Un paseo alrededor de la teoría de conjuntos

por

José Luis Gómez Pardo

Introducción

La teoría de conjuntos ha ocupado, desde que Cantor la estableció como una disciplina independiente a finales del siglo XIX, un lugar especial en las matemáticas. A lo largo del siglo XX se ha ido generalizando la idea de que los conjuntos son un concepto fundamental debido a que proporcionan un lenguaje al cual, en cierto sentido, pueden reducirse todas las matemáticas. Esta idea ya estaba presente en la construcción de los números reales a partir de los enteros realizada por Dedekind y la teoría de conjuntos, desde el momento en que se formalizó con el objetivo de que pudiera servir para desarrollar las matemáticas al amparo de las amenazas planteadas por las paradojas surgidas a principios del siglo pasado, pasó a ser considerada como parte integrante de lo que se puede llamar *fundamentos de las matemáticas*. Una de las ideas básicas que justifican esta adscripción es la de que, en principio, se supone que cualquier demostración matemática se podría reducir a una deducción formal, en el sentido de la lógica, dentro de la teoría de conjuntos axiomática. Es cierto que nadie ha visto una demostración matemática no trivial totalmente formalizada en la teoría de conjuntos —y, como se ha señalado a menudo, nadie querría verla si existiera— pero a muchos les tranquiliza el pensar que esta traducción de las matemáticas a los conjuntos es posible "en principio". Otros, sin embargo, han puesto en duda que esta traducción sea realmente posible y, más aun, que el fundamento sólido que pretende proporcionar sea necesario para las matemáticas. Por otra parte, con independencia de los aspectos fundacionales, la teoría de conjuntos también se ha desarrollado como una disciplina matemática autónoma, con sus propios problemas. Quizá el ejemplo más importante sea la hipótesis del continuo, que fue formulada por Cantor y ya figuraba en la lista de los *Problemas de Hilbert* —como el primer problema— y que, a pesar de la demostración de su indecidibilidad en el marco de la teoría de conjuntos axiomática usual, sigue siendo considerada por muchos como un problema no resuelto, al cual se han dedicado grandes esfuerzos en años recientes. Puede ser pertinente señalar que, a pesar del carácter básico que se le supone al concepto de conjunto, en el estudio de este y de otros problemas conjuntistas importantes, se han desarrollado métodos muy sofisticados y se han obtenido resultados muy profundos, en contra de la idea que algunos matemáticos tienen —derivada quizá de la asociación con los problemas fundacionales y con la filosofía— de que la teoría de conjuntos carece de interés matemático. Por otra parte, la teoría de conjuntos tiene importantes aplicaciones a las matemáticas y, de la mano de la lógica, también a la informática, a la que presta una estructura de datos básica.

En estas notas se pasa revista a algunas de las cuestiones básicas sobre los conjuntos y, en concreto, a las que conciernen a su interacción con las matemáticas —y, en particular, con los fundamentos de las matemáticas— y con la informática. Están escritas desde el punto de vista de un matemático que no es especialista en teoría de conjuntos y que, a lo largo de su trabajo, solo ha tenido contactos ocasionales con los aspectos no triviales de dicha teoría, a través de los ordinales y cardinales infinitos y de la "combinatoria infinita". No pretenden ser exhaustivas y, debido a la elección bastante subjetiva de los temas tratados, tampoco serán muy sistemáticas. No obstante, están escritas con la esperanza de que puedan contribuir a arrojar luz sobre algunas de estas cuestiones básicas, aunque solo sea a través de las referencias que se incluyen en la bibliografía, en las cuales se discuten más detenidamente muchas de estas cuestiones. Entre ellas figuran: las distintas formas de concebir el concepto de conjunto, el papel de los conjuntos y de las sucesiones en matemáticas y en informática, la "sencillez" del concepto de conjunto, la hipótesis del continuo como problema abierto y los argumentos en favor y en contra de su verificación, la utilidad de los conjuntos para modelar los "fenómenos circulares" y, finalmente, la discusión sobre si las matemáticas son reducibles a la teoría de conjuntos. Hay muchos otros aspectos que serían dignos de consideración, pero creo que los mencionados son más que suficientes para dar una idea de las múltiples formas en que la teoría de conjuntos influye en otras disciplinas; en particular, no haré hincapié en el desarrollo histórico de la teoría, para el cual la referencia principal es [41].

LOS CONJUNTOS Y LOS FUNDAMENTOS DE LAS MATEMÁTICAS

La teoría de conjuntos ha sido ampliamente usada para desarrollar los fundamentos de las matemáticas. La idea subyacente a este hecho se puede condensar en las dos premisas siguientes:

1. *Los conjuntos son objetos matemáticos muy sencillos y fáciles de comprender.*
2. *Todas las matemáticas se pueden formular en términos de la teoría de conjuntos.*

La primera de estas afirmaciones puede parecer bastante evidente, debido al hecho de que los conjuntos tienen muy poca "estructura" pero, como indicaré más adelante, si se profundiza un poco más, se observa que los conjuntos pueden plantear problemas muy complicados y estar sujetos a diferentes interpretaciones. La segunda afirmación[1] también es muy discutible pues, aunque a primera vista parece claro que todas las matemáticas se pueden formular de manera natural en el lenguaje conjuntista —por ejemplo, en la teoría de conjuntos ZFC (Zermelo-Fraenkel, con el

[1] Una formulación explícita —debida a Y. Moschovakis— de esta idea es la siguiente: *"La teoría de conjuntos es el lenguaje oficial de las matemáticas, de la misma forma que las matemáticas son el lenguaje oficial de la ciencia"* [85]. La versión de K. Kunen es: *"La teoría de conjuntos es el fundamento de las matemáticas. Todos los conceptos matemáticos se definen en términos de las nociones primitivas de conjunto y pertenencia"* [66].

axioma de elección) [66]—, en la práctica los matemáticos no traducen todo a teoría de conjuntos sino que se contentan con suponer que, en principio, esta traducción es posible. De hecho, sólo una parte muy pequeña de las matemáticas ha sido traducida a la teoría de conjuntos axiomática y esto ya proporciona un indicio que arroja dudas sobre la viabilidad de dicha traducción.

En el resto de estas notas analizaré ambas cuestiones con mayor detalle pero antes mencionaré brevemente las interpretaciones más habituales del universo de la teoría de conjuntos.

