fraenkel) un número de una manera precisa que permite, por ejemplo, saber cuándo un número dado es de Gödel y a qué expresión corresponde. A continuación demuestra que todas las afirmaciones metamatemáticas acerca de las propiedades estructurales de las expresiones del cálculo formal pueden ser transplantadas como relaciones aritméticas entre los correspondientes números de Gödel.

Finalmente Gödel le da la vuelta a la paradoja de Epiménides, o a la de Richard, construyendo una fórmula del sistema axiomático que es la transcripción aritmética de la afirmación metamatemática: "Esta fórmula no es demostrable siguiendo las reglas de la teoría axiomática".

Se demuestra entonces que $\mathcal{G}$ es demostrable si y solo si $\neg\mathcal{G}$ es demostrable. Sin embargo si una fórmula y su negación son demostrables entonces la teoría es inconsistente. Por lo tanto si la teoría es consistente entonces ni $\mathcal{G}$ ni $\neg\mathcal{G}$ pueden ser derivadas formalmente a partir de los axiomas. En otras palabras, $\mathcal{G}$ es una fórmula indecidible.

Los teoremas de Gödel son teoremas de la llamada lógica de primer orden que ha sido esbozada en el párrafo anterior, pero tienen también una interpretación natural en términos de la llamada Ciencia de la Computación. En la lógica de primer orden los teoremas forman un conjunto numerable y computable: Podemos escribir un programa de ordenador que vaya generando todas las demostraciones válidas. Pero podríamos pedir también la propiedad más potente de que sea recursivo: ¿es posible escribir un programa que determine sin lugar a dudas el carácter, cierto o falso, de cualquier proposición? Según ha demostrado Gödel, la respuesta es negativa.

El programa de Hilbert respecto a un sistema axiomático formal puede pues ser adaptado con facilidad y ser expresado en términos de los computadores: alfabeto, sintaxis, axiomas, reglas de inferencia y algoritmo que comprueba la corrección de las demostraciones. Un hito importante en esta historia ocurrió en torno al año 1936 cuando Alan Turing publicó su trabajo

sobre números no computables al que hicimos referencia en el capítulo 5. Turing "inventó" un computador virtual, o máquina de Turing, capaz de llevar a cabo cualquier computación que la mente humana pueda imaginar. Cuando Turing escribió su artículo no estaban tan familiarizados como lo estamos ahora con la idea de un computador, así que se molestó en describir su máquina con todo detalle. Pero hoy podemos seguir la esencia de su pensamiento con mayor facilidad: Un programa de ordenador estará escrito en un lenguaje formal, de acuerdo con unas reglas precisas, que reciba el visto bueno del compilador. Una vez aceptado podemos hacerlo "correr" y caben dos posibilidades: a) la máquina se para, dándonos una respuesta a la pregunta o cálculo formulado en un número finito de operaciones lógicas; b) la máquina no se detiene.

Veamos un ejemplo: supongamos que formulamos las proposiciones "todo número de la forma $2^{2^n}+1$ *es primo" y "La ecuación* $n^2 = r^4 + s^4$ *no tiene solución en enteros* n, r, s*". Nosotros sabemos que la primera es falsa, mientras que la segunda es verdadera por un celebrado teorema de Fermat que vimos en el capítulo 3. Pero ahora eso no nos interesa especialmente. Lo que nos interesa es que podemos abordar ambas proposiciones a través de un programa de nuestra máquina. En cada caso le pediríamos que empezando con* $n = 1, 2, \ldots$ *fuese analizando la verdad o falsedad de la afirmación, lo que puede hacerse en un número finito de comprobaciones, y que se pare la primera vez que la afirmación resulte falsa. En el primer caso la máquina se pararía cuando* $n = 5$, *pues* $F_5 = 2^{2^5}+1$ *es un número compuesto. Por el contrario, con el segundo programa la máquina seguiría ad nauseam sin detenerse jamás.*

El problema de la parada consiste en ver si hay una manera de decidir a priori cuándo un programa va a detenerse o, por el contrario, continuar indefinidamente. ¿Es posible diseñar un programa que compruebe cuándo cualquier otro programa va o no va a pararse?

Supongamos que tuviéramos tal programa al que al suministrarle cualquier programa nos diría si este se para o no se para. Llamémosle el Gran Comprobador. Diseñemos ahora otro programa, al que llamamos Vicioso, que use al Gran Comprobador para evaluar otros programas: si el programa considerado se para y así lo constata el Gran Comprobador entonces Vicioso se enrolla en un bucle sin fin, por el contrario si el Gran Comprobador se da cuenta de que el programa original no se para, entonces Vicioso se detiene. La parte dramática aparece cuando abastecemos a Vicioso con su propio programa: ¿se para o no se para? Esa es la cuestión.

Naturalmente que se trata de otra versión de las paradojas de Epiménides y de Richard, pero Turing hizo todo esto con sumo cuidado para concluir rigurosamente que no existe tal algoritmo de parada.

Finalmente Turing dedujo que la no existencia del Gran Comprobador implica que el sistema axiomático de partida no puede ser al mismo tiempo consistente y completo, es decir, el teorema de Gödel.

Una demostración muy interesante del teorema de incompletitud, distinta de las de Gödel y Turing, ha sido obtenida recientemente por G. Chaitin usando el número Ω que fue analizado en el capítulo de los números reales.

Chaitin introduce la noción de complejidad algorítmica. En román paladino, dado nuestro ordenador con su lenguaje de programación, o máquina Universal de Turing, un programa consiste en un rosario finito de bits, es decir una sucesión de 0 y 1. Un programa eficiente, o elegante, es aquel que minimiza su número de bits entre todos los que producen el mismo resultado, y ese número mínimo es una medida de la complejidad del algoritmo o programa.

Fijándonos ahora en los números reales, podemos considerar su "complejidad" de acuerdo con la longitud de los algoritmos que nos calculan sus cifras decimales. En este sentido un número como $\frac{1}{3} = 0{,}33333\ldots$ es muy "simple". Algo menos lo son $\sqrt{2}$ y π, pero ambos son números computables en el sentido de Turing y podemos escribir un programa, es decir una sucesión finita de bits, que calcule sucesivamente todas sus cifras decimales. Chaitin ha definido la noción de número algorítmicamente aleatorio como un número real x para el que existe una constante finita $c(x)$ tal que todo programa que calcule la enésima cifra decimal de x haya de tener, por lo menos, $n - c(x)$ bits. Y ha exhibido un ejemplo: el número Ω que mide la probabilidad de que un programa generado al azar se detenga al procesarlo en nuestra máquina de Turing (ver capítulo 5). Dicho número Ω es un objeto definido que no es computable: en cada teoría axiomática formal solo cabe calcularle un número finito de cifras decimales. Luego en todo sistema axiomático formal, en el sentido de Hilbert, que contenga a la Aritmética podemos formular una pregunta tan sencilla como es saber la enésima cifra decimal de Ω (para n suficientemente grande), cuya respuesta es indecidible dentro de él.

Pero, tampoco este párrafo puede hacer justicia a la profundidad y belleza de los teoremas mencionados y solo pretende estimular al lector para que vaya a las fuentes originales, o vicarias, donde aprender más de esta fascinante historia.

> *Alguna vez, los senderos de este laberinto convergen: por ejemplo, usted llega a esta casa, pero en uno de los pasados posibles usted es mi enemigo, en otro mi amigo.*
>
> Jorge Luis Borges
>
> ("El jardín de los senderos que se bifurcan")

— 9 —

Álgebra: Números y letras

Llegaron a un pueblo donde fue ventura hallar un algebrista con quien se curó el Sansón desgraciado.

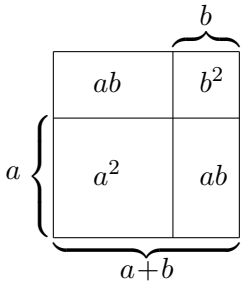
Miguel de Cervantes
(El Quijote)

Una de las características más notables del Álgebra radica en el uso sistemático de letras y números que aparecen "juntos y revueltos" en expresiones como las siguientes:

$$7x^2 - (1+100i)xy^3 + x^4y^2 - 13iy^6$$
$$a^3b^2 - 7ab^4 + 10ib^5$$

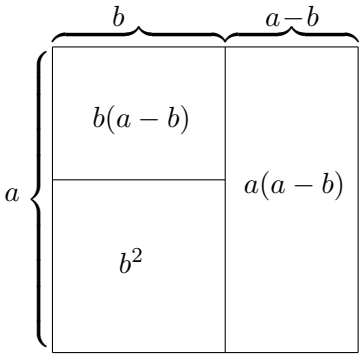
Cuadrado de una suma

$$(a+b)^2 = a^2 + 2ab + b^2$$



Diferencia de cuadrados

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



No obstante, en estos comienzos del siglo XXI *los ciudadanos ilustrados saben usar estas expresiones en el planteamiento y solución de diversos problemas.*

La igualdad $(a+b)^2 = a^2+2ab+b^2$ *significa que cuando sustituimos* a *y* b *por dos números cualesquiera obtenemos una verdadera identidad numérica. Por ejemplo, si* $a = 1$ *y* $b = 3$*, obtenemos:*

$$\begin{aligned} (1+3)^2 &= 4^2 = 4\times 4 = 16 \\ 1^2+2\times 1\times 3+3^2 &= 1+6+9 = 16. \end{aligned}$$

Análogamente, la igualdad $x + y = y + x$ *puede considerarse como una versión condensada y conveniente de las infinitas identidades:*

$$\begin{aligned} 1+3 &= 3+1 \\ \frac{3}{4}+\frac{5}{6} &= \frac{5}{6}+\frac{3}{4} \\ i+27 &= 27+i \\ \vdots\quad &\vdots\quad \vdots \end{aligned}$$

Sin embargo, la igualdad $x^3-6x^2+11x-6 = 0$ *solo se satisface cuando sustituimos la variable* x *por los números* 1, 2 *y* 3*, pero es falsa para todos los demás. Se trata de un ejemplo de ecuación algebraica.*

Los babilonios de hace más de treinta siglos ya sabían resolver la ecuación de segundo grado, como muestran las tabletas de su escritura cuneiforme. Un problema tratado por ellos pide calcular un número que sumado con su recíproco produzca un resultado prefijado de antemano. En la notación moderna se trata de resolver

$$x+\frac{1}{x} = a,$$

dando lugar a la ecuación $x^2-ax+1 = 0$*. Los babilonios conocían la manera de resolver* $ax^2+bx+c = 0$*,* $a \neq 0$*, cuya solución escribimos ahora con la fórmula*

$$x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

Una manera de obtenerla es completando el cuadrado:

$$\begin{aligned} ax^2+bx+c = 0 &\iff x^2+\frac{b}{a}x+\frac{c}{a} = 0 \\ &\iff \big(x+\frac{b}{2a}\big)^2-\frac{b^2}{4a^2}+\frac{c}{a} = 0 \\ &\iff x+\frac{b}{2a} = \pm\sqrt{\frac{b^2}{4a^2}-\frac{c}{a}} \\ &\iff x = -\frac{b}{2a}\pm\frac{\sqrt{b^2-4ac}}{2a}. \end{aligned}$$

La palabra Álgebra es de origen árabe y proviene de un libro escrito en torno al año 830 por el astrónomo Mohamed Ibn Musa al–Juarizmi, quien vivió en la ciudad de Bagdad durante el reinado de Harum al–Rashid, el sultán de las Mil y una noches. El título de la obra de al–Juarizmi es Al–jabr w'al muqâbala.

La palabra "jabr" significa "restauración", en el sentido de restaurar el equilibrio de una ecuación por el procedimiento de colocar en uno de sus miembros el término que ha sido eliminado antes del otro. Si quitamos -6 *del primer miembro de la ecuación* $2x+7x-6=3$*, el "equilibrio" se alcanza añadiendo* 6 *al segundo miembro:* $2x+7x=3+6$*.*

"Muqâbala" significa "simplificación", por ejemplo: combinando los términos $2x+7x$ *obtenemos la ecuación* $9x=9$*.*

En español la palabra "algebrista" comenzó su existencia designando a la profesión de los primitivos traumatólogos, o restauradores de huesos rotos, a la que hace referencia la cita del Quijote con la que iniciamos el capítulo. No resultaba extraño que los barberos se anunciaran, en tiempos de Cervantes, con el letrero de "algebrista y sangrador", porque administraban diversos tratamientos curativos: sangrías, sacar muelas y arreglar los huesos rotos.

En nuestra sociedad, más evolucionada, los algebristas están ubicados en las Facultades universitarias, donde enseñan su arte e investigan en áreas tales como: Teoría de grupos, Geometría Algebraica, Teoría de los Números, Álgebra Homológica y Criptografía. Pero, al menos los que yo conozco, han perdido sus poderes curativos.