El universo V descrito por la teoría ZFC se "construye" partiendo de las premisas siguientes.[2] Todos los elementos de los conjuntos han de ser a su vez conjuntos[3] y, dado que por el axioma de regularidad o fundación (*"todo conjunto no vacío x tiene un elemento $\in$-minimal, es decir, un $a \in x$ tal que $a \cap x = \emptyset$"*), no puede haber "cadenas descendentes infinitas de pertenencia",[4] se deduce que el último elemento de una $\in$-cadena descendente tiene que ser el conjunto vacío, de forma que todos los conjuntos se construyen "a partir de la nada". Por otra parte, dado que la hipótesis de que todas las colecciones de conjuntos de V son conjuntos de V, conduce a paradojas (como la de Russell que discutiré más adelante), las operaciones que se permiten para construir nuevos conjuntos de V son únicamente las proporcionadas por los axiomas de ZFC. De hecho, V se construye por recursión transfinita a partir del conjunto vacío aplicando solamente la operación de tomar el "conjunto de partes", aunque se puede demostrar que, además, V es cerrado para las otras operaciones conjuntistas definidas por los axiomas de ZFC. Recordemos que un *ordinal* es un conjunto transitivo (en el que la relación $\in$ es transitiva, es decir, todos sus elementos son subconjuntos), bien ordenado por $\in$. Cada ordinal es el conjunto de los ordinales anteriores y, por tanto, se tiene que los primeros ordinales son $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, ... Un ordinal límite es un ordinal que no es sucesor[5] de otro ordinal, y un cardinal es un ordinal κ tal que para ningún ordinal $\alpha < \kappa$ existe una biyección entre κ y α.[6] El primer ordinal infinito (orden-isomorfo al conjunto $\mathbb{N}$ de los números naturales, que se suele identificar con él), es también un cardinal y se denota usualmente por la letra ω. A partir de él se define la sucesión de los cardinales transfinitos $\omega_0 = \omega$, ω_1, ..., ω_α, ... Una notación alternativa frecuente consiste en usar *alefs*, de modo que los cardinales infinitos son $\aleph_0$, $\aleph_1$, etc. A menudo, se usa la "notación ω" cuando los consideramos como ordinales y la "notación $\aleph$" cuando los consideramos como cardinales (por ejemplo, $\omega_0 + \omega_0 \neq \omega_0$, pero $\aleph_0 + \aleph_0 = \aleph_0$). La definición del universo V, denotando On a la clase de los ordinales y $\mathcal{P}$ a la operación "conjunto de partes", es la siguiente:

[2] V se llama *universo de Von Neumann* y la idea de su construcción se atribuye a Zermelo y a Von Neumann.

[3] También es posible admitir la existencia de elementos atómicos —es frecuente usar, para referirse a ellos, el término alemán *Urelemente*—, cuya naturaleza no se especifica.

[4] Esta cuestión se discutirá con más detalle en una sección posterior, donde se introducirán los "hiperconjuntos", que no satisfacen el axioma de fundación.

[5] El sucesor del ordinal α es $\alpha + 1 = \alpha \cup \{\alpha\}$.

[6] Los cardinales son así representantes de las clases de equivalencia definidas por la existencia de una biyección y a cada conjunto X le corresponde un único cardinal $|X|$, que se llama la cardinalidad de X.

$V_0 = \emptyset,$
$V_{\alpha+1} = \mathcal{P}(V_\alpha),$
$V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, si α es un ordinal límite,
$V = \bigcup_{\alpha\in\mathrm{On}} V_\alpha.$

En el universo de conjuntos así construido,[7] los conjuntos sólo se obtienen después de "coleccionar" otros conjuntos y reunirlos para formar uno nuevo, pero existe un enfoque completamente diferente basado en introducir los conjuntos como "conjuntos abstractos", que se obtienen despojando a objetos matemáticos ya existentes de toda estructura. En el primer caso, el conjunto de los números reales se obtendría "de abajo arriba" comenzando por definir los números naturales en ZFC, los cuales forman un conjunto por el *axioma de infinitud.* A partir de los números naturales se construyen los enteros, a partir de estos los racionales y, finalmente, a partir de los racionales, se obtienen los reales usando *cortaduras de Dedekind* o *sucesiones de Cauchy.* Por el contrario, en el "enfoque abstracto", consideraríamos a los reales como un cuerpo ordenado completo e iríamos descartando la estructura, olvidándonos de que es completo, de que es ordenado y de que es un cuerpo para obtener, finalmente, el conjunto abstracto subyacente a los números reales.

Este enfoque de la teoría de conjuntos ha sido promovido por F. William Lawvere,[8] siendo su punto de partida una axiomatización de la categoría de conjuntos [70] que, además de permitir describir de forma elegante (por ejemplo, en términos de funtores adjuntos) muchas nociones conjuntistas básicas, tiene la ventaja de que sus axiomas se pueden debilitar dando lugar a *categorías de topos* que, aun pareciéndose bastante a la de conjuntos, tienen mucha mayor flexibilidad pues, por una parte, permiten usar lógicas diferentes de la clásica y, por otra, engloban categorías diferentes de la de conjuntos como, por ejemplo, las categorías de haces. Además de estas ventajas, se puede argumentar ([13]) que la noción de conjunto abstracto y el enfoque categórico están más próximos a la práctica matemática habitual que la "jerarquía acumulativa (o iterativa) de conjuntos" proporcionada por el universo V.

Por otra parte, todavía se puede dar un paso más en esta dirección y tratar de fundamentar las matemáticas directamente en la teoría de categorías. La idea inicial consiste, como es bien sabido, en poner énfasis en los morfismos entre estructuras y no en las propias estructuras. Además, en general los objetos de una categoría $\mathcal{C}$ no son conjuntos, aunque sí lo son los morfismos entre dos objetos X e Y, $\mathrm{Hom}_\mathcal{C}(X,Y)$. Este contexto introduce cambios en nuestra percepción de los objetos matemáticos. Por ejemplo, un objeto X de la categoría $\mathcal{C}$ se puede identificar, a través del *lema de Yoneda* con el funtor que representa: $Y \to \mathrm{Hom}_\mathcal{C}(Y,X)$. Como observa Manin [78], si C es *pequeña*, esto convierte al objeto X, que inicialmente no tenía estructura, en un

[7] En [80], Manin se refiere al universo de Von Neumann con estas palabras: *"Es difícil imaginar un objeto de contemplación más puro que esta discreta y poderosa jerarquía".*

[8] Lawvere describió los conjuntos abstractos, en [69], de la manera siguiente: *"Un conjunto abstracto X tiene elementos que no tienen estructura interna alguna. X no tiene estructura interna excepto en lo que se refiere a la igualdad de pares de elementos, y no tiene propiedades externas salvo su cardinalidad; aun así, un conjunto abstracto es más refinado (menos abstracto) que un número cardinal por el hecho de tener elementos, mientras que el número cardinal carece de ellos".*

conjunto estructurado y es *“una caracterización externa, ‘sociológica’, de un objeto matemático a través de su interacción con todos los objetos de la misma categoría y no de su estructura intrínseca”*. De esta manera, en lugar de estudiar directamente la categoría $\mathcal{C}$, se puede estudiar la categoría de funtores contravariantes de $\mathcal{C}$ en la categoría de conjuntos (o, en ocasiones, en una categoría con “más estructura” como, por ejemplo, una *categoría abeliana*), siendo cada uno de estos funtores una “representación” de $\mathcal{C}$. La categoría $\mathcal{C}$ se sumerge así en la categoría de funtores, en la cual aparecen nuevos objetos que no estaban presentes en la categoría original pero que proporcionan información adicional sobre la misma que, a menudo, resulta enormemente útil. Este enfoque fue utilizado con gran éxito por Grothendieck en geometría algebraica. Otra diferencia importante entre este enfoque y el puramente conjuntista es que, como también observa Manin, el hecho de que dos objetos matemáticos isomorfos tienen las mismas propiedades hace que no importe cuántos objetos isomorfos a uno dado estén contenidos en una categoría $\mathcal{C}$, lo que lleva al concepto de *categorías equivalentes* (cuando ambas tienen las mismas clases de objetos isomorfos y de morfismos entre sus representantes), que es mucho más importante que el de categorías isomorfas. Esto sugiere que las categorías son algo más que conjuntos con estructura, pues es natural identificarlas cuando existe entre ellas una equivalencia, que no tiene que ser necesariamente biyectiva en las clases de objetos. A partir de aquí surge una imagen jerárquica cuando se considera a las propias categorías como objetos de una categoría cuyos morfismos son los funtores que, a su vez, son los objetos de una categoría. Cuando esta construcción se axiomatiza surge el concepto de 2-categoría y la construcción se puede iterar para obtener las n-categorías. En este contexto, se produce el siguiente fenómeno que también observa Manin [78]: *“no hay igualdad de objetos matemáticos sino sólo equivalencias y, a su vez, dado que las equivalencias son objetos matemáticos, no hay igualdad entre ellas, sino equivalencias, etc”*. Manin señala que esta visión es mucho más adecuada para la descripción cuántica del mundo, en la que los conjuntos no son ya *conjuntos de cosas* en la tradición de Cantor sino más bien *conjuntos de posibilidades* pero, a pesar de todo, su conclusión es que este enfoque no es contrario a la visión conjuntista original de Cantor sino que lo que hace es enriquecerla.[9]

Conjuntos versus sucesiones

Si pensamos en los conjuntos desde la perspectiva de los “conjuntos abstractos”, cabe plantearse la posibilidad de que existan otros conceptos que, aun siendo más complejos desde el punto de vista estructural, puedan parecernos intuitivamente más idóneos para modelar ciertos fenómenos matemáticos. Por otra parte, el ámbito de aplicación de los conjuntos no se limita a las matemáticas sino que también están

[9] De hecho, en [80], Manin considera las ideas de Cantor como el origen de la teoría de categorías: *“La intuición de Cantor subyace en la mayor parte del trabajo fundacional en matemáticas del siglo XX: o es vigorosamente refutada por logicistas de varias cosechas o funciona como un gran proyecto de unificación, tanto en la forma de Teoría de Conjuntos como en la de su sucesor, la Teoría de Categorías”*.

siendo ampliamente usados en otras disciplinas relacionadas y, en particular, en informática, fundamentalmente en el campo de la verificación formal y también en el de las bases de datos, para cuyo manejo se utilizan *lenguajes de consulta* ("query languages") basados en la teoría de conjuntos. Sin embargo, en informática y en computación es mucho más frecuente que los lenguajes utilicen sucesiones o listas (sucesiones finitas) que conjuntos, y esto sugiere la posibilidad de que las sucesiones pueden ser un concepto más natural en este contexto. La mayoría de los lenguajes de programación no poseen un tipo de datos que corresponda a conjuntos (aunque algunos como, por ejemplo, *Python*, sí lo tienen). Si nos fijamos en dos de los más importantes sistemas de cálculo simbólico de tipo general que se utilizan en matemáticas y que contienen lenguajes de programación, a saber, *Maple* y *Mathematica*, vemos que el primero sí tiene un tipo de datos que corresponde a conjuntos ("set"), mientras que *Mathematica* (inspirado en *Lisp*) carece de él. En la práctica, al ser los lenguajes de programación secuenciales, los conjuntos se representan normalmente como sucesiones y habrá que especificar en ellos un orden antes de poder escribirlos a un fichero o mostrarlos en una pantalla. En *Maple*, los elementos de un conjunto son ordenados, en base a consideraciones de eficiencia, según la posición que ocupan en la memoria. Aunque esto puede incrementar un poco la velocidad del sistema, también tiene sus inconvenientes. Si el resultado de una computación es un conjunto y se nos muestra en la pantalla, puede que sea difícil reconocerlo aunque esté formado por números o caracteres alfabéticos, debido a que, probablemente, los elementos no aparecerán en el orden usual al que estamos acostumbrados. Por eso nosotros siempre solemos escribir los elementos de un conjunto de números en su orden natural, ya que de no hacerlo así puede ser muy difícil reconocer si dos de estos conjuntos son o no el mismo.

El uso de listas en lugar de conjuntos tiene claras ventajas computacionales, que son fáciles de ilustrar con ejemplos cotidianos. Una de ellas es que la búsqueda en una lista puede ser mucho más eficiente que la búsqueda en el conjunto correspondiente. Pensemos en el listín telefónico de una ciudad grande, en el cual podrían figurar varios millones de teléfonos. Cuando queremos averiguar el teléfono de una persona, aprovechamos el hecho de que los nombres están ordenados alfabéticamente para encontrar rápidamente el que estamos buscando. Para ello recorremos los caracteres del nombre y, en consecuencia, la búsqueda se realiza en tiempo polinómico en función de la longitud del mismo.[10] Si, por el contrario, queremos averiguar el nombre de la persona que tiene un teléfono determinado, habremos de ir buscando uno por uno y, por término medio, habría que recorrer individualmente la mitad de los teléfonos presentes en la guía hasta encontrar el buscado. Esto significa que el tiempo de búsqueda sería exponencial en función de la longitud de los números telefónicos.[11]

[10]Un algoritmo es de tiempo polinómico cuando su tiempo de ejecución crece, asintóticamente, como una función polinómica del tamaño del input. En el caso de una guía con n nombres, este tamaño será la longitud de n en un sistema de numeración —que podemos suponer el binario— y, en consecuencia, sería esencialmente $\log_2 n$. Si los nombres de la guía estuviesen en binario y careciesen de redundancia, el recorrer los símbolos del nombre buscado requeriría $\log_2 n$ operaciones. En general, el número de operaciones requerido será, aproximadamente, proporcional a $\log_2 n$.

[11]Este tiempo es exponencial como consecuencia de que n crece exponencialmente en función

Si se analiza el proceso de búsqueda del número telefónico de una persona, se observa que la eficiencia del mismo no reside meramente en la existencia de un orden sino más bien en el hecho de que el orden de la lista de nombres está generado por el orden —que nos resulta perfectamente conocido— de una lista mucho más pequeña, a saber, la sucesión de los caracteres alfabéticos. El paso del orden alfabético de los caracteres individuales al orden alfabético único de la lista de nombres es posible porque estos últimos también son listas de caracteres y esto hace que, para reconocer un nombre, baste con recorrer sus caracteres secuencialmente, lo que no ocurriría si el nombre fuese un conjunto de caracteres. Por tanto, en este proceso juegan un papel importante tres tipos de listas: la lista de nombres, la lista formada por el alfabeto con su orden habitual y las listas formadas por cada uno de los nombres. Por el contrario, cuando se busca el nombre del usuario que tiene un número de teléfono dado, también buscamos en una lista —la de los números de teléfono—, pero nos encontramos con la dificultad de que el orden de esta lista nos es desconocido y, al no tener relación con el orden natural de los dígitos, no podemos explotarlo para buscar recorriendo caracteres individualmente. A pesar de todo, incluso en este caso, el hecho de que los números telefónicos forman una lista facilita mucho la tarea, pues basta irlos recorriendo secuencialmente hasta encontrar el buscado. Además, al ser cada número telefónico una lista, podemos reconocerlo mucho más fácilmente que si fuera meramente un conjunto de dígitos.

Podemos imaginarnos lo que ocurriría si prescindimos de estas ventajas y consideramos una guía telefónica puramente conjuntista, que podría consistir en una relación entre el conjunto U de los usuarios y el conjunto T de los números telefónicos, es decir, sería simplemente un subconjunto del producto cartesiano $U \times T$ (que podemos suponer que es una aplicación biyectiva). Dicha guía podría estar físicamente representada en un gran panel bidimensional por una "nube de puntos" (como en la forma tradicional de presentar un conjunto y sus elementos mediante diagramas de Venn), cada uno de ellos etiquetado por el elemento correspondiente del conjunto $U \times T$ que nos proporciona el nombre de un usuario y su número de teléfono. De hecho, para que la guía fuese puramente conjuntista, cada uno de estos elementos debería de ser representado no en la forma habitual (u, t) que corresponde a un par ordenado, sino como un conjunto que podría ser $\{\{u\}, \{u, t\}\}$, en la modelación habitual debida a Kuratowski.[12] Esto haría que la búsqueda del usuario correspondiente a un teléfono dado fuese ahora aun más difícil que la correspondiente búsqueda exponencial en una guía ordinaria, puesto que tendríamos dificultades para ir recorriendo los números de teléfono al no estar estos dados en forma ordenada, aunque esto resultaría mucho más fácil si marcamos los números ya examinados, formando el subconjunto correspondiente.[13] Hay que tener en cuenta que incluso es-

de $\log_2 n$.