9.1. Los polinomios y sus monomios

Un polinomio es una expresión que contiene letras, las variables, y números, los coeficientes, relacionados por medio de las operaciones de suma, resta y multiplicación, por ejemplo:

$$\frac{1}{5}x^3-3x^2+y+\sqrt{3}xy^2-y^3$$
$$(1+2i)xy^2-7x^4+(1+\sqrt{5})y^3$$
$$(x+y+z)^3.$$

Un polinomio en el que no aparecen sumas o restas se dice un monomio: x^3y^2*,* $3\sqrt{5}ixyz^7$*, son monomios.*

Podríamos objetar que estos ejemplos no solo contienen las operaciones indicadas, sino también a potencias positivas de las variables. Es cierto, pero una potencia positiva como x^3 *es una abreviación para el producto* $x\cdot x\cdot x$*.*

Luego nuestra definición se sostiene y es legal usar potencias positivas en los polinomios. Lo que no estará permitido son las potencias negativas, tales como x^{-3}, o fraccionarias, como $x^{1/2}$ o $x^{1/3}$.

Identificaremos siempre los monomios que tengan el mismo coeficiente y las mismas letras elevadas a los mismos exponentes, sin que nos importe el orden de los factores. Diremos que dos monomios son semejantes siempre que contengan las mismas letras elevadas a idénticas potencias, aunque los coeficientes sean distintos.

Ejemplos:

$$3xyxx7y^3 = 21x^3y^4$$
$$(-4)x^2y(-3)y^2x^2 = 12x^4y^3$$
$$(-5)xyy^3ix^2 = -5ix^3y^4$$
$$x^2(-3)y5xxy^2 = -15x^4y^3.$$

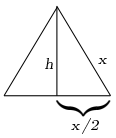
El monomio $21x^3y^4$ es semejante al monomio $-5ix^3y^4$, mientras que $12x^4y^3$ lo es a $-15x^4y^3$.

Un monomio es, por tanto, un caso particular de polinomio, y todo polinomio es una suma de monomios.

"Polis" es una raíz griega que significa "muchos"; "mono" es también raíz griega para "uno solo": polifacético, políglota, monopatín, monogamia, polígono, monocorde, ..., son ejemplos de palabras de nuestro idioma que contienen esas raíces.

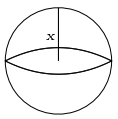
Ejemplos:

1. *Área del triángulo equilátero de lado x:*



$$A(x) = \frac{1}{2}\,hx = \frac{1}{2}\,x\sqrt{x^2 - \frac{x^2}{4}} = \frac{\sqrt{3}}{4}\,x^2.$$

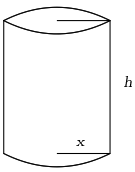
2. *Área de la esfera de radio x:*



$$A(x) = 4\pi x^2.$$

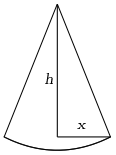
3. *Volumen de la esfera de radio x:* $V(x) = \dfrac{4}{3}\,\pi x^3$.

4. *Volumen del cilindro de radio x y altura h:*



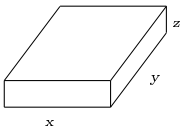
$$V(x,h) = \pi x^2 h.$$

5. *Volumen del cono de radio x y altura h:*



$$V(x,h) = \frac{1}{3}\pi x^2 h.$$

6. *Paralelepípedo de lados x, y y z:*



Su volumen es $V(x,y,z) = xyz$; mientras que su área es $A(x,y,z) = 2(xy + xz + yz)$.

Dos monomios semejantes que aparezcan en un polinomio pueden siempre agruparse en uno solo, sin más que sumar los coeficientes:

$$\begin{array}{rcl} 21x^3y^4 - 5ix^3y^4 & = & (21-5i)x^3y^4 \\ 21x^4y^3 - 15x^4y^3 & = & 6x^4y^3 \\ \vdots & \vdots & \vdots \end{array}$$

Luego un polinomio es una suma de monomios; cada monomio es el producto de un número, su coeficiente, y potencias de letras distintas, las variables. Los monomios semejantes del polinomio se agrupan en uno solo por el procedimiento de sumar sus coeficientes, por lo que en la llamada forma normal (o reducida) un polinomio es una suma de monomios que no son semejantes entre sí.

Para sumar polinomios dados en forma reducida, se suman los coeficientes de los monomios semejantes. Si esta suma resultara ser cero, entonces el monomio correspondiente desaparece de la suma.

Ejemplos:

1)
$$\begin{array}{rl} & x + 3x^2 - 2y + 6y^2 - 4xy \\ + & \\ & 2 - x + 2x^2 + 3y - 6y^2 + 5xy \\ \hline & 2 + (1-1)x + (3+2)x^2 + (-2+3)y + (6-6)y^2 + (-4+5)xy \\ = & 2 + 5x^2 + y + xy. \end{array}$$

2)
$$\begin{array}{rl} & x^3 - 2x^2y + 3y^3 - 7x^2 - 3y + 1 \\ + & \\ & \sqrt{3}x^4 - x^3 - 2y^3 + x + 3y + \dfrac{2}{3} \\ \hline & (0+\sqrt{3})x^4 + (1-1)x^3 + (-2+0)x^2y + (3-2)y^3 + (-7+0)x^2 \\ & +(0+1)x + (-3+3)y + 1 + \dfrac{2}{3} \\ = & \sqrt{3}x^4 - 2x^2y + y^3 - 7x^2 + x + \dfrac{5}{3}. \end{array}$$

El producto de dos monomios se obtiene multiplicando los coeficientes y sumando los exponentes de cada variable. En el caso de que una variable no aparezca en uno de los monomios, se considerará que su exponente es cero.

Para multiplicar dos polinomios, multiplicamos cada monomio del primero por cada monomio del segundo y sumamos los monomios obtenidos. Conviene simplificar el resultado reduciendo los términos semejantes.

Ejemplos:

$$\begin{aligned} (\sqrt{3}x^3y^2z)\cdot(-\sqrt{3}xyz^4) &= -3x^4y^3z^5 \\ (5xy^2)\cdot(7yz^3) &= 35xy^3z^3 \end{aligned}$$

(obsérvese que el exponente de x en el monomio $5xy^2$ es 1, $x^1 = x$, mientras que el de z es 0).

$$\begin{aligned} (x+y)\cdot(x^2-3xy-y^2) &= x^3 - 3x^2y - xy^2 + yx^2 - 3xy^2 - y^3 \\ &= x^3 - 2x^2y - 4xy^2 - y^3. \end{aligned}$$

¿Es posible que al multiplicar dos polinomios obtengamos menos monomios que en cada uno de los factores? La respuesta es afirmativa como muestra el siguiente ejemplo:

$$(x^2+2x+1)\cdot(x^2-2x+1) = x^4 - 1.$$

¿Puede ocurrir que al multiplicar dos polinomios distintos de cero, y simplificar los monomios semejantes, obtengamos el polinomio 0?

Ejercicios

1) *Efectuar las siguientes multiplicaciones:*

$$\begin{array}{l} (1 + x + 2x^2 - x^5)\cdot(-3 + 2x + x^5) \\ (x^2 + y)\cdot(x^3 + x^2y + xy^2 + y^3) \\ (x^2 + y^2 + z^2)\cdot(xy + xz + yz) \\ (x + y + z + w)^2\cdot(x + y - z - w) \\ (x-1)\cdot(1 + x + x^2 + x^3 + x^4 + x^5) \\ (x+1)\cdot(1 - x + x^2 - x^3 + x^4) \end{array}$$

2) *Agrupar todos los monomios semejantes entre sí:*

$$\sqrt{3}\,x^2,\ ab^2,\ \frac{2}{3}\,a^2b,\ -7x^2,\ -\sqrt{5x^4},\ -\frac{1}{2}\,ab^2,\ -\frac{1}{2}\,x.$$

3) *Buscar los valores de m y n para que los polinomios siguientes sean iguales:*

a) $7mx^2y-(\sqrt{3}+7)yx^n=-\sqrt{3}\,x^2y+2yx^2$;

b) $\dfrac{20}{3}\,x^3(mx)=\dfrac{1}{3}\,x^n+x^4$;

c) $\dfrac{25a^3b^4}{ma^2b}=\dfrac{1}{3}\,a^nb^3$.

9.2. Fracciones algebraicas

En nuestra definición de los polinomios no hemos permitido el uso de la división por las variables; las operaciones eran solamente la suma, la resta y la multiplicación. Si introducimos la división entonces la clase de los polinomios se enriquece para dar lugar a las fracciones algebraicas, como las siguientes:

$$\frac{xyz}{1+x},\ \frac{1}{\frac{1}{x}+\frac{1}{y}}\quad,\quad\frac{x^2+x-1}{2x+1}$$
$$\frac{1}{2+\frac{1}{2+\frac{1}{2+\frac{1}{x}}}}\quad,\quad\frac{(x+y)^3}{x^2+\frac{1}{y}}.$$

Ejemplo 1: *(Media armónica) La media armónica de dos números positivos, x e y, es el número cuyo inverso es la media aritmética de los inversos de x e y:*

$$\frac{1}{\left(\frac{1}{x}+\frac{1}{y}\right):2}=\frac{2}{\frac{1}{x}+\frac{1}{y}}=\frac{2xy}{x+y}.$$

Ejercicio 1. *Probar que la media armónica de dos números positivos, x e y, es menor o igual que la media geométrica ($\sqrt{xy}$), y esta, a su vez, es menor o igual que la media aritmética ($(x+y)/2$).*

A pesar de sus expresiones tan variopintas, todas ellas pueden, sin embargo, convertirse en el cociente de dos polinomios, P/Q ($Q\not\equiv 0$), que es lo que denominaremos una fracción algebraica.

Para conseguir ese objetivo haremos uso de las siguientes transformaciones que son consistentes con la leyes de la Aritmética:

Suma. *Dadas dos fracciones algebraicas, M/N y P/Q, su suma es la fracción dada por la fórmula:*

$$\frac{M}{N}+\frac{P}{Q}=\frac{MQ+PN}{QN}.$$

Ejemplos:

a) *La suma* $\dfrac{2x+3}{1+y}+\dfrac{x^3-2x+1}{x^2}$, *es:*

$$\begin{aligned}\frac{2x+3}{1+y}+\frac{x^3-2x+1}{x^2} &= \frac{2x^3+3x^2+x^3-2x+1+x^3y-2xy+y}{x^2+x^2y}\\ &= \frac{x^3y+3x^3+3x^2-2xy-2x+y+1}{x^2+x^2y}.\end{aligned}$$

b) *Por su parte, al sumar* $\dfrac{x^2+1}{x-1}$ *y* $\dfrac{3}{x+1}$ *obtenemos:*

$$\frac{x^2+1}{x-1}+\frac{3}{x+1} = \frac{x^3+x^2+4x-2}{x^2-1}.$$

Resta. *La diferencia entre las fracciones algebraicas M/N y P/Q es la fracción:*

$$\frac{M}{N}-\frac{P}{Q}=\frac{MQ-PN}{NQ}.$$

Ejemplo:

$$\begin{aligned}\frac{3y^2+x}{1+x}-\frac{xy}{1+y} &= \frac{3y^2+x+3y^3+xy-xy-x^2y}{(1+x)(1+y)}\\ &= \frac{3y^3-x^2y+3y^2+x}{1+x+y+xy}.\end{aligned}$$

Multiplicación. *El producto de dos fracciones algebraicas viene dado por la fórmula:*

$$\frac{M}{N}\cdot\frac{P}{Q}=\frac{M\cdot P}{N\cdot Q}.$$

Ejemplo:

$$\begin{aligned}\frac{2x+3}{1+y}\cdot\frac{x^2+1}{x-1} &= \frac{(2x+3)(x^2+1)}{(1+y)(x-1)}\\ &= \frac{2x^3+3x^2+2x+3}{xy+x-y-1}.\end{aligned}$$

División. *El cociente de las fracciones M/N y P/Q obedece a la regla siguiente:*

$$\frac{M}{N} : \frac{P}{Q} = \frac{MQ}{NP}.$$

Ejemplos:

$$\begin{aligned}
\frac{1}{\frac{1}{x}+\frac{1}{y}} = \frac{1}{\frac{x+y}{xy}} &= \frac{xy}{x+y} \\
\frac{1}{2+\frac{1}{2+\frac{1}{2+\frac{1}{x}}}} &= \frac{1}{2+\frac{1}{2+\frac{1}{\frac{2x+1}{x}}}} = \frac{1}{2+\frac{1}{2+\frac{x}{2x+1}}} = \frac{1}{2+\frac{1}{\frac{5x+2}{2x+1}}} \\
&= \frac{1}{2+\frac{2x+1}{5x+2}} = \frac{1}{\frac{12x+5}{5x+2}} = \frac{5x+2}{12x+5} \\
\frac{1}{a+\frac{1}{a+\frac{1}{a+\frac{1}{x}}}} &= \frac{1}{a+\frac{1}{a+\frac{1}{\frac{ax+1}{x}}}} = \frac{1}{a+\frac{1}{a+\frac{x}{ax+1}}} = \frac{1}{a+\frac{1}{\frac{(a^2+1)x+a}{ax+1}}} \\
&= \frac{1}{a+\frac{ax+1}{(a^2+1)x+a}} = \frac{1}{\frac{(a^3+2a)x+(a^2+1)}{(a^2+1)x+a}} \\
&= \frac{(a^2+1)x+a}{(a^3+2a)x+(a^2+1)}
\end{aligned}$$

Simplificación. *La simplificación consiste en suprimir un factor que sea común al numerador y al denominador:*

$$\frac{PM}{QM} = \frac{P}{Q}.$$

Ejemplos:

$$\begin{aligned}
\frac{x^2-1}{x^2-3x+2} &= \frac{(x-1)(x+1)}{(x-1)(x-2)} = \frac{x+1}{x-2} \\
\frac{x^2-6x+9}{x^2-9} &= \frac{(x-3)^2}{(x-3)(x+3)} = \frac{x-3}{x+3} \\
\frac{xyz+z^2}{z(x^2+y^2)} &= \frac{z(xy+z)}{z(x^2+y^2)} = \frac{xy+z}{x^2+y^2}.
\end{aligned}$$

Ejercicio 2. *Simplificar el resultado de la suma siguiente:*

$$S(y) = \frac{(y-a)(y-b)}{(c-a)(c-b)} + \frac{(y-a)(y-c)}{(b-a)(b-c)} + \frac{(y-b)(y-c)}{(a-b)(a-c)}.$$

(SOLUCIÓN: $S(y) = 1$).