[12]Existen muchas otras formas posibles de representar conjuntistamente un par ordenado (u, t), por ejemplo, $\{\{u, t\}, \{t\}\}$ sería otra. Por otra parte, el conjunto $\{\{u\}, \{u, t\}\}$ puede ser presentado secuencialmente, en la notación habitual, de cuatro formas diferentes, correspondientes a las formas de ordenar el conjunto y sus elementos.

[13]Esta dificultad se acrecentaría todavía más si no sólo la guía sino todo el sistema fuese conjuntista. Si los nombres de los usuarios y los "números" (o nombres) de teléfono fuesen conjuntos y no listas, el número de caracteres necesario aumentaría mucho y, además, tendríamos que dedicar

ta representación bidimensional de los conjuntos implicados proporciona una cierta información adicional no contenida en el concepto de conjunto, pues podríamos usar nuestro sentido de la orientación para ir estableciendo un orden aproximado entre los elementos, recorriéndolos, por ejemplo, de izquierda a derecha y de arriba abajo. Para que la búsqueda fuese puramente conjuntista, este proceso habría que realizarlo a ciegas, es decir, no podría haber "izquierda" y "derecha" que nos permitieran situar y ordenar de alguna forma los elementos del conjunto. Podemos pensar en un conjunto de bolas con símbolos contenidas en una urna. Si queremos determinar si una bola dada está en la urna (es decir, si un elemento pertenece al conjunto) y si solamente podemos hacerlo extrayendo bolas y volviéndolas a introducir en la urna, de una en una, el proceso sería muy difícil incluso si podemos ir marcando las bolas ya examinadas pues, mientras la bola buscada no aparezca, nunca tendríamos la seguridad de haber completado la búsqueda.

La discusión anterior muestra las ventajas de las sucesiones sobre los conjuntos en algunos contextos, pero no resuelve la siguiente cuestión básica, que está relacionada con la premisa inicial sobre la sencillez del concepto de conjunto:

> *¿Qué objectos son más sencillos para nuestra percepción: los conjuntos, o las sucesiones o listas?*

El hecho de tener "menos estructura" sugiere que son los conjuntos, pero esto no está tan claro si tenemos en cuenta que muchos de los conjuntos que aparecen en matemáticas y en informática tienen una estructura adicional —en muchos casos son sucesiones o listas— y hay que hacer un esfuerzo de abstracción suplementario para verlos como conjuntos abstractos. De hecho, la discusión anterior de lo que sería un listín telefónico puramente conjuntista se puede interpretar como una abstracción de las guías telefónicas usuales construidas como listas. Pero también existen conjuntos que carecen de un orden natural como, por ejemplo, grafos y otros conjuntos geométricos, y sería muy difícil tratar de imaginarlos como sucesiones o listas. El lenguaje matemático usual, aunque no esté completamente formalizado, comparte con los lenguajes de programación la característica de ser esencialmente secuencial y unidimensional, y nos obliga a representar secuencialmente los elementos de los conjuntos que se mencionan explícitamente. Sin embargo, es habitual intercalar en dicho lenguaje fragmentos no lineales para facilitar la percepción de los hechos matemáticos. El ejemplo más evidente son las figuras geométricas que aparecen a menudo en demostraciones matemáticas informales,[14] aunque no formen parte de las deducciones formales. Otro ejemplo del uso de imágenes en el lenguaje lo proporcionan los diagramas conmutativos, que son muy útiles en álgebra. Un caso instructivo, citado en [76], lo proporciona el diagrama correspondiente al *lema de la serpiente*, un resultado básico de álgebra homológica que encierra brevemente un enunciado que en la escritura secuencial ordinaria es mucho más complicado. El diagrama de la serpiente

---

cierto tiempo a examinar cada teléfono y cada usuario hasta decidir si el conjunto correspondiente es o no el que estamos buscando (pues no sería fácil decidir si dos conjuntos, cuyos elementos están dados como "nubes de símbolos", son o no iguales).

[14] Véase [19] para una provocativa discusión del papel de las imágenes en las demostraciones.

es un grafo dirigido, que puede ser interpretado conjuntistamente[15] aunque no haya una forma natural de representarlo secuencialmente, y la forma gráfica tiene la ventaja de que nos permite reconocer fácilmente si el lema es aplicable en multitud de situaciones. Sin embargo, si quisiésemos trabajar con objetos geométricos o con diagramas utilizando un lenguaje informático estándar, forzosamente habríamos de representarlos en forma secuencial, con la consiguiente pérdida de naturalidad que eso conlleva, a diferencia de lo que ocurre en el lenguaje informal de las matemáticas.

A pesar de esto, es posible plantearse la posibilidad de que las matemáticas se pudieran “reducir” a sucesiones en el mismo sentido en que se supone que se pueden “reducir” a conjuntos. Esta cuestión se menciona en [13], y en [30] se proponen las sucesiones transfinitas como fundamento de las matemáticas.[16] Sin embargo, parece que la sencillez estructural de los conjuntos los hace más adecuados que las sucesiones como lenguaje básico de las matemáticas, aunque no parece que sea así en el caso de la informática, donde el uso de sucesiones es muy natural (y más aún cuando uno se acerca al nivel del hardware, que procesa los datos en forma secuencial). No obstante, la gran economía del lenguaje conjuntista y su gran versatilidad para proporcionar modelos también encuentra importantes aplicaciones en informática, donde hay conceptos que tradicionalmente han sido modelados como sucesiones pero que también son susceptibles de ser modelados como conjuntos. Un ejemplo —que puede servir como test para decidir entre conjuntos y sucesiones en una situación concreta— lo proporcionan los flujos (“streams”), que se pueden considerar como sucesiones infinitas de elementos de un alfabeto A. Por ejemplo, si $a, b \in A$, podemos definir un flujo, de manera informal, como a seguido de b, seguido de a, seguido de b, etc. Para definirlo de manera precisa, podríamos usar la función $f : \mathbb{N} \to A$ dada por

$$f(n) = \begin{cases} a & \text{si } n \text{ es par,} \\ b & \text{si } n \text{ es impar.} \end{cases}$$

Pero también podríamos tratar de imaginar el flujo de otra manera, usando pares ordenados. Si se quitan los dos primeros elementos se obtiene el mismo flujo y, por tanto, parece natural modelar el flujo en la forma $f = (a, (b, f))$.[17] En el fondo ambos modelos están expresados en términos conjuntistas, pero el segundo está mucho más próximo a nuestra intuición del concepto de conjunto que el primero, aunque ello no significa que sea necesariamente más intuitivo, pues también tenemos una percepción muy clara del concepto de sucesión (que no presupone la definición conjuntista de este concepto). Este ejemplo será de nuevo discutido, más adelante, en relación con los conjuntos que no satisfacen el axioma de fundación.