Ejercicio 3. *Observemos que:*

$$\begin{aligned} 1+\frac{1}{x} &= \frac{x+1}{x} \\ \frac{1}{1+\frac{1}{x}} &= \frac{1}{\frac{x+1}{x}} = \frac{x}{x+1} \\ \frac{1}{1+\frac{1}{1+\frac{1}{x}}} &= \frac{1}{1+\frac{x}{x+1}} = \frac{x+1}{2x+1} \\ \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{x}}}} &= \frac{1}{1+\frac{x+1}{2x+1}} = \frac{2x+1}{3x+2}. \end{aligned}$$

Calcular los tres términos siguientes.

En cierto sentido, la simplificación puede resultar, a veces, una operación sospechosa, que bordea la ilegalidad, por cuanto el factor simplificado puede hacerse igual a cero para algún valor de las variables. Por ejemplo, en

$$\frac{x^2-1}{x^2-3x+2} = \frac{(x-1)(x+1)}{(x-1)(x-2)} = \frac{x+1}{x-2},$$

el factor que se simplifica, $x-1$, se anula cuando la variable x toma el valor 1.

Sin embargo, nosotros ignoraremos, por ahora, este fenómeno, aunque tiene su importancia cuando se estudian las funciones representadas por medio de fracciones algebraicas.

Ejercicio 4. *El valor del producto*

$$\left(x^4+x^3+x^2+x+1+\frac{2}{x-1}\right)\cdot\left(x^4-x^3+x^2-x+1-\frac{2}{x+1}\right)$$

no cambia si se suprimen las fracciones, ¿por qué?

Escribamos cada factor como una fracción:

$$\begin{aligned} x^4+x^3+x^2+x+1+\frac{2}{x-1} &= \frac{x^5-1}{x-1}+\frac{2}{x-1} = \frac{x^5+1}{x-1} \\ x^4-x^3+x^2-x+1-\frac{2}{x+1} &= \frac{x^5+1}{x+1}-\frac{2}{x+1} = \frac{x^5-1}{x+1}, \end{aligned}$$

y multipliquemos ambas:

$$\begin{aligned} \frac{x^5+1}{x-1}\cdot\frac{x^5-1}{x+1} &= \frac{x^5-1}{x-1}\cdot\frac{x^5+1}{x+1} \\ &= (x^4+x^3+x^2+x+1)\cdot(x^4-x^3+x^2-x+1). \end{aligned}$$

La fracción P/Q se obtiene simplificando la fracción R/S si existe un polinomio factor común, M, tal que $R=MP$, $S=MQ$, $PS=PMQ=RQ$. Esta última identidad sugiere una relación de equivalencia entre fracciones

algebraicas que es análoga a la que usamos entre las fracciones ordinarias al crear los números racionales. En cada clase de equivalencia tendríamos una fracción irreducible. Sin embargo, analizar este concepto nos llevaría a profundizar en la teoría de la divisibilidad de polinomios y ahora tenemos otras tareas más urgentes.

Ejemplo 2: *¿Son equivalentes las fracciones* $x/(x+y)$ *y* $x^2/(x^2+y^2)$*? La respuesta es negativa, pues:*

$$x(x^2+y^2) = x^3 + xy^2 \neq x^3 + x^2y = x^2(x+y),$$

como queda claro al tomar, por ejemplo, $x = 2$ *e* $y = 1$*:*

$$2(2^2+1^2) = 2\cdot 5 = 10 \neq 12 = 4\cdot 3 = 2^2(2+1).$$

Problema. *Calcular el valor de* a *para que las dos fracciones*

$$\frac{x^2+ax+a}{x^2+2x} \quad y \quad \frac{x+2}{x},$$

sean equivalentes.

SOLUCIÓN. *Si las dos fracciones son equivalentes, ha de verificarse la igualdad de los productos cruzados:* $x(x^2+ax+a)$ *y* $(x+2)(x^2+2x)$*; es decir:*

$$x^3 + ax^2 + ax = x^3 + 4x^2 + 4x.$$

Así, la solución es $a = 4$*.*

Problema. *Una piscina se llena por medio de dos grifos. El primero tardaría* x *horas en llenarla, mientras que al segundo le llevaría* y *horas. ¿Cuánto tiempo tardaría en llenarse la piscina si abrimos los dos grifos simultáneamente?*

SOLUCIÓN. *Supongamos que la piscina tiene una capacidad de* z *litros. Entonces, el primer grifo lanza el agua a una velocidad de* z/x *litros por hora, mientras que el segundo lo hace a* z/y *litros por hora. La cantidad de agua que lanzan cada hora ambos grifos juntos es igual a la suma:*

$$\frac{z}{x} + \frac{z}{y} = \frac{z(x+y)}{xy}.$$

El tiempo pedido en el problema viene dado, entonces, por la fracción algebraica:

$$T = \frac{z}{\frac{z(x+y)}{xy}} = \frac{xy}{x+y}.$$

En particular, si $x = 10$ *horas, e* $y = 12$ *horas, ambos juntos tardarían:*

$$\frac{10\cdot 12}{10+12} = \frac{120}{22} = \frac{60}{11} = 5,\widehat{45} \text{ horas.}$$

Ejercicios

1) *Calcular la suma:* $\dfrac{1}{2ab^2}+\dfrac{3}{5a^2b}+\dfrac{6}{abc^2}$.

2) *Sumar:* $\dfrac{1}{x^2-4}+\dfrac{2(x-2)}{x^3-x^2-x-2}+\dfrac{3(x^2+x+1)}{x-2}$.

3) *Determinar si son equivalentes las siguientes parejas de fracciones algebraicas:*

a) $\dfrac{2x^3+x^2-5x+2}{2x^2-7x+3}$ *y* $\dfrac{x^3+2x^2-x-2}{x^2-2x-3}$.

b) $\dfrac{x^3+x^2-9x-9}{x^3-2x^2-9x-18}$ *y* $\dfrac{x^4-x^2}{x^4-3x^3+2x^2}$.

4) *Simplificar, cuando sea posible, las siguientes fracciones:*

a) $\dfrac{(x^2-1)x}{(x+1)^2(x^2-2x)}$, b) $\dfrac{x^3-x}{(3x^2-3)(x+2)}$,

c) $\dfrac{x^4+81-18x^2}{2(x^4-81)}$, d) $\dfrac{x^2+x+1}{x^2-x-1}$.

5) *Operar y simplificar, todo lo que se pueda:*

a) $\dfrac{1}{x-1}-\dfrac{3}{2(x+1)}-\dfrac{2}{x^2-1}$;

b) $\left(\dfrac{2x-1}{(x-1)(x+1)}-\dfrac{x}{x-1}\right):\dfrac{3}{2x-2}$;

c) $\dfrac{ab^2-3a^2b}{b+(b-a)(b-2a)-(b^2+2a^2)}$.

9.3. El caso de una variable: El anillo $\mathbb{C}[x]$

Una clase especialmente importante de polinomios es la formada por los que contienen una sola variable, que generalmente designaremos con la letra x, y cuyos coeficientes son números complejos. Al conjunto formado por todos estos polinomios lo designaremos $\mathbb{C}[x]$, y los siguientes son elementos suyos:

$$x-3,\quad x^2+x+1,\quad 3ix^3+(7-2i)x^2+2x+5,$$
$$\sqrt{5}\,x^4+2ix^3-x^2+7x+5-\sqrt{2}\,i.$$

A menudo consideraremos expresiones de la forma ax^2+bx+c como polinomios de la variable x. Aunque, en un principio, ax^2+bx+c contiene también a las letras a, b y c, además de la x, seguiremos llamándoles polinomios de la única variable x, por cuanto, a, b y c serán consideradas no como

variables, sino como los coeficientes que habrá que especificar. Por ejemplo: si $a = 3$, $b = 1$ *y* $c = 7$, *obtenemos el trinomio* $3x^2 + x + 7$.

Esta notación resulta muy útil para expresar propiedades generales de los polinomios. No obstante, la elección de la letra x *para la variable (a veces* y *o* z*), y de las primeras letras del alfabeto,* $\{a, b, c, d, \dots\}$, *para designar a los coeficientes, es tan solo una costumbre, sin más legitimidad que la comodidad de su uso generalizado. Ahora bien, si alguien quisiera (o tuviera que) usar la letra* a *para la variable y las últimas letras del alfabeto para los coeficientes, estaría en su perfecto derecho, siempre que lo hiciese saber a los demás.*

Un elemento genérico de $\mathbb{C}[x]$ *puede ser escrito de la manera siguiente:*

$$P(X) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = \sum_{j=0}^{n} a_j x^j,$$

siendo los coeficientes, a_j, *números complejos y* $a_n \neq 0$.

Una noción importante es la de grado. El grado de un monomio, distinto de cero, es el exponente de la variable x*: si* $P(x) = a_n x^n$ *es un monomio no cero, escribiremos* $\operatorname{grad}(P) = n$ *para indicar que el grado del monomio* P *es* n*, así:*

$$\begin{aligned} \operatorname{grad}(\frac{5}{3}x^7) &= 7, \\ \operatorname{grad}(-7x^3) &= 3, \\ \operatorname{grad}(11x) &= 1, \\ \operatorname{grad}(7) &= 0, \\ \operatorname{grad}(10^3) &= 0 \dots \end{aligned}$$

Pero el grado de 0 *lo dejaremos sin definir (o bien diremos que* $\operatorname{grad}(0) = -\infty$*, por la razón que veremos en el ejercicio propuesto más abajo).*

El grado de un polinomio es, por definición, el de su monomio de mayor grado. Los polinomios de grado cero son las constantes no nulas. Los polinomios de grado uno son los binomios: $ax + b$ *con* $a \neq 0$. *Los polinomios de grado dos son los trinomios:* $ax^2 + bx + c$, $a \neq 0$; *...*

Si $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $a_n \neq 0$, *entonces* $\operatorname{grad}(P(x)) = n$.

Ejercicio 5. *Supongamos que* $\operatorname{grad}(P) = n \geq 0$, $\operatorname{grad}(Q) = m \geq 0$. *Demostrar que:*

1) $\operatorname{grad}(P \cdot Q) = m + n$.

2) $\operatorname{grad}(P + Q) \leq \operatorname{máx}\{m, n\}$.

3) *Supongamos las siguientes reglas aritméticas:* $n + (-\infty) = -\infty$, *para todo* $n \in \mathbb{N}$; $(-\infty) + (-\infty) = -\infty$. *Demostrar que 1) y 2) siguen siendo válidas en el caso en el que* P, *o* Q, *sean la constante cero.*

Ejercicio 6. *Demostrar que el conjunto $\mathbb{C}[x]$, dotado con las operaciones de suma y producto de polinomios, es un anillo abeliano con elemento unidad. Es decir, se verifican:*

1. *La suma y el producto tienen las propiedades asociativa, conmutativa y distributiva del producto respecto de la suma.*

2. *El polinomio 0 es elemento neutro para la suma, y dado el polinomio $P(x) = \sum_{j=0}^{n} a_j x^j$, su opuesto es $Q(x) = -P(x) = \sum_{j=0}^{n}(-a_j)x^j$.*

3. *El polinomio 1 es elemento neutro para el producto.*

Ejercicio 7. *Completar la igualdad: $(x^2-4)(x+\_\,) = (x+2)(x+3)(x+\_\,)$.*

Ejercicio 8. *(Polinomios interpoladores). Dados dos números, $a \neq b$, existe un polinomio, P, de grado ≤ 1 que toma valores prefijados, $P(a)$ y $P(b)$, a saber:*

$$P(x) = P(a)\frac{x-b}{a-b} + P(b)\frac{x-a}{b-a}.$$

Análogamente, si damos tres números distintos, a, b y c, y valores $P(a)$, $P(b)$ y $P(c)$, el polinomio:

$$P(x) = P(a)\frac{(x-b)(x-c)}{(a-b)(a-c)} + P(b)\frac{(x-a)(x-c)}{(b-a)(b-c)} + P(c)\frac{(x-a)(x-b)}{(c-a)(c-b)},$$

es de grado ≤ 2 y toma estos valores.

Hallar un polinomio, P, de grado a lo más 3 de manera que $P(0) = 1$, $P(1) = 2$, $P(2) = 3$ y $P(3) = 4$.

9.4. Funciones polinómicas. Igualdad de polinomios

Todo polinomio, $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, da lugar a una función con dominio y rango el conjunto de los números complejos, $\mathbb{C}$, por el procedimiento de asignar a cada $c \in \mathbb{C}$ el complejo:

$$P(c) = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_0 \in \mathbb{C}.$$

Es decir, $P(c)$ se obtiene sustituyendo en la expresión del polinomio la variable x por el número complejo c, y efectuando luego todas las operaciones en el cuerpo $\mathbb{C}$.

El concepto de igualdad de polinomios puede ser interpretado de diversas maneras. Podemos considerar dos polinomios iguales si es posible transformar uno en el otro por medio de operaciones algebraicas legales, tales como quitar paréntesis y sumar monomios semejantes. Según esta definición dos

polinomios de la variable x son iguales si y solo si tienen la misma forma normal o reducida:

$$P(x) = \sum_{j=0}^{n} a_j x^j, \qquad Q(x) = \sum_{k=0}^{m} b_x^k$$

$$P(x) = Q(x) \iff \begin{cases} m = n \\ a_j = b_j, \quad \text{para todo } 0 \leq j \leq n. \end{cases}$$

Pero existe otra definición igualmente plausible: dos polinomios, P y Q de $\mathbb{C}[x]$, son iguales si lo son sus funciones polinómicas asociadas. Es decir, si $P(c) = Q(c)$ cualquiera que sea el número complejo c.

Ocurre, no obstante, que estas dos definiciones son equivalentes: si dos polinomios son iguales respecto a una de ellas, entonces también lo son respecto de la otra. La sencilla demostración se deja como ejercicio al lector (después de estudiada la sección siguiente).

9.5. La división de polinomios y sus consecuencias

Recordemos el algoritmo de la división de números enteros: dados dos enteros, a y $d > 0$, que llamaremos dividendo y divisor, existen dos enteros, c y r, denominados, respectivamente, cociente y resto, que están unívocamente determinados por las relaciones:

$$\begin{aligned} a &= dc + r \\ 0 &\leq r < d. \end{aligned}$$

Una fracción propia es aquella en la que el numerador es menor que el denominador: $3/5$, $10/13$ y $101/729$ son ejemplos de fracciones propias, sus partes enteras son siempre iguales a cero. Por el contrario una fracción impropia, como $13/3$, tiene una parte entera distinta de cero:

$$\frac{13}{3} = 4 + \frac{1}{3}\,.$$

Otra manera de entender el algoritmo de la división consiste en plantearse el problema de escribir una fracción general como la suma de su parte entera más su parte fraccionaria, que es una fracción propia:

$$\frac{13}{3} = 4 + \frac{1}{3} \text{ “es equivalente a” } 13 = 4 \times 3 + 1$$

$$\frac{1}{3} \text{ es fracción propia “es equivalente a” } 0 \leq 1 < 3.$$

Pues bien, nuestro empeño consiste ahora en realizar operaciones similares con fracciones cuyo numerador y denominador sean polinomios en una variable.

$$\frac{x^5}{7x^3} = \frac{1}{7}x^2$$

$$\frac{-\sqrt{6}x^7}{\sqrt{2}x^4} = -\sqrt{3}x^3$$

Si $n \geq m$: $\dfrac{x^n}{x^m} = x^{n-m}$

$$\frac{6x^5 - x^3 + x^2 - 2x + 1}{3x^2} = 6x^3 - \frac{1}{3}\,x + \frac{1}{3} + \frac{-2x+1}{3x^2}$$

Cociente$= 6x^3 - \dfrac{1}{3}\,x + \dfrac{1}{3}$; *Resto*$= -2x + 1$.

Diremos que la fracción $P(x)/Q(x)$ es propia si el grado del numerador es menor que el denominador. La siguientes son fracciones propias:

$$\frac{\sqrt{3}\,x+1}{x^2},\ \frac{1}{x},\ \frac{10x^3+7x^2-1}{2x^5+x+7},\ \frac{x^5+x^4+x^3+x^2+1}{x^6+1},\ \frac{100\,000\,x^2}{1+x^3}\,.$$

Resulta que toda fracción impropia puede escribirse como la suma de un polinomio y una fracción propia:

$$\begin{aligned}
\frac{x^2}{x-1} &= x+1+\frac{1}{x-1}\\
\frac{x+2}{x+1} &= 1+\frac{1}{x+1}\\
\frac{x^4+1}{x^2-1} &= x^2+1+\frac{2}{x^2-1}\,.
\end{aligned}$$

Problema. *Dividimos un polinomio de grado 5 por otro de grado 3.*

¿Qué podemos afirmar acerca de los grados del cociente y el resto?

RESPUESTA: *El grado del cociente es $2 = 5 - 3$. El grado del resto puede ser 2, 1, 0 o bien indefinido $(-\infty)$ en el caso de que el resto sea el polinomio cero.*

Ejercicio. *Poner ejemplos de cada uno de estos casos.*

En realidad, existe un procedimiento sistemático para conseguir ese objetivo. Veamos unos ejemplos:

$$\begin{array}{rl|l}
x^5 & & x+2\\
\cline{3-3}
\underline{-x^5-2x^4} & & x^4-2x^3+4x^2-8x+16\\
-2x^4 & & \uparrow\\
\underline{2x^4+4x^3} & & \boxed{\text{cociente}}\\
4x^3 & &\\
\underline{-4x^3-8x^2} & &\\
-8x^2 & &\\
\underline{8x^2+16x} & &\\
16x & &\\
\underline{-16x-32} & &\\
-32 & \longleftarrow \boxed{\text{resto}} &
\end{array}$$

Podemos por tanto escribir:

$$\frac{x^5}{x+2} = x^4 - 2x^3 + 4x^2 - 8x + 16 - \frac{32}{x+2}\,.$$

$$\begin{array}{rl|l}
x^4 & +3x^2+2x-1 & 2x^2-x+3 \\
\cline{3-3}
-x^4+\frac{1}{2}x^3-\frac{3}{2}x^2 & & \frac{1}{2}x^2+\frac{1}{4}x+\frac{7}{8} \\
\cline{1-1}
\frac{1}{2}x^3+\frac{3}{2}x^2+2x-1 & & \uparrow \\
-\frac{1}{2}x^3+\frac{1}{4}x^2-\frac{3}{4}x & & \boxed{\text{cociente}} \\
\cline{1-1}
\frac{7}{4}x^2+\frac{5}{4}x-1 & & \\
-\frac{7}{4}x^2+\frac{7}{8}x-\frac{21}{8} & & \\
\cline{1-1}
\frac{17}{8}x-\frac{29}{8} & \longleftarrow \boxed{\text{resto}} &
\end{array}$$

Y así:

$$\frac{x^4+3x^2+2x-1}{2x^2-x+3} = \frac{1}{2}x^2 + \frac{1}{4}x + \frac{7}{8} + \frac{\frac{17}{8}x-\frac{29}{8}}{2x^2-x+3}\,.$$

El algoritmo es transparente. Consideremos el segundo ejemplo:

$$\frac{x^4+3x^2+2x-1}{2x^2-x+3}\,.$$

En primer lugar, dividimos el monomio de mayor grado del dividendo, x^4, por el de mayor grado del divisor, $2x^2$. El resultado:

$$\frac{x^4}{2x^2} = \frac{1}{2}x^2,$$

es el primer monomio del cociente.

A continuación, restamos del dividendo el resultado de multiplicar el divisor por el primer cociente:

$$\begin{aligned}
(x^4+3x^2+2x-1) - \frac{1}{2}\,x^2\,(2x^2-x+3) &= (x^4+3x^2+2x-1) - \left(x^4 - \frac{1}{2}\,x^3 + \frac{3}{2}\,x^2\right) \\
&= \frac{1}{2}\,x^3 + \frac{3}{2}\,x^2 + 2x - 1,
\end{aligned}$$

lo que nos permite escribir la identidad:

$$\frac{x^4+3x^2+2x-1}{2x^2-x+3} = \frac{1}{2}\,x^2 + \frac{\frac{1}{2}\,x^3+\frac{3}{2}\,x^2+2x-1}{2x^2-x+3}\,.$$

Como la fracción obtenida en el miembro de la derecha sigue siendo impropia, podemos repetir el proceso. Sin embargo, en cada paso hemos

rebajado el grado del numerador. Luego, después de un número finito de ellos, obtendremos la fracción propia buscada.

¿Qué pasa si el grado del dividendo es menor que el del divisor? En este caso la fracción algebraica ya es propia: el cociente es cero y el resto coincide con el dividendo.

Consideremos el cociente:

$$\frac{x^2+1}{x-a}.$$

¿Es posible encontrar un número real, a, de manera que la división dé resto cero?

La respuesta es negativa, pues si suponemos que el resto es cero, entonces la división daría la siguiente expresión

$$\frac{x^2+1}{x-a} = x + b.$$

Pero esta igualdad lleva a

$$x^2 + 1 = x^2 + (b-a)x - ab.$$

Así hemos de tener:

$$b - a = 0 \quad y \quad -a^2 = 1.$$

Pero, ¡no existe ningún número real, a, tal que $a^2 = -1$!

Ejercicio 9. *Efectuar las divisiones siguientes:*

1) $(x^5 + x^4 + x^3 + x^2 + x + 1) : (x^2 + x + 1)$;

2) $\dfrac{x^4 - x^3 + x^2 - x + 1}{x^2 - 1}$;

3) $\dfrac{7x^6 + 6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1}{x^3 + x - 1}$;

4) $\dfrac{\sqrt{3}x^4 - \sqrt{2}x^3 + x - 2}{\sqrt{6}x^2 - x + 1}$;

5) $\dfrac{\frac{1}{5}x^5 + \frac{1}{4}x^4 - \frac{1}{3}x^3 - \frac{1}{2}x^2 + x}{\frac{1}{120}x - \frac{1}{240}}$;

6) $\dfrac{x^7 + 1}{x + 1}$.

Definición. *Dados dos polinomios de una variable, que llamaremos dividendo y divisor (siendo el divisor siempre distinto de 0), la división consiste en encontrar otros dos polinomios, denominados cociente y resto, de tal manera que:*

$$\begin{aligned} \textit{Dividendo} &= \textit{Divisor} \times \textit{Cociente} + \textit{Resto} \\ & \quad \operatorname{grad}(\textit{Resto}) < \operatorname{grad}(\textit{Divisor}). \end{aligned}$$

Poseemos una técnica para encontrar cociente y resto, pero, a priori, nadie nos puede asegurar que, por medio de otro procedimiento, no fuera posible encontrar un cociente y resto distintos. Sin embargo eso no ocurre: "el cociente y el resto son únicos".

Supongamos por un momento que tenemos dos expresiones:

$$\begin{aligned} P &= D \times C + R, \quad \operatorname{grad}(R) < \operatorname{grad}(D) \\ P &= D \times Q + S, \quad \operatorname{grad}(S) < \operatorname{grad}(D). \end{aligned}$$

Restando estas expresiones quedaría:

$$D \times (C - Q) = S - R.$$

Ahora bien, si $C - Q$ fuera distinto de cero, tendríamos que

$$\operatorname{grad}(D \times (C - Q)) = \operatorname{grad}(D) + \operatorname{grad}(C - Q) \geq \operatorname{grad}(D) > \operatorname{grad}(S - R),$$

lo cual es absurdo si es que se tiene la igualdad: $D \times (C - Q) = S - R$.