A pesar del importante papel de las sucesiones en informática, existen también, al menos desde el punto de vista teórico, ejemplos de lenguajes informáticos basados

[15] De hecho, la relación entre conjuntos y grafos es más estrecha de lo que podría parecer porque, como veremos más adelante, hay una metáfora muy sugestiva que permite considerar a los conjuntos como grafos.

[16] También en [30] se propone fundamentar las matemáticas en los *multiconjuntos*, que son similares a los conjuntos en que carecen de orden pero pueden tener “elementos repetidos”.

[17] En este caso existe autorreferencia (pues estamos definiendo f en términos del propio f) pero, como se verá más adelante, esta construcción es completamente legítima, aunque no puede ser realizada dentro de ZFC.

en conjuntos que ganan en expresividad con respecto a lenguajes similares basados en sucesiones. Un caso concreto se menciona en [13] y consiste en un lenguaje de consulta para bases de datos. Estos son lenguajes especializados que se utilizan para solicitar información (a través de una *consulta*) a una base de datos como, por ejemplo, el lenguaje SQL ("Structured Query Language"), que se puede considerar como una "variante sintáctica" de la lógica de primer orden.

Hay un tipo especial de consultas, llamadas *consultas invariantes* en las cuales los inputs son estructuras finitas, por ejemplo, grafos, en lugar de cadenas de caracteres. Las consultas invariantes se restringen a propiedades que dependen sólo del tipo de isomorfismo de la estructura-input. Por ejemplo, consideremos un *grafo bipartido*, es decir, un grafo cuyos vértices se pueden descomponer en la unión de dos conjuntos disjuntos V_1, V_2, con la propiedad de que en cada uno de estos conjuntos no hay dos vértices adyacentes (conectados por una arista del grafo). Entonces, un *emparejamiento* (matching) del grafo se define como un conjunto de aristas que no tienen ningún vértice en común, y el emparejamiento se dice perfecto si todo vértice es incidente con una arista del emparejamiento. El problema del emparejamiento bipartido (también llamado el *problema del matrimonio*) consiste en encontrar un emparejamiento perfecto en un grafo bipartido tal que $|V_1| = |V_2|$. El problema de decidir si un grafo bipartido dado tiene un emparejamiento perfecto es una consulta invariante, pues el resultado, como en una consulta a una base de datos, no debe depender de la forma en que los datos están almacenados. En los modelos usuales de computación, como el proporcionado por las máquinas Turing, el problema es resoluble en tiempo polinómico, como consecuencia de que las estructuras están codificadas secuencialmente. Una vez que el grafo está presentado dando, por ejemplo, la matriz de incidencia, existen algoritmos de tiempo polinómico (el primero de ellos debido a Edmonds (1965)) para encontrar un emparejamiento perfecto en caso de que exista, partiendo de un emparejamiento parcial (por ejemplo, el emparejamiento vacío) y aumentándolo iterativamente. Pero la situación cambia si la estructura (el grafo, en nuestro ejemplo) no tiene un orden especificado, pues no se conoce un modo de codificar eficientemente como cadenas las clases de isomorfismos de estructuras.

Esto está relacionado con el problema de determinar si existe una lógica para capturar la clase de complejidad P (los problemas resolubles en tiempo polinómico) en el sentido de que la clase de problemas definibles en dicha lógica coincida con P (véase [35] para una formulación más precisa).[18] La dificultad principal de este cuestión reside, como en el ejemplo anterior, en tener que resolver un problema (o responder a una consulta) sobre una estructura, en tiempo polinómico, cuando no hay especificado un orden lineal en dicha estructura. Una dirección de ataque

[18]Este es un problema fundamental de la *teoría de la complejidad descriptiva* [56], que trata de caracterizar las clases de complejidad mediante el tipo de lógica necesario para expresar los problemas de dichas clases. El punto de partida de esta teoría fue un resultado de R. Fagin (1974) que dice que la clase NP (de tiempo polinómico no determinista) corresponde a la *lógica existencial de segundo orden*, mostrando así, por primera vez, cómo caracterizar la complejidad sin hacer referencia a conceptos como tiempo o espacio. La dificultad del problema en lo referente a la clase P viene avalada por el hecho de que la forma natural de obtener una solución positiva implicaría que el *problema del isomorphismo de grafos* estaría en P, mientras que una solución negativa implicaría que P $\neq$ NP.

consiste en tratar de encontrar un procedimiento de tiempo polinómico que asigna uno de sus órdenes a cada estructura (el número de órdenes posibles puede ser exponencial en función del tamaño de la misma). Otra posibilidad es desarrollar modelos de computación o, en los términos expresados antes, lenguajes de consulta (el concepto de "lógica" que se maneja en este contexto es amplio e incluye los modelos de computación y los lenguajes de consulta) que traten directamente con las estructuras, sin usar una codificación secuencial de las mismas. En [14], se utiliza este último enfoque y para ello se formula un lenguaje de consulta, llamado BGS, que es puro, en el sentido de que no proporcione medios para expresar una propiedad del input que no es preservada por isomorfismos. Este lenguaje está basado en la teoría de conjuntos y no permite elecciones arbitrarias (no permite elegir un orden) pero utiliza paralelismo. Un algoritmo de este lenguaje no es capaz de resolver un problema como el del emparejamiento bipartido en tiempo polinómico [14], pues no puede trabajar con una codificación secuencial del grafo. En consecuencia, la lógica asociada a BGS no resuelve el problema de capturar la clase P, sin embargo, se demuestra en [15] que una versión de BGS limitada a tiempo polinómico (Ptime BGS) es más expresiva —pues captura más problemas de tiempo polinómico— que un lenguaje de consulta similar que trabaja con sucesiones en lugar de conjuntos. Por tanto, en este contexto, los conjuntos son preferibles a las listas y la razón es la dificultad de simular conjuntos (no ordenados) mediante listas (ordenadas) sin introducir mucha duplicación.

En conclusión, parece difícil decidir globalmente entre conjuntos o sucesiones pues la utilidad de unos o de otros puede depender fuertemente del contexto. En cuanto a la pregunta en [13] sobre la posibilidad de tomar los conjuntos como tipo de datos básico en informática, aun no descartando esta posibilidad, no parece que fuera a tener ventajas prácticas en la mayoría de las situaciones. Una vía que es, en cierto modo, intermedia entre los conjuntos y las sucesiones, la proporcionan los multiconjuntos que ya están siendo extensamente utilizados en diversas áreas de la informática.

¿Son los conjuntos realmente tan sencillos?

Analicemos con mayor detalle la premisa inicial de que los conjuntos son muy sencillos y fáciles de comprender. A primera vista, la última parte de esta afirmación parece deducirse de la sencillez estructural de los conjuntos, pero si se profundiza un poco más, pronto se encuentran dificultades serias que arrojan dudas sobre la claridad de nuestra comprensión del concepto. Para someterla a prueba no es necesario recurrir a construcciones exóticas y nos mantendremos en el ámbito del conjunto de los números naturales ω (o $\mathbb{N}$ en la notación matemática tradicional) y de sus subconjuntos. En este contexto, son naturales —nunca mejor dicho— las siguientes cuestiones básicas:

¿Qué es un conjunto de números naturales?

¿Cuántos conjuntos de números naturales hay?