La única escapatoria posible a este dilema es que $C = Q$ y $S = R$. Es decir, hagamos como hagamos la división (siempre que no nos equivoquemos al operar, ¡claro!), el cociente y el resto que encontremos van a ser los mismos.

Si al dividir P por Q obtenemos resto cero, diremos que la división es exacta, que P es un múltiplo de Q, o bien que Q es un divisor de P.

Las constantes no nulas, o polinomios de grado cero, son divisores universales: todo polinomio $P(x)$ es siempre divisible por un número $q \neq 0$:

$$\frac{3x^2 - 2x + 1}{7} = \frac{3}{7}\,x^2 - \frac{2}{7}\,x + \frac{1}{7}\,,$$

y el resto es cero.

Si $q \neq 0$ es un número y $P(x) \neq 0$ un polinomio, entonces $Q(x) = qP(X)$ es un divisor de $P(x)$:

$$\frac{P(x)}{Q(x)} = \frac{1}{q}\,,$$

y el resto es cero.

Las siguientes son divisiones exactas:

$$\begin{aligned}
\frac{x^2-1}{x-1} &= x+1\\
\frac{x^3-1}{x-1} &= x^2+x+1\\
\frac{x^4-1}{x-1} &= x^3+x^2+x+1\\
\frac{x^5-1}{x-1} &= x^4+x^3+x^2+x+1\\
&\quad \textit{en general:}\\
\frac{x^n-1}{x-1} &= x^{n-1}+x^{n-2}+x^{n-3}+\cdots+x+1.
\end{aligned}$$

Una aplicación curiosa:

$$1+3+3^2+3^3+3^4=\frac{3^5-1}{3-1}=121.$$

¿Cuánto vale la suma $1+5+5^2+5^3+5^4+5^5+5^6$*?*

División de un polinomio por el binomio $x-a$

Si dividimos un polinomio, $P(x)$*, por el binomio* $x-a$*, el cociente,* $Q(x)$*, será un polinomio de grado una unidad inferior al de* $P(x)$*, pero el resto,* $R(x)$*, ha de ser una constante:*

$$P(x)=(x-a)Q(x)+R.$$

En particular, si sustituimos el valor $x=a$ *en la identidad anterior, obtenemos:*

$$P(a)=(a-a)Q(a)+R=R, \qquad \textit{esto es: } \boxed{R=P(a)}$$

En otras palabras: el resto de la división del polinomio $P(x)$ *por el binomio* $x-a$ *es el valor obtenido al sustituir* x *por* a *en el polinomio* $P(x)$*.*

Ejemplos:

$$\begin{array}{rl}
x^4-2x^3-x^2+3x-7 & \big|\, x-2\\
\cline{2-2}
-x^4+2x^3 & x^3-x+1\\
\cline{1-1}
-x^2+3x-7 & \\
x^2-2x & \\
\cline{1-1}
x-7 & \\
-x+2 & \\
\cline{1-1}
-5 &
\end{array}$$

$$\boxed{\textit{Resto}=-5=2^4-2\cdot 2^3-2^2+3\cdot 2-7}$$

$$
\begin{array}{rl}
x^5-7x^4+x^3-3x^2+x-1 & \big| \, x-1 \\
\cancel{-x^5+x^4} & \hline \\
-6x^4+x^3-3x^2+x-1 & x^4-6x^3-5x^2-8x-7 \\
\cancel{6x^4+6x^3} & \\
-5x^3-3x^2+x-1 & \\
\cancel{5x^3-5x^2} & \\
-8x^2+x-1 & \\
\cancel{8x^2-8x} & \\
-7x-1 & \\
\cancel{7x-7} & \\
-8 &
\end{array}
$$

$$\boxed{Resto = -8 = 1^5 - 7\cdot 1^4 + 1^3 - 3\cdot 1^2 + 1 - 1}$$

En particular, tenemos que el polinomio $P(x)$ es divisible por el binomio $x-a$ si y solo si $P(a)=0$.

Recordemos que a los números que verifican la identidad $P(a)=0$ les hemos llamado las raíces del polinomio. Por lo tanto, podemos afirmar que el número a es raíz del polinomio $P(x)$ si y solo si este es divisible por el binomio $x-a$.

Regla de Ruffini. *La llamada regla de Ruffini consiste en una manera rápida de realizar la división por el binomio $x-a$. Veamos nuestro primer ejemplo de división:*

$$\frac{x^4-2x^3-x^2+3x-7}{x-2} = x^3-x+1+\frac{-5}{x-2}.$$

El primer monomio del cociente, x^3, tiene grado 3 y coeficiente 1, que es igual al coeficiente del monomio x^4 en el dividendo. El coeficiente de x^2 en el cociente, $C(x)$, es

$$0 = (-2) + 2\cdot 1 = \text{coeficiente de } x^3 \text{ en } P(x) + 2\cdot(\text{coeficiente anterior de } C(x)),$$

y así sucesivamente:

$$\begin{aligned} -1 &= -1 + 2\cdot 0, \\ 1 &= 3 + 2\cdot(-1) \\ Resto = -5 &= -7 + 2\cdot 1. \end{aligned}$$

En general, la regla de Ruffini, para dividir un polinomio $P(x)$ entre el binomio $x-a$, sigue los siguientes pasos:

1º) Se escribe el polinomio de manera que aparezcan todas las potencias de x menores o iguales que el grado. Si una de ellas no estaba presente se le asigna coeficiente 0:

$$P(x) = \sum_{k=0}^{n} a_k x^k, \operatorname{grad}(P) = n \;\longrightarrow\; a_n\ a_{n-1}\ \ldots\ a_1\ a_0.$$

2º) *El grado del cociente es igual al del dividendo menos* 1*:*

$$\frac{P(x)}{x-a} = Q(x) + R \implies \text{grad}(Q(x)) = n-1,\ Q(x) = \sum_{j=0}^{n-1} b_j\, x^j.$$

3º) *El primer coeficiente del cociente (el de mayor grado) es igual al primer coeficiente del dividendo:*

$$b_{n-1} = a_n.$$

4º) *Cada uno de los demás coeficientes del cociente se obtiene multiplicando el anterior por* a *y sumando el resultado al coeficiente siguiente del dividendo:*

$$b_j = b_{j+1} \cdot a + a_{j+1}.$$

5º) *El resto es igual al último coeficiente del cociente multiplicado por* a *y sumado con el término independiente del dividendo:*

$$R = b_0 \cdot a + a_0.$$

En los ejemplos que siguen se utiliza una cómoda notación. En ella, puesto que basta conocer los coeficientes de $C(x)$*, hemos eliminado los monomios* x^k*.*

$$\frac{x^4 - 2x^3 - x^2 + 3x - 7}{x-2}$$

	1	-2	-1	3	-7
2	↓	2	0	-2	2
	1	0	-1	1	-5

$$Q(x) = x^3 - x + 1$$
$$R = -5.$$

$$\frac{2x^3 - x^2 + 3x + 4}{x-4}$$

	2	-1	3	4
4	↓	8	28	124
	2	7	31	128

$$Q(x) = 2x^2 + 7x + 31$$
$$R = 128.$$

Si a *es una raíz del polinomio* $P(x)$*, entonces podemos escribir*

$$P(x) = (x-a)Q(x),$$

y podría ocurrir que $Q(a) = 0$*. En tal caso, el polinomio* $Q(x)$ *también será divisible por* $x - a$*:*

$$Q(x) = (x-a)S(x) \implies P(x) = (x-a)^2 S(x),$$

y resulta que $P(x)$ *es divisible por* $(x-a)^2$*.*

En general, dada una raíz a del polinomio $P(x)$, podemos considerar el mayor entero positivo, m, tal que $(x-a)^m$ sea un divisor de $P(x)$. Es decir: $(x-a)^m$ es un divisor de $P(x)$, pero $(x-a)^{m+1}$ no lo es.

A dicho entero positivo, m, le llamaremos la multiplicidad de la raíz. Si $m=1$, la raíz se dice simple; si $m=2$, doble; ...

Ejemplos: a) $x^3-x^2-x+1=(x-1)^2(x+1)$

$$\begin{aligned} x=1 &\quad \text{es una raíz doble} \\ x=-1 &\quad \text{es una raíz simple.} \end{aligned}$$

b) $x^5-6x^4+13x^3-14x^2+12x-8=(x-2)^3(x^2+1)$

$$x=2 \quad \text{es una raíz triple.}$$

Supongamos que el polinomio $P(x)$ tiene las raíces:

$$\begin{aligned} &a \text{ con multiplicidad } r \\ &b \text{ con multiplicidad } s \\ &c \text{ con multiplicidad } t \\ &\dots \end{aligned}$$

Entonces, $P(x)=(x-a)^rQ(x)$, y como $P(b)=0$, resulta que b es una raíz de $Q(x)$ con multiplicidad s. Luego $Q(x)=(x-b)^sR(x)$, y $P(x)=(x-a)^r(x-b)^sR(x)$, para cierto polinomio $R(x)$. De nuevo, $P(c)=0$ y la multiplicidad de c, implica que $R(x)=(x-c)^tS(x)$, y, por tanto, $P(x)=(x-a)^r(x-b)^s(x-c)^tT(x)$, y así sucesivamente.

Luego el polinomio $P(x)$ se factoriza en la forma siguiente:

$$P(x)=(x-a)^r(x-b)^s(x-c)^t\cdots M(x),$$

donde el polinomio $M(x)$ carece de raíces. Podría ocurrir que $M(x)$ fuese constante, en cuyo caso el polinomio $P(x)$ se descompone totalmente en producto de binomios pero: ¿es esa la única posibilidad?

Si calculamos el grado de ambos miembros de la identidad anterior, obtenemos:

$$\begin{aligned} \operatorname{grad}(P(x)) &= r+s+t+\cdots+\operatorname{grad}(M(x)) \\ &\geq r+s+t+\cdots \end{aligned}$$

Parafraseando esta desigualdad diremos que: el número total de raíces reales o complejas (cada una contada tantas veces como indica su multiplicidad) es siempre menor o igual que el grado del polinomio. De hecho es siempre igual, pero eso lo analizaremos a continuación.

9.6. Teorema Fundamental del Álgebra

Hay polinomios que carecen de raíces reales, tales como x^2+1. Recordemos que la razón de ser de los números complejos es precisamente esta: resolver la ecuación $x^2+1=0$, cuyas "raíces complejas" son $+i$ y $-i$.

Cuando se estudian las ecuaciones de segundo grado ($ax^2+bx+c=0$), se observa que si el discriminante es negativo, $b^2-4ac<0$, entonces, para resolverlas hay que usar también los números complejos. Todo trinomio ax^2+bx+c se factoriza en la forma:

$$ax^2+bx+c=a(x-r_1)(x-r_2)$$

donde

$$r_1=\frac{-b+\sqrt{b^2-4ac}}{2a},\quad r_2=\frac{-b-\sqrt{b^2-4ac}}{2a}\,.$$

El fenómeno es más general y válido para todo polinomio $P(x)$, cualquiera que sea su grado. Con la ayuda de los números complejos todo polinomio de grado $n\geq 1$ se descompone en un producto de n binomios, aunque algunos pueden repetirse por corresponder a las raíces múltiples:

$$P(x)=a_n(x-r_1)\cdots(x-r_n).$$

Ejemplos:

$$x^2+1=(x-i)(x+i)$$
$$x^5-4x^4+9x^3-18x^2+20x-8=(x-1)^2(x-2)(x+2i)(x-2i).$$

Este resultado recibe el nombre de Teorema Fundamental del Álgebra, y fue demostrado por C. F. Gauss.

Teorema. *Todo polinomio $P(x)\in\mathbb{C}[x]$ de grado $n\geq 1$ tiene exactamente n raíces en $\mathbb{C}$ (contadas con su multiplicidad).*

Demostración. *Basta con probar que un polinomio $P(x)$ de grado $n\geq 1$ tiene siempre una raíz en $\mathbb{C}$. La razón estriba en que podemos escribir $P(x)=(x-r_1)P_1(x)$, siendo $P_1(x)$ un polinomio de grado $n-1$. Ahora bien, si $n-1\geq 1$, $P_1(x)$ tendrá a su vez una raíz, r_2, de donde $P_1(x)=(x-r_2)P_2(x)$, y $P(x)=(x-r_1)(x-r_2)P_2(x)$, esto es, r_2 también será raíz de $P(x)$. Iterando este procedimiento, obtendremos la factorización total de $P(x)$ en factores lineales, uno por cada raíz.*

La prueba de que un polinomio de grado $n\geq 1$ tiene al menos una raíz en $\mathbb{C}$ se hace por reducción al absurdo.

Supongamos que $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *carece de raíz en* $\mathbb{C}$. *La contradicción se obtiene en la siguiente serie de pasos:*

1º) Como $|P(z)| \geq \frac{1}{2}|z|^n$, *siempre que* $|z| \geq 1 + 2(|a_{n-1}| + \cdots |a_0|)$, *podemos concluir que la función* $|P(z)|$ *alcanzará su valor mínimo en un punto* z_0:

$$\min_{z\in\mathbb{C}} |P(z)| = |P(z_0)| > 0.$$

2º) El polinomio $P(x) - P(z_0)$ *se anula en* $x = z_0$, *y puede escribirse en la forma:*

$$P(x) - P(z_0) = (x - z_0)^m \left(b_0 + b_1(x - z_0) + \cdots + b_{n-m}(x - z_0)^{n-m}\right),$$

siendo el coeficiente $b_0 \neq 0$, *y* $m \geq 1$. *Es decir:*

$$P(x) = P(z_0) + b_0(x - z_0)^m + (x - z_0)^{m+1}Q(x)$$
$$Q(x) = b_1 + b_2(x - z_0) + \cdots + b_{n-m}(x - z_0)^{n-m-1}.$$

Sea $b_0 = |b_0|e^{i\varphi}$, *y tomemos* x *recorriendo la circunferencia centrada en* z_0 *y de radio* $\varepsilon > 0$: $x = z_0 + \varepsilon e^{i\theta}$ *con* $0 \leq \theta < 2\pi$. *Se obtiene entonces que:*

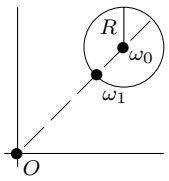
$$P(z_0 + \varepsilon e^{i\theta}) = P(z_0) + |b_0|\varepsilon^m e^{i(m\theta+\varphi)} + \varepsilon^{m+1}e^{i(m+1)\theta}Q(z_0 + \varepsilon e^{i\theta}).$$

Observemos que cuando θ *recorre el intervalo* $[0, 2\pi)$, *el punto*

$$\omega = P(z_0) + |b_0|\varepsilon^m e^{i(m\theta+\varphi)}$$

da m *vueltas a la circunferencia centrada en* $\omega_0 = P(z_0)$ *y radio*

$$R = |b_0|\varepsilon^m.$$



El punto ω_1 *(ver figura) de esa circunferencia está a una distancia del origen estrictamente menor que* ω_0. *Sea* $\omega_1 = P(z_0) + |b_0|\varepsilon^m e^{i(m\theta_1+\varphi)}$, *tenemos que:*

$$|\omega_1| = |\omega_0| - |b_0|\varepsilon^m.$$

Tomando ε *suficientemente pequeño obtenemos:*

$$\begin{aligned}\left|P(z_0 + \varepsilon e^{i\theta_1})\right| &\leq |\omega_1| + \varepsilon^{m+1} \max_{0\leq\theta<2\pi} \left|Q(z_0 + \varepsilon e^{i\theta})\right| \\ &\leq |\omega_0| - |b_0|\varepsilon^m + \varepsilon^{m+1} \max_{0\leq\theta<2\pi} \left|Q(z_0 + \varepsilon e^{i\theta})\right| \\ &\leq |\omega_0| - \frac{1}{2}|b_0|\varepsilon^m \ < \ |P(z_0)|,\end{aligned}$$

siempre que $\varepsilon < \min(|b_0|/2M, 1)$, *siendo* $M = \max_{|z|\leq 1} |Q(z_0 + z)|$.

Pero esto contradice la hipótesis inicial de que $|P(z)|$ *alcanzaba su valor mínimo en* z_0. ■

Es notable que los números complejos fuesen creados para encontrar las raíces de la ecuación $x^2+1=0$, y ahora resulte que cualquier polinomio $P(x)\in\mathbb{C}[x]$ de grado ≥ 1 tenga n raíces en $\mathbb{C}$. Esta propiedad recibe un nombre: el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado. Todo polinomio $P(x)\in\mathbb{C}[x]$ de grado ≥ 1 se descompone en producto de binomios lineales.

Dentro de $\mathbb{C}[x]$ está el subconjunto $\mathbb{R}[x]$ de los polinomios cuyos coeficientes son números reales. Sea $P(x)\in\mathbb{R}[x]$ y $z\in\mathbb{C}$ una raíz:

$$\begin{aligned} &P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \quad a_j\in\mathbb{R}\\ &P(z)=0, \quad z\in\mathbb{C}. \end{aligned}$$

Si tomamos conjugados complejos resulta que:

$$\begin{aligned} 0=\overline{P(z)} &= \overline{a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0}\\ &= \overline{a_n}\,(\overline{z})^n+\overline{a_{n-1}}\,(\overline{z})^{n-1}+\cdots+\overline{a_1}\,\overline{z}+\overline{a_0}\\ &= a_n\,(\overline{z})^n+a_{n-1}\,(\overline{z})^{n-1}+\cdots+a_1\,\overline{z}+a_0 \;=\; P(\overline{z}), \end{aligned}$$

puesto que al ser los coeficientes reales, $\overline{a_j}=a_j$.

CONCLUSIÓN: *Si $P(x)\in\mathbb{R}[x]$ es un polinomio con coeficientes reales, sus raíces son, o bien reales, $x_1,\ldots,x_r$, o bien las encontramos en parejas, z_1, $\overline{z_1}$, $\ldots$, z_s, $\overline{z_s}$, de números complejos conjugados con parte imaginaria no nula.*

Sean $m_1,\ldots,m_r$ las multiplicidades respectivas de las raíces reales y $n_1,\ldots,n_s$ las de los pares de raíces complejas, entonces:

$$\begin{aligned} P(x)=a_n(x-x_1)^{m_1}\ldots(x-x_r)^{m_r}\big((x-z_1)(x-\overline{z_1})\big)^{n_1}\ldots\big((x-z_s)(x-\overline{z_s})\big)^{n_s},\\ n=m_1+\cdots+m_r+2(n_1+\cdots+n_s). \end{aligned}$$

Observemos que

$$(x-z_j)(x-\overline{z_j})=x^2-2\mathrm{Re}(z_j)x+|z_j|^2$$

es un trinomio cuadrático de coeficientes reales. Luego todo polinomio $P(x)$ de coeficientes reales se descompone en producto de binomios lineales y de trinomios cuadráticos del anillo $\mathbb{R}[x]$. Los binomios corresponden a las raíces reales de $P(x)$, mientras que cada trinomio se hace cargo de un par de raíces complejas conjugadas; por ejemplo:

$$x^6-5x^5+11x^4-15x^3+14x^2-10x+4=(x-1)(x-2)(x^2+1)(x^2-2x+2).$$

9.7. Factorización en $\mathbb{Q}[x]$ y en $\mathbb{Z}[x]$

La divisibilidad en los anillos de polinomios $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$ resulta algo más compleja que en $\mathbb{C}[x]$ donde, como hemos visto antes, los únicos polinomios irreducibles son los binomios $x-a$, $a \in \mathbb{C}$; o en $\mathbb{R}[x]$, en cuyo caso a los binomios $x-a$, $a \in \mathbb{R}$, hay que añadir los trinomios x^2+bx+c, con $b, c \in \mathbb{R}$ y $b^2-4ac < 0$. Por el contrario, ocurre que en $\mathbb{Q}[X]$ hay polinomios irreducibles de cualquier grado, es decir polinomios que no pueden descomponerse en producto de otros de grado estrictamente menor.

La factorización en $\mathbb{Z}[X]$ y en $\mathbb{Q}[x]$ están estrechamente relacionadas. Diremos que un polinomio $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ del anillo $\mathbb{Z}[x]$ es primitivo si el máximo común divisor de sus coeficientes es igual a 1.

Lema. *Si $P(x)$ y $Q(x)$ son polinomios primitivos entonces también lo es su producto $P \cdot Q$.*

Demostración. *Sean:*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0\,, \qquad a_n \neq 0$$
$$Q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0\,, \qquad b_m \neq 0.$$

Entonces $P \cdot Q = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \ldots + c_0$ donde:

$$c_r = \sum_{j+k=r} a_j\, b_k.$$

Si $P \cdot Q$ no fuera primitivo habría un primo p divisor de todos sus coeficientes: $p \mid c_r$, $r = 0, 1, \ldots, m+n$. Pero esto no puede ocurrir por la razón siguiente: Sean a_i, b_j los primeros coeficientes de P y Q, respectivamente, que no son divisibles por p, tenemos que:

$$c_{i+j} = a_i\, b_j + \sum_{\substack{s+t=i+j \\ s\neq i,\, t\neq j}} a_s\, b_t = a_i\, b_j + C.$$

Pero p resulta ser un divisor de C (porque lo es de cada uno de los sumandos $a_s\, b_t$ ya que la condición $s+t = i+j$, $s \neq i$, $t \neq j$ implica que ora $s < i$ ya $t < j$. Es decir o bien $p \mid a_s$ o bien $p \mid b_t$) y esto es una contradicción con el hecho de que $p \mid c_{i+j}$ mientras que p no es divisor del producto $a_i b_j$. ■

Lema. (Gauss) *Un polinomio con coeficientes enteros que puede descomponerse en factores polinómicos con coeficientes racionales, puede también descomponerse en factores del mismo grado pero de coeficientes enteros.*

Demostración. *Observemos en primer lugar que podemos suponer, sin pérdida de generalidad, que el polinomio es primitivo.*

Sea pues $P(x)$ un polinomio primitivo y $P = Q \cdot R$ una factorización donde los polinomios $Q(x)$ y $R(x)$ pertenecen al anillo $\mathbb{Q}[x]$. Entonces existen dos

enteros q y r tales que $\widetilde{Q}(x) = q\,Q(x)$ y $\widetilde{R}(x) = r\,R(x)$ son primitivos en $\mathbb{Z}[x]$ y $\widetilde{P} = \widetilde{Q}\,\widetilde{R}$ es un polinomio primitivo en $\mathbb{Z}[x]$ que verifica la identidad $\widetilde{P} = q\,r\,P$. Ahora bien, por ser $\widetilde{P}$ y P primitivos la única posibilidad es que tengamos $q \cdot r = \pm 1$; es decir, $q = 1$ (o -1) y $r = \pm 1$. Y esto nos permite concluir fácilmente la demostración. ■

La factorización de un polinomio en producto de irreducibles es muy laboriosa, aunque existen procedimientos sistemáticos para llevarla a cabo. En este empeño son también muy importantes los criterios de irreducibilidad. Uno especialmente sencillo se debe a Eisenstein y dice lo siguiente:

Proposición. *Sea $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$, un polinomio con coeficientes enteros tal que existe un número primo p que satisface las siguientes condiciones:*

$$a_n \not\equiv 0 \ mod(p)\,, \quad a_{n-1} \equiv a_{n-2} \equiv \ldots \equiv a_0 \equiv 0 \ mod(p) \ \text{ y } a_0 \not\equiv 0 \ mod(p^2).$$

Entonces $P(x)$ es irreducible en $\mathbb{Z}[x]$ (y en $\mathbb{Q}[x]$).

Demostración. *Sea una factorización*

$$P(x) = \big(b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0\big)\big(c_j x^j + c_{j-1}x^{j-1} + \ldots + c_0\big)$$

en la que, por el lema de Gauss, podemos suponer que los factores tienen coeficientes enteros b_r, c_s. Como $a_0 = b_0 c_0$ y $a_0 \not\equiv 0\, mod(p^2)$ uno de los dos coeficientes b_0, c_0 no es divisible por p. Sin pérdida de generalidad podemos suponer que $b_0 \not\equiv 0\, mod(p)$ y $c_0 \equiv 0 \ mod(p)$.

Sea s el menor índice $\leq j$ tal que $0 \equiv c_0 \equiv \ldots \equiv c_{r-1} \ mod(p)$ pero $c_r \not\equiv 0\, mod(p)$. Tenemos que:

$$a_s = b_0 c_r + b_1 c_{r-1} + \ldots + b_r c_0 \equiv b_0 c_r \ mod(p)$$

y como $b_0 \not\equiv 0\, mod(p)$, $c_r \not\equiv \ mod(p)$ y p es primo, resulta que $a_s \not\equiv 0\, mod(p)$.

Por hipótesis esto solo puede ocurrir con el coeficiente a_n, luego $s = n$. Es decir el grado del segundo factor es igual al de $P(x)$ por lo que este es irreducible. ■

Corolario. *El polinomio llamado ciclotómico $P(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$ asociado a un primo p es irreducible.*

Demostración. *El cambio de variable $x = y + 1$ convierte $P(x)$ en $Q(y) = P(y+1)$. Es claro que si P fuese reducible también lo tendría que ser $Q(y)$. Ahora bien*

$$Q(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + p\,y^{p-2} + \binom{p}{2} y^{p-3} + \ldots + \binom{p}{p-2} y + p$$

y este polinomio satisface las condiciones del criterio de Eisenstein, luego es irreducible como lo es también $P(x)$. ■

Ejercicios

1) *Formular el algoritmo de Euclides en $\mathbb{Q}[x]$ y demostrar que dados dos polinomios $f(x)$ y $g(x)$, el último resto no nulo del algoritmo es el máximo común divisor de f y g.*

2) *Usar el ejercicio anterior para representar $d(x) = m.c.d.(f, g)$ en la forma*

$$d(x) = \alpha(x)\, f(x) + \beta(x)\, g(x)$$

donde α y β son también polinomios.