La respuesta a la segunda pregunta depende de la respuesta a la primera y parece mucho más difícil de obtener. No obstante, la respuesta a la primera tampoco es tan obvia como puede parecer a primera vista. Como observa Timothy Gowers en [53], parece natural pensar que un conjunto de números naturales es un subconjunto de $\mathbb{N}$ obtenido aplicando alguna "regla" para seleccionar los elementos que lo forman. Pero es fácil ver que el número de reglas (usando cadenas finitas de un número finito de símbolos para expresarlas) es numerable y, en cambio, el número de subconjuntos de $\mathbb{N}$ no lo es (en virtud del famoso "argumento diagonal" de Cantor). Por tanto, existen *conjuntos indefinibles* de números naturales y, de hecho, se puede decir que "casi todos" los conjuntos de números naturales son indefinibles. En particular, como indica Gowers, esto significa que no podemos comprender el significado general de la palabra "conjunto" mediante la observación de ejemplos concretos; para describir todos los conjuntos mediante "reglas" necesitaríamos admitir que estas pueden no ser expresables en tiempo finito (para una discusión más precisa de este fenómeno en el contexto de los lenguajes formalizados, véase [76, Proposition 2.12, Corollary 2.13]).

Pero las dificultades planteadas por la primera cuestión no terminan aquí pues, aun considerando conjuntos definibles, diferentes matemáticos o lógicos podrían dar respuestas muy distintas sobre su existencia. Por ejemplo, podemos preguntarnos por la existencia del conjunto de los números naturales menores que $10^{10^{10}}$. Antes de nada, es preciso señalar que la palabra "existencia" puede tener, en matemáticas, muchos significados distintos. La mayoría de los matemáticos son *realistas* (o *platónicos*), es decir, creen que los conjuntos —y los objetos matemáticos en general— tienen una existencia objetiva que es independiente de nuestro conocimiento de los mismos y que cualquier pregunta significativa sobre ellos tiene que ser verdadera o falsa.[19] Según esta idea, los objetos matemáticos son descubiertos por nosotros pero no creados ni inventados y no hay duda de que para un realista el conjunto antes mencionado tiene existencia propia. Opuesto al realismo, en lo que a la existencia de objetos matemáticos se refiere, es el *formalismo*, homologable al nominalismo filosófico: *"los términos abstractos no son nombres de objetos abstractos"*. En su versión más extrema (y más simple), el formalismo postula que los objetos matemáticos no existen y que las matemáticas se reducen al estudio de los sistemas formales.[20] En consecuencia, no cabe hablar propiamente de "la teoría de conjuntos", sino más bien de diversas teorías axiomáticas de conjuntos: ZFC, NBG (Von Neumann-Bernays-Gödel), MK (Morse-Kelley), etc. Para un formalista, el conjunto anterior no plantea dificultad alguna pues, aunque no existe en sentido estricto ("realmente"), su "existencia" puede ser demostrada fácilmente en la teoría ZFC a partir de los axiomas. Sin embargo, la respuesta de David Van Dantzig (matemático holandés fallecido en 1959) habría sido probablemente negativa, pues en una ocasión se preguntó si $10^{10^{10}}$ es un número finito [26]. Este es un ejemplo de lo que se suele llamar *ultraintuicionismo* o *ultrafinitismo*, una versión radical del intuicionismo. El intuicionismo se originó con Brouwer y postula que las matemáticas han de ser desarrolladas por

[19] También es frecuente distinguir entre *realismo* (la matemática es *objetiva*) y la versión más radical llamada *platonismo* (los objetos matemáticos existen realmente).

[20] Tanto el realismo como el formalismo tienen variantes mucho más complejas y sutiles que las versiones básicas aquí descritas que son, sin embargo, suficientes para la discusión que nos ocupa.

métodos constructivos a partir de la "intuición primordial" de los números enteros y de contar; siendo así una variante de lo que, más generalmente, se conoce como constructivismo. Otro finitista radical —o, quizá mejor, un matemático cuyo punto de vista es una mezcla de formalismo y finitismo radical— es Edward Nelson quien, después de haber hecho un trabajo muy importante en física matemática, dedicó sus esfuerzos a cuestiones de fundamentos. En su libro [88], Nelson admite sin problemas el número $2^{2^{2^2}} = 65536$ pero no $2^{2^{2^{2^2}}} = 2^{65536}$, que sería sólo un "número formal", pero no un "número genético" pues, como argumenta en [88, p. 75], si uno cuenta a razón de uno cada 10^{-24} segundos, que es el tiempo aproximado que tarda la luz en atravesar el diámetro de un protón, y si la edad del universo es de 20 mil millones de años, entonces tardará más de 10^{19684} edades del universo antes de contar hasta 2^{65536}. Así llega a la conclusión [88, p. 97] de que el nivel V_5 del universo V, con sus 65536 objetos, existe, pero V_6, con sus 2^{65536} objetos, es sólo una construcción formal.[21]

Es posible también considerar conjuntos mucho más pequeños que los que se acaban de mencionar sobre cuya existencia tampoco habría unanimidad. Recordemos que la *conjetura de Goldbach* afirma que todo entero par ≥ 4 se puede escribir como la suma de dos primos. Aunque existe la creencia (desde un punto de vista realista) de que la conjetura de Goldbach es cierta (basándose en argumentos heurísticos y resultados experimentales), por el momento no ha sido demostrada; para el argumento que sigue, cualquier otro problema matemático no resuelto (como, por ejemplo, la *Hipótesis de Riemann*) serviría también. Supongamos que definimos un conjunto X postulando que $X = \{0\}$ si la conjetura de Goldbach es cierta y que $X = \{1\}$ en caso de que sea falsa y, a continuación, afirmamos que el conjunto X así definido verifica que $|X| = 1$. Desde el punto de vista clásico, es decir, desde una visión realista de las matemáticas, es indudable que el resultado es cierto ya que X tiene un único elemento, aunque no sepamos si dicho elemento es 0 o es 1. Pero desde el punto de vista constructivista no es así, pues el conjunto X no existe, dado que no lo hemos definido por un procedimiento constructivo. De hecho, uno de los puntos de partida históricos del constructivismo y, más concretamente, del intuicionismo tal como lo formuló Brouwer, fue el rechazo explícito del *principio del tercio excluso* que postula que cualquier enunciado matemático significativo es verdadero o falso. Brouwer admitía la validez de dicho principio sobre conjuntos finitos pues, en tal caso, la verificación de una propiedad se podría ir comprobando para cada uno de sus elementos, pero pensaba que su generalización a un conjunto infinito no estaba justificada. Por eso, Brouwer no admitiría la existencia del conjunto X antes definido hasta que pudiésemos dar una demostración (¡constructiva!) o un contraejemplo de la conjetura de Goldbach, en cuyo caso ya tendríamos una construcción de X. Sin embargo, la mayoría de los constructivistas sí admitirían que el conjunto Y, definido como $Y = \{0\}$ si todo entero par menor que $10^{10^{10}}$ es suma de dos primos e $Y = \{1\}$

[21]La *aritmética predicativa* que Nelson desarrolló en su libro citado se puede enmarcar en el contexto de lo que se conoce como *aritmética acotada*, que se originó con el artículo [92] y engloba diferentes teorías cuya característica común es que están axiomatizadas por un conjunto de fórmulas acotadas. La aritmética acotada está relacionada con el estudio de la complejidad computacional y su desarrollo no presupone la adopción de una postura filosófica radical como la de Nelson.

si no es así, es un conjunto bien definido. Pero otros, entre los que, probablemente, se encontraría Nelson, tampoco admitirían la existencia del conjunto Y.