3) *Determinar la irreducibilidad de los siguientes polinomios en $\mathbb{Q}[x]$:*

$$x^3 + 2x^2 + 6x + 2\,, \quad x^5 - 4\,, \qquad x^3 - 1\,,$$
$$x^3 + x^2 - 5x - 2\,, \quad x^5 + 2x^4 + 8x^3 + 2x^2 + 4x + 16.$$

9.8. Números algebraicos y números trascendentes

Las raíces de los polinomios con coeficientes racionales se llaman números algebraicos.

Todo racional q es algebraico ya que es raíz del polinomio $x - q$; pero también lo son $\sqrt{2}$ e $i = \sqrt{-1}$ por ser raíces, respectivamente, de $x^2 - 2$ y $x^2 + 1$. Los números que no son algebraicos son llamados trascendentes.

Es claro que si un número es raíz de un polinomio con coeficientes racionales también lo es de otro con coeficientes enteros (el obtenido multiplicando por el mínimo común múltiplo de los denominadores de los coeficientes). Por tanto una definición equivalente de número algebraico es pedir que sea raíz de un polinomio de $\mathbb{Z}[x]$. Como los polinomios de $\mathbb{Z}[x]$ se descomponen en producto de factores irreducibles, todo número algebraico es raíz de un polinomio irreducible y primitivo. Resulta fácil ver que este es único (salvo multiplicación por -1) y se denomina el polinomio mínimo del número algebraico.

Si $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$, es el polinomio mínimo de α entonces $P'(\alpha) \neq 0$ y, por lo tanto, α es una raíz simple de su polinomio mínimo, siendo $P'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$ el polinomio derivado de P (ejercicio). Las otras raíces de P son los conjugados algebraicos de α.

No es difícil demostrar que los números algebraicos forman un cuerpo contenido en los complejos: la suma, el producto y el cociente de algebraicos (siempre que el divisor sea distinto de 0) también pertenecen al club.

Sabemos que el conjunto $\mathbb{Z}[x]$ es numerable y que un polinomio de grado n tiene, a lo sumo, n raíces distintas en $\mathbb{C}$. Luego el conjunto de los números algebraicos es numerable, por ser unión numerable de conjuntos finitos. Por el contrario el conjunto de los trascendentes es no–numerable, y su cardinal es el continuo. Hay pues muchos más trascendentes que algebraicos, pero: ¿podemos identificar a un número trascendente?

El primero que pudo dar una respuesta afirmativa fue J. Liouville en 1844, *demostrando que el número*

$$\lambda = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

es trascendente.

Proposición. (Liouville) *Si α es algebraico de grado $n \geq 2$ entonces existe una constante positiva $c_\alpha > 0$ tal que:*

$$\left|\alpha - \frac{p}{q}\right| \geq c_\alpha \, \frac{1}{q^n}$$

para toda fracción irreducible $\dfrac{p}{q}$.

Demostración. *Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ el polinomio mínimo de α. Sin pérdida de generalidad podemos suponer que la fracción irreducible $\frac{p}{q}$ verifica la desigualdad*

$$\left|\alpha - \frac{p}{q}\right| \leq 1$$

(ya que si fuera $|\alpha - \frac{p}{q}| > 1$ no habría nada que demostrar). El teorema del valor medio nos permite escribir:

$$\left|f\left(\tfrac{p}{q}\right)\right| = \left|f\left(\tfrac{p}{q}\right) - f(\alpha)\right| = \left|f'(c)\right| \cdot \left|\frac{p}{q} - \alpha\right|$$

donde c es un punto entre α y $\frac{p}{q}$.

La irreducibilidad de f nos asegura que

$$0 \neq \left|f\left(\tfrac{p}{q}\right)\right| = \left|\sum_{k=0}^{n} a_k \left(\tfrac{p}{q}\right)^k\right| = \frac{1}{q^n}\left|a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_0 q^n\right| \geq \frac{1}{q^n}.$$

Luego:

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{q^n} \min_{|c-\alpha|\leq 1} \frac{1}{|f'(c)|} = \frac{1}{q^n} \, \frac{1}{\max\limits_{|c-\alpha|\leq 1} |f'(c)|} = c_\alpha \, \frac{1}{q^n} \, .$$

■

Esta proposición nos permite demostrar que, cualquiera que sea n, el número λ de Liouville no puede ser la raíz de un polinomio de grado n y coeficientes enteros. En otras palabras que λ es trascendente:

$$\begin{aligned}\lambda - \sum_{k=1}^{n} \frac{1}{10^{k!}} &= \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \dots \\ &\le \frac{1}{10^{(n+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \dots\right) \\ &= \frac{10}{9}\,\frac{1}{10^{(n+1)!}}\,.\end{aligned}$$

La demostración se concluye observando que:

$$\sum_{k=1}^{n} \frac{1}{10^{k!}} = \frac{p_n}{10^{n!}} \quad \textit{siendo } p_n \textit{ entero y} \quad \frac{1}{10^{(n+1)!}} = \frac{1}{\left(10^{n!}\right)^{n+1}}.$$

Ejercicio 10. *Demostrar que los números siguientes son trascendentes:*

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n^n}}\,, \quad \beta = \sum_{n=1}^{\infty} \frac{(-1)^n}{10^{n!}}\,, \quad \gamma = \sum_{n=1}^{\infty} \frac{n}{10^{n!}}\,.$$

Llamaremos número de Liouville a un número α tal que para todo n natural y para todo $\varepsilon > 0$ exista un número racional $\frac{p}{q}$ tal que $\left|\alpha - \frac{p}{q}\right| < \varepsilon\,\frac{1}{q^n}$. Según el teorema de Liouville tales números son trascendentes.

Ejercicio 11. *Demostrar que el conjunto de los números de Liouville no es numerable.*

En el año 1873 Hermite logró demostrar la trascendencia del número e. Unos años más tarde Lindemann extendió los métodos de Hermite para probar que π también lo es, dando respuesta final al problema de la cuadratura del círculo con regla y compás. Axel Thue, en el año 1909, mejoró el teorema de Liouville demostrando que para cualquier número algebraico α, de grado $n > 1$, y para cualquier entero $k > \frac{n}{2} + 1$, existe $c = c(\alpha, k) > 0$ tal que:

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^k}$$

para todas las fracciones irreducibles $\frac{p}{q}$.

El método de Thue marcó un camino que fue luego recorrido por Siegel, Dyson y Gelfond, entre otros, quienes produjeron sucesivas mejoras del resultado que culminaron en el teorema obtenido por Roth en el año 1955 y que le valió una Field Medal. La proposición anterior sigue siendo válida para todo real $k > 2$; y eso es lo mejor posible.

Teorema. *e es trascendente.*

Demostración. *Por reducción al absurdo: supondremos que e satisface una ecuación*

$$a_n e^n + a_{n-1} e^{n-1} + \ldots + a_1 e + a_0 = 0$$

con coeficientes enteros, tales que $a_n \neq 0$ *y* $a_0 \neq 0$*, y obtendremos una contradicción.*

Fijado un número primo p consideremos el polinomio

$$P(x) = x^{p-1}(x-1)^p \cdots (x-n)^p$$

y la función

$$I(y) = \int_0^y e^{y-x} P(x)\,\mathrm{d}\,x\,, \quad y \geq 0.$$

Sucesivas integraciones por partes nos permiten escribir:

$$I(y) = e^y \sum_{k=0}^{d} P^{(k)}(0) \; - \sum_{k=0}^{d} P^{(k)}(y)$$

donde $d = (n+1)p - 1$ *es el grado del polinomio* $P(x)$ *y* $P^{(j)}(z)$ *designa a la* j*–ésima derivada de* P *evaluada en* z*.*

A continuación consideremos el número:

$$A = a_0 I(0) + a_1 I(1) + \ldots + a_n I(n) = -\sum_{j=0}^{d} \sum_{k=0}^{n} a_k P^{(j)}(k).$$

Resulta que:

i) $P^{(j)}(k)$ *es un múltiplo de* $p!$ *si* $j \geq p$*.*

ii) $P^{(j)}(k) = 0$ *si* $j < p$ *y* $k > 0$ *o si* $j < p-1$ *y* $k = 0$*.*

iii) $P^{(j)}(k)$ *es un entero divisible por* $p!$ *excepto en el caso* $j = p-1$*,* $k = 0$*.*

iv) $P^{(p-1)}(0) = (p-1)!(-1)^{np}(n!)^p$*. Por tanto, si* $p > n$ *resulta que* $P^{(p-1)}(0)$ *es un entero divisible por* $(p-1)!$ *pero no por* $p!$*.*

Luego si $p > n$ *resulta que* A *es un entero no nulo y divisible por* $(p-1)!$ *En particular tenemos que* $|A| \geq (p-1)!$ *Ahora bien, la integral que define la función* $I(y)$ *verifica la acotación:*

$$|I(y)| \;\leq\; y e^y \sup_{0 \leq x \leq y} |P(x)| \;\leq\; y e^y (n+y)^d.$$

Sustituyendo en la expresión de A obtenemos:

$$|A| \leq \sum_{j=1}^{n} |a_j|\,|I(j)| \leq \sum_{j=1}^{n} |a_j|\, j\, e^j\, (n+j)^d \leq a^p$$

para una cierta constante positiva a.

Pero esto es absurdo ya que la desigualdad

$$(p-1)! \leq |A| \leq a^p$$

es falsa para cualquier a si p es suficientemente grande. ■

Un polinomio $P(x_1, \ldots, x_n)$ es simétrico si no varía cuando se permutan sus variables. Es decir $P(x_{\phi(1)}, \ldots, x_{\phi(n)}) = P(x_1, \ldots, x_n)$ para cualquier permutación ϕ del conjunto $\{1, 2, \ldots, n\}$. Ejemplos de polinomios simétricos son los siguientes:

$$\begin{aligned}
\Sigma_1(x_1, \ldots, x_n) &= x_1 + x_2 + \ldots + x_n \\
\Sigma_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\
\vdots \qquad & \qquad \vdots \\
\Sigma_n(x_1, \ldots, x_n) &= x_1 \cdot x_2 \cdots x_n.
\end{aligned}$$

Las Σ_j son las funciones simétricas elementales, y un resultado fundamental de la teoría afirma que si $P(x_1, \ldots, x_n)$ es un polinomio simétrico entonces existe otro polinomio Q de n variables tal que

$$P(x_1, \ldots, x_n) = Q\big(\Sigma_1(x_1, \ldots, x_n), \ldots, \Sigma_n(x_1, \ldots, x_n)\big).$$

Además, si P tiene sus coeficientes enteros (racionales) entonces Q también los tiene enteros (racionales).

Supongamos que α y β son dos números algebraicos y $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $Q(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$ son los dos polinomios irreducibles, de coeficientes racionales, tales que $P(\alpha) = 0$ y $Q(\beta) = 0$. Sean $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_n$ y $\beta_1 = \beta$, $\beta_2, \ldots, \beta_m$ todas las raíces complejas de P y Q. Entonces tenemos que

$$P(x) = (x - \alpha_1) \cdots (x - \alpha_n), \qquad Q(x) = (x - \beta_1) \cdots (x - \beta_m),$$

y el teorema fundamental de las funciones simétricas nos permite concluir que los dos polinomios siguientes tienen también coeficientes racionales:

$$S(x) = \prod_{j,k} (x - \alpha_j - \beta_k), \qquad T(x) = \prod_{j,k} (x - \alpha_j\beta_k)$$

lo que implica que $\alpha + \beta$ y $\alpha\beta$ son números algebraicos.

Teorema. (Lindemann) *π es trascendente.*

Demostración. *Supongamos lo contrario, es decir que π y, por tanto, $i\pi$ son números algebraicos. Sean $\alpha_1 = i\pi$, $\alpha_2, \ldots, \alpha_n$ todas las raíces del polinomio irreducible de coeficientes enteros satisfecho por $i\pi$:*

$$P(x) = a_n x^n + \ldots + a_0 = a_n(x-\alpha_1)\cdots(x-\alpha_n).$$

Habida cuenta de que $e^{i\pi} = -1$, tenemos que

$$0 = (1+e^{\alpha_1})\cdot(1+e^{\alpha_2})\cdots(1+e^{\alpha_n}),$$

que podemos escribir de la siguiente manera:

$$0 = \nu + e^{\beta_1} + \ldots + e^{\beta_m}$$

donde los exponentes no nulos β_j provienen del desarrollo del producto:

$$\beta_j = \varepsilon_1(j)\alpha_1 + \varepsilon_2(j)\alpha_2 + \ldots + \varepsilon_n(j)\alpha_n, \qquad \varepsilon_k(j) = 0, 1;$$

mientras que $\nu = 2^n - m \geq 1$ designa al número de exponentes nulos.

Análogamente a lo que hicimos en la demostración de Hermite, consideremos la integral

$$I(y) = \int_0^y e^{y-x} Q(x)\,\mathrm{d}\,x$$

$$Q(x) = a_n^{mp} x^{p-1}(x-\beta_1)^p \cdots (x-\beta_m)^p$$

siendo p un primo suficientemente grande. Integrando por partes obtenemos:

$$A = I(\beta_1) + \ldots + I(\beta_m) = -\nu \sum_{j=0}^{d} Q^{(j)}(0) \; - \; \sum_{j=0}^{d}\sum_{k=1}^{m} Q^{(j)}(\beta_k)$$

donde $d = (m+1)p - 1 = \mathrm{grad}(Q(x))$. Ocurre que la suma $\sum_{k=1}^{m} Q^{(j)}(\beta_k)$ es simétrica en

$$a_n\beta_1, \ldots, a_n\beta_m$$

con coeficientes enteros y, por tanto, es también un polinomio simétrico con coeficientes enteros en $a_n\alpha_1, \ldots, a_n\alpha_n$. Por el teorema fundamental sabemos entonces que esa suma es un entero.

Ahora bien, $Q^{(j)}(\beta_k) = 0$ cuando $j < p$, y es un múltiplo de $p!$ cuando $j \geq p$. Por lo tanto $\sum_{k=1}^{m} Q^{(j)}(\beta_k)$ es un múltiplo de $p!$

También $Q^{(j)}(0)$, $j \neq p-1$, *es un entero divisible por* $p!$ *Pero*

$$Q^{(p-1)}(0) = (p-1)!(-a_n)^{mp}(\beta_1 \cdots \beta_m)^p$$

es divisible por $(p-1)!$ *pero no por* $p!$, *si* p *es suficientemente grande.*

Resumiendo: desde un valor de p *en adelante resulta que*

$$(p-1)! \leq |A|.$$

Pero por razones idénticas a las que encontramos en la demostración de Hermite, resulta que $|A| \leq a^p$ *para cierto número* a.

Como la desigualdad $(p-1)! \leq a^p$ *es falsa si el primo* p *es suficientemente grande, obtenemos una contradicción en la hipótesis de que* π *es algebraico. Luego* π *es trascendente.* ■

Construcciones geométricas: Los tres problemas de los griegos

> *... El emperador Hui–Tsung pintó con exquisito cuidado en el detalle una codorniz y un narciso. El pájaro y la flor no ocupan en la hoja del álbum el centro del espacio iluminado, sino un lugar de más ligera luz en la esquina derecha. Aunque pintados con la pericia de un experto en la contemplación de la naturaleza, ni pájaro ni flor pueden ser centro, sino tan solo indicación del centro o guía del ojo que los mira para alcanzar la forma no visible en que pájaro y flor están inscritos. Del poder y la gloria, de las victorias militares poco supo el monarca derrotado. Sobreviven, en cambio, en una esquina de luz atenuada el pájaro y la flor. Señalar una esquina ya es bastante, según Hui–Tsung sabía de Confucio. Para quienes no pueden hallar las otras tres inútil fuera repetirse.*
>
> José Ángel Valente

Los griegos de la época clásica formularon tres problemas de construcciones geométricas que devinieron famosos y que han tenido ocupados a los matemáticos durante muchos siglos. La solución ha necesitado de grandes dosis de ingenio y el desarrollo de teorías que no estaban al alcance de aquellos maravillosos pensadores. Pero las condiciones estaban perfectamente elegidas y las construcciones tenían que ser con regla y compás: la regla para unir pares de puntos con una recta y el compás para trazar circunferencias.

A partir de los puntos $(0,0)$, $(1,0)$ *y* $(0,1)$ *(o bien* 0, 1, i *del plano complejo) y con el uso exclusivo de la regla y el compás, ¿qué otros puntos del plano* $\mathbb{C}$ *podemos trazar?*

Resulta fácil obtener cualquier punto de coordenadas enteras $(m,n) \in \mathbb{Z} \times \mathbb{Z}$, *o racionales* $\mathbb{Q} \times \mathbb{Q}$, *pero también muchos de coordenadas irracionales tales como* $(\sqrt{2},0)$, $(\sqrt{2},\sqrt{3})$ *o* $(\sqrt{2}+\sqrt{5},\sqrt{3}+\sqrt{7})$, *etc.*

En general el número complejo $\alpha = x + iy = (x, y)$ es construible si lo son $(x, 0)$ y $(0, y)$, por lo que es equivalente hablar de puntos del plano $\mathbb{R} \times \mathbb{R}$ construibles o de números, complejos o reales, construibles.

Si el punto (a, b) es construible y también el radio r, entonces podemos trazar la circunferencia $(x - a)^2 + (y - b)^2 = r^2$. Si esta la intersecamos con una recta $y = c + mx$ donde c y m son construibles, los puntos de intersección se obtendrán resolviendo una ecuación de segundo grado que involucra a los números construibles a, b, r, c, m, a^2, b^2, r^2, c^2, m^2. Las soluciones, por lo tanto, introducirán combinaciones de raíces cuadradas de sumas y productos de esas cantidades.

La teoría de cuerpos de números, que no nos proponemos desarrollar aquí, permite precisar la observación anterior en el siguiente sentido:

a) *Un número construible se obtiene a partir de un número finito de racionales combinados, en un número finito de pasos, con las operaciones suma, producto y extracción de raíces cuadradas.*

b) *El grado del polinomio mínimo de un número construible es de la forma 2^n, para un entero positivo n.*

Ejemplos: $\sqrt{2}: \quad x^2 - 2;$

$$\sqrt{2} + \sqrt{3}: \quad x^4 - 10x^2 + 1.$$

Los tres problemas clásicos antes aludidos son:

1. ***Duplicación del cubo**: construir con regla y compás un cubo de volumen doble que otro dado.*
2. ***Cuadratura del círculo**: construir con regla y compás un cuadrado de área igual al círculo de radio unidad.*
3. ***Trisección del ángulo**: dado un ángulo dividirlo en tres partes iguales con la regla y el compás.*

Cuenta la leyenda que en tiempos en los que una plaga asolaba Atenas se enviaron dignatarios para consultar al Oráculo de Apolo sito en la isla de Delfos. Y el Oráculo respondió que la plaga remitiría duplicando exactamente el cubo del altar de Apolo.

Al parecer la primera medida que se tomó fue duplicar el lado del cubo y la plaga arreció, furiosos los dioses por tamaño error aritmético. Ante la dificultad de construir, con regla y compás (que era la única construcción

aceptable a los dioses del Olimpo), un cubo de doble volumen, los ciudadanos consultaron a Platón quien, sopesando la dificultad del problema, dijo que a los dioses seguramente no les importaba tanto el tamaño del altar como poner de manifiesto los pocos recursos que los atenienses dedicaban a las Matemáticas.

Ahora sabemos que dicha construcción es imposible, porque el número $\sqrt[3]{2}$ *no es construible ya que su polinomio mínimo es* $x^3 - 2$ *cuyo grado* 3 *es distinto de* 2^n *cualquiera que sea el entero positivo* n*.*

Tampoco se puede cuadrar el círculo porque π *es trascendente. La trisección del ángulo resulta algo diferente ya que algunos ángulos (por ejemplo el de* 90^o*) sí se pueden trisecar, pero la mayoría no ya que la trisección del ángulo* θ *implica que* $\cos(\theta/3)$ *sea un número construible, y hay muchos* θ *(por ejemplo* 60^o*) para los que eso no es cierto.*

Concluyamos invocando un conocido paradigma del Análisis Armónico, la descomposición de funciones integrables a la Calderón–Zygmund, un conocido paradigma del Análisis Armónico que ha dado lugar a un acertado aforismo: "Toda demostración que se precie ha de disponer siempre de un tiempo de parada oportuno". Creo sinceramente que ese principio puede también ser aplicado a la escritura de libros.

Símbolos

q.e.d.	*quod erat demostrandum, se emplea para indicar el fin de una demostración*
$\blacksquare$	*significa lo mismo que q.e.d.*
$\in$	*pertenece*
$\subset$	*inclusión*
$\cap$	*intersección*
$\cup$	*unión*
$\exists$	*existe*
$\forall$	*para todo*
$\mathbb{N}$	*conjunto de los números naturales*
$\mathbb{Z}$	*conjunto de los números enteros*
$\mathbb{Q}$	*conjunto de los números racionales*
$\mathbb{R}$	*conjunto de los números reales*
$\mathbb{C}$	*conjunto de los números complejos*
$\neg$	*negación lógica*
$\wedge$	*conjunción lógica: "y"*
$\vee$	*disyunción lógica: "o"*
$\Longrightarrow$	*implicación lógica*
$\vdash \mathcal{A}$	$\mathcal{A}$ *es un teorema*
$\sum_j x_j$	*suma de los números* x_j
$\prod_j x_j$	*producto de los números* x_j
m.c.d.	*máximo común divisor*
m.c.m.	*mínimo común múltiplo*
$n!$	*factorial de* n
$\binom{n}{k}$	*número combinatorio* n *sobre* k
$[x]$	*parte entera de* x
$\{x\}$	*parte fraccionaria de* x
$\lvert x\rvert$	*valor absoluto de* x
$f'(x)$	*derivada de* f
$\frac{\mathrm{d}^j}{\mathrm{d}x}(f) = D_x^j f$	*derivada* j*–ésima de* f
$\int_a^b f(x)\mathrm{d}\,x$	*integral de* f *en el intervalo* $[a, b]$

Bibliografía

[1] T. M. Apostol: *Introducción a la Teoría de los Números. Ed. Reverté, 1980.*

[2] G. Birkhoff y S. Mac Lane: *Álgebra Moderna. Ed. Vicens–Vives, 1963.*

[3] G. Chaitin: *Meta Math: the quest for Omega. Pansheon Books, N.Y., 2005.*

[4] G. Chaitin: *Algorithmic Information theory. Cambridge Univ. Press, 1987.*

[5] J. Cilleruelo y A. Córdoba: *La Teoría de los Números. Biblioteca Mondadori, 1992.*

[6] P. Cohen: *Set theory and the continuum hypothesis. Edit. W.A. Benjamin, 1966.*

[7] H. Davenport: *Multiplicative Number Theory. Springer–Verlag, segunda edición, 1980.*

[8] M. Davis: *What is a computation? Mathematics today: twelve informal essays. Springer–Verlag, 1978.*

[9] P. Davis y R. Hersch: *La experiencia matemática. Ed. Labor, 1989.*

[10] K. Devlin: *Sets functions and logic. Chapman and Hall, segunda edición, 1992.*

[11] J. Ferreirós: *El nacimiento de la teoría de conjuntos, 1854–1908. Ediciones de la Universidad Autónoma de Madrid, 1992.*

[12] J. Ferreirós: *Labyrinth of thought: A history of set theory and its role un modern mathematics. Birkhäuser, Verlag, 1999.*

[13] C. F. Gauss: *Disquisitiones Arithmeticae. Yale Univ. Press, 1966.*

[14] K. Gödel: *On indecidable propositions of formal mathematical systems. Princeton, 1934.*

[15] G. H. Hardy y E. M. Wright*: An introduction to the Theory of Numbers. Oxford, Clarendon Press, 1938.*

[16] D. R. Hofstadter*: Gödel, Escher, Bach: un Eterno y Grácil Bucle. Ed. Tusquets, edición en español, 1999.*

[17] E. Mendelson*: Mathematical logic. Ed. Van Nostrand, 1963.*

[18] J. Mosterín*: Los lógicos. Ed. Espasa, 2000.*

[19] E. Nagel y J. R. Newand*: Gödel's proof. N.Y. Univ. Press, edición revisada, 2002.*

[20] R. Penrose*: La nueva mente del emperador. Biblioteca Mondadori, 1991.*

[21] R. Penrose*: Las sombras de la mente. Crítica, Drakontos, 1994.*

[22] J. Rey Pastor, P. Pi Calleja y C. A. Trejo*: Análisis Matemático. Ed. Kapelusz, Buenos Aires, 1952.*

[23] T. Tymoczko*: New directions in the Philosophy of Mathematics. Princeton Univ. Press, 1998.*

[24] H. Wang*: Reflections on K. Gödel. The MIT Press, 1987.*

Índice alfabético