Por supuesto que aún puede haber muchas posiciones intermedias entre la aceptación platónica de la existencia de todos los conjuntos del universo V y la posición de Nelson rechazando la existencia de V_6.[22] Por ejemplo, un realista moderado podría admitir sin ningún problema la existencia del conjunto $\mathbb{N}$ y de todos los subconjuntos de $\mathbb{N}$ que son definibles mediante una propiedad (expresable mediante una fórmula del lenguaje de primer orden).[23] De esta forma, consideraría que el conjunto de los números pares o el conjunto de los números primos existen realmente y para él no habría duda alguna de que la conjetura de Goldbach tiene que ser verdadera o falsa. Sin embargo, esta misma persona podría no creer en la existencia real de los subconjuntos no definibles de $\mathbb{N}$.

Los comentarios anteriores solamente pretenden mostrar que el concepto de conjunto —y, más aun, de "conjunto de números naturales"— quizá no sea tan sencillo y fácil de comprender como puede parecer a primera vista, pero los ejemplos mostrados no deben inducir a pensar que las ideas constructivistas son mayoritarias en matemáticas, pues dista mucho de ser así. Por ejemplo, en la introducción de [84], J.D. Monk estima que el universo matemático está poblado por un 65 % de platónicos, un 30 % de formalistas y un 5 % de constructivistas.[24] Aunque puede que esta estimación no sea muy rigurosa porque, además de estas alternativas (con sus numerosas variantes y subdivisiones), en la actualidad existen muchas otras filosofías de las matemáticas. Una de ellas es el *cuasi-empirismo* [27, 107], cuyos orígenes se remontan a Putnam [94] y Lakatos [67], y considera que las matemáticas son falibles y usan métodos cuasi-empíricos (o incluso empíricos, cf. [37]) que las aproximan a las ciencias experimentales. Otra alternativa es el *ficcionalismo*, según el cual los objetos matemáticos son ficticios [5]. También es relevante el *naturalismo* [73] que, más que una filosofía de las matemáticas, es un método para evaluar la metodología matemática y su relación con la filosofía, que fue definido por Quine como "*el reconocimiento de que es dentro de la propia ciencia y no en alguna filosofía previa, donde la realidad tiene que ser identificada y descrita".* Las cuestiones filosóficas sobre la realidad o la objetividad de los objetos matemáticos, etc., son, desde este punto de vista, externas a las matemáticas y, en consecuencia, totalmente irrelevantes en lo que concierne a la evaluación de su metodología. Por esta razón, el naturalismo es compatible con "versiones moderadas" (o "sutiles", en la terminología de Maddy [74]) del platonismo, el formalismo y el ~~ficcionalismo.~~ En palabras de Maddy [72]:

[22]Un ejemplo lo proporciona la siguiente declaración de S. Feferman en [39]: *"En el lado negativo, soy un anti-platónico confirmado. En el lado positivo, soy un realista en lo que a los números naturales se refiere, es decir, creo que los enunciados sobre la estructura de los números naturales tienen un valor de verdad determinado, independiente de las demostraciones y construcciones humanas".*

[23]Esta idea de considerar solamente subconjuntos definibles se aplica para el paso de un nivel al siguiente en la definición del *universo constructible* de Gödel, al que me referiré más adelante. Sin embargo, "constructible" no tiene un sentido finitario en este caso, pues la construcción se realiza por recursión transfinita sobre todos los ordinales.

[24]Yuri Gurevich menciona en [54] que el constructivismo le recuerda al perrito Moska, que en la fábula de Ivan Krylov "El elefante y Moska", ladra furiosamente a un elefante, el cual, a pesar de ello, lo ignora totalmente. Sin embargo, esto hace que Moska se sienta fuerte. . .

"la tarea del filósofo de las matemáticas es describir y explicar las matemáticas, no reformarlas".

Abordemos ahora la cuestión de cuántos conjuntos de números naturales hay o, en otras palabras, cuál es la cardinalidad de $\mathcal{P}(\omega)$.[25] Cantor demostró que este conjunto no es numerable pero, si trabajamos en ZFC, vemos que si dicha teoría es consistente (lo que es sólo un artículo de fe), entonces tiene un modelo numerable M (por el teorema de Löwenheim-Skolem, [76, p. 65]). En dicho modelo (que se puede incluso suponer que es transitivo por un resultado de Mostowski), existe el conjunto infinito ω (por el axioma de infinitud), y también el conjunto $\mathcal{P}(\omega)$, por el axioma de partes. Por otra parte, por el teorema de Cantor —que es consecuencia de los axiomas de ZF— se tiene que $\mathcal{P}(\omega)$ es no numerable. Por tanto, el modelo transitivo numerable M ¡contiene conjuntos no numerables! (paradoja de Skolem). Desde el punto de vista externo, al ser M numerable, todos los conjuntos de M también lo son, pero la paradoja de Skolem se resuelve interpretando que si X es un conjunto infinito de M, y consideramos una enumeración del conjunto numerable $\mathcal{P}(X)$, dicha enumeración (su grafo) no puede estar dentro de M. Skolem y otros especialistas en fundamentos aceptaban trabajar con conjuntos numerables infinitos pero no con infinitos no numerables, puesto que consideraban esta paradoja como una manifestación del carácter relativo de los conceptos conjuntistas. En particular, creían que existen "diferentes continuos", $\mathcal{P}(\omega)_M$, correspondientes a los diferentes modelos M, ninguno de los cuales coincide con el "verdadero" $\mathcal{P}(\omega)$ [76, p. 69].[26]

Desde el punto de vista realista, tanto la paradoja de Skolem como el hecho de que casi todos los subconjuntos de $\mathbb{N}$ sean indefinibles significan simplemente que los lenguajes formales tienen limitaciones a la hora de imitar los razonamientos intuitivos [76, p. 69]. Desde este punto de vista es perfectamente legítimo hablar de "la teoría de conjuntos", aunque no cabe identificarla con un sistema formal, p. ej. ZFC, puesto que este no la describe totalmente. Veamos, no obstante, hasta qué punto los sistemas formales son capaces de dar respuesta satisfactoria a la segunda pregunta sobre el número de conjuntos de números naturales. El primer intento de responder a esta pregunta fue obra del propio Cantor. Después de demostrar que la cardinalidad del continuo, $2^{\aleph_0}$, es mayor que $\aleph_0$ (y, por lo tanto, mayor o igual que $\aleph_1$), Cantor se preguntó dónde está situado $2^{\aleph_0}$ en la sucesión de los cardinales transfinitos y conjeturó que $2^{\aleph_0} = \aleph_1$, lo que se conoce con el nombre de *hipótesis del continuo* (abreviadamente CH).[27] Cantor dedicó grandes esfuerzos a tratar de demostrarla sin conseguirlo, lo cual no es nada extraño si se tiene en cuenta que, andando el tiempo, Gödel demostraría, en 1940, la consistencia de CH con ZFC [49]

[25] Dado que $\mathcal{P}(\omega)$ está en correspondencia biunívoca con el conjunto $\mathbb{R}$ de los números reales, esta pregunta equivale a: ¿Cuántos números reales hay?

[26] En un sentido diferente y desde un punto de vista ultrafinitista, Alexander Esenin-Volpin, hijo del gran poeta ruso Sergei Esenin, llegó mucho más lejos, al poner en duda la unicidad de la sucesión de los números naturales. Yu. Gurevich cuenta en [54] que una vez le instó a comparar *"la sucesión potencialmente infinita de los segundos a partir de un instante dado y la sucesión potencialmente infinita de las guerras mundiales".*

[27] Dado que existe una biyección natural —que hace corresponder a cada conjunto su función característica— entre $\mathcal{P}(X)$ y el conjunto 2^X de las aplicaciones de X al conjunto $2 = \{0, 1\}$, si $|X| = \aleph$, se denota $2^{\aleph}$ el cardinal de $\mathcal{P}(X)$, de modo que $2^{\aleph_0}$ es el cardinal del continuo $\mathcal{P}(\omega)$.

y, más tarde, Cohen demostraría, en 1963, la independencia de CH de ZFC [22], lo que se puede resumir diciendo que CH es indecidible en ZFC. Por tanto, ZFC (y también otros sistemas formales como NBG) es incapaz de responder a la pregunta básica sobre el número de conjuntos de números naturales. Sin embargo, el significado de este hecho está sujeto a interpretación y la de un realista es muy diferente de la de un formalista (para un finitista CH ni siquiera tiene sentido). La interpretación realista la formuló claramente Gödel en [51], una vez que ya había demostrado la consistencia de CH con ZF y ya se suponía que también resultaría ser independiente:

> *... se deduce que los conceptos y teoremas conjuntistas describen una realidad bien determinada en la cual la conjetura de Cantor tiene que ser verdadera o falsa. Por tanto, su posible indecibilidad de los axiomas sólo puede significar que estos axiomas no contienen una descripción completa de esta realidad.*

En cambio, desde el punto de vista formalista, CH no es una proposición de "la teoría de conjuntos" sino de un sistema formal como ZFC o NBG y lo que hicieron Gödel y Cohen al probar que CH es indecidible fue simplemente demostrar una propiedad de algunos de esos sistemas. Esta era, aunque un poco a regañadientes, la posición de Cohen sobre CH en 1971 [76, p. 172]. Así, desde el punto de vista formalista estricto, tan lícito sería trabajar en el sistema ZFC + CH como en ZFC + $(2^{\aleph_0} = \aleph_2)$, ZFC + $(2^{\aleph_0} = \aleph_{17})$ o, incluso, ZFC + $(2^{\aleph_0} = \aleph_{\omega+17})$, pues por el trabajo de Gödel y Cohen sabemos que todas estas teorías tienen modelos en caso de tenerlos ZFC (en cambio, ZFC + $(2^{\aleph_0} = \aleph_\omega)$ es inconsistente, véase, por ejemplo, [66, Lemma I.10.38, Corollary I.10.41]). Otra cosa es el interés que podrían tener estas teorías y cuál podría ser la razón de preferir una a otra, algo que no resulta fácil de dilucidar desde un punto de vista estrictamente formalista.[28]

En conclusión, hay que reconocer que no disponemos de una respuesta completamente satisfactoria a las preguntas del principio pero, en el caso de CH, los matemáticos no se resignan y siguen buscando esa respuesta. En el apartado siguiente se analizará con más detalle cuál es el sentido de esta búsqueda una vez que ya sabemos que CH es indecidible en los sistemas formales habituales.

La hipótesis del continuo

Desde una óptica realista, el problema de la hipótesis del continuo no puede considerarse cerrado por los resultados de Gödel y Cohen y aun sin necesidad de enmarcarse en esta postura filosófica, la mayoría de los especialistas en teoría de conjuntos consideran que CH —y, más en general, la hipótesis del continuo generalizada, GCH, según la cual $2^{\aleph_\alpha} = \aleph_{\alpha+1}$— es una cuestión significativa e importante,

[28] Nelson describió en [89] la tarea del matemático con las siguientes palabras: *"Los símbolos en la fórmula son marcas en el papel, y el trabajo del matemático es idear profundas y hermosas concatenaciones de esas marcas siguiendo reglas estrictas"*. Pero no está del todo claro cuáles serían los criterios de belleza y profundidad en este contexto.

que debe ser resuelta.[29] Un camino natural para tratar de hallar una solución consiste en añadir algún axioma a ZFC que permita hacerlo (como ya propuso Gödel). Sin embargo, no es, ni mucho menos, evidente, cuáles serían los "buenos axiomas" que podrían ser añadidos (obviamente, el problema se resolvería agregando a ZFC bien CH o bien su negación, pero esta solución no se considera satisfactoria).

Una postura discrepante con la idea que acabo de exponer es la manifestada por el lógico Solomon Feferman en [38] donde, después de analizar el hecho de que, a pesar de la gran cantidad de axiomas nuevos que se han considerado en teoría de conjuntos, incluyendo los llamados *axiomas de cardinales grandes*, la hipótesis del continuo permanece sin decidir, concluye que esto arroja serias dudas sobre si CH es un problema bien definido y, más aun, sobre si el continuo es un ente matemático bien definido. Este hecho no ofrece dudas desde una perspectiva platónica, pero Feferman rechaza este punto de vista y concluye: *"Estoy convencido de que la Hipótesis del Continuo es un problema inherentemente vago que* ningún *axioma nuevo resolverá de forma convincentemente definida."* (cf. [38] para los detalles y también [40], donde se añaden más explicaciones sobre esta posición y se discuten algunas opiniones contrarias).[30]

Para los especialistas que creen que CH es un problema significativo, la cuestión crucial es determinar cuáles pueden ser los axiomas a agregar a ZFC para decidirla. Los criterios manejados habitualmente son que los axiomas a añadir tengan un buen contenido intuitivo y, dado que es posible decidir la cuestión en uno u otro sentido, que conduzcan pragmáticamente a la solución más deseable. Hay un interesante artículo de Penelope Maddy en el que se discute esta cuestión, [72], analizando algunos de los más importantes argumentos que se han dado, tanto en favor como en contra de CH, así como los axiomas que podrían ser relevantes para el problema.

Comenzando por los argumentos a favor, uno de ellos podría ser el hecho de que CH se verifica en el *universo constructible* L, que fue utilizado por Gödel para probar la consistencia del axioma de elección y de la hipótesis del continuo. L se puede caracterizar como el menor modelo transitivo de ZF que contiene a todos los ordinales (el menor *modelo interno*) pero, más explícitamente, se puede definir como una subclase de V que se obtiene de forma similar por recursión transfinita a partir de $L_0 = \emptyset$, con la única diferencia de que, mientras que el paso de V_α a $V_{\alpha+1}$ se hace mediante la aplicación no restrictiva del axioma de partes, $L_{\alpha+1}$ está formado únicamente por los subconjuntos de L_α que son definibles a partir de un número finito de elementos de L_α por una fórmula del lenguaje de la teoría de conjuntos

[29] Manin distingue en [80] entre un *problema* (que es, básicamente, una cuestión sí/no) y un *programa de investigación* (*"un esbozo de una visión amplia, un mapa de un paisaje. . . "*) y señala que CH, que en la época de Cantor y Hilbert parecía una cuestión sí/no acabó generando un vasto programa de investigación que llevó a la prueba de su indecidibilidad. Para muchos especialistas, este programa de investigación aún no ha sido completado.

[30] Como test adicional sobre la cuestión, Feferman menciona en [40] que, pese a ser CH uno de los pocos "problemas de Hilbert" que siguen abiertos, no ha sido incluido entre los *Problemas del Milenio*, por la solución de cada uno de los cuales el Instituto Clay ofrece un millón de dólares. El test que propone está contenido en la siguiente pregunta: *¿Se sentiría usted legitimado para dirigirse al comité científico de ese Instituto y argumentar que el problema del continuo ha sido descartado injustificadamente, y que su solución también debería valer un millón limpio?*

relativizada a L_α. Así, mientras $|V_{\omega+1}| = 2^{\aleph_0}$, se tiene que $|L_{\omega+1}| = \aleph_0$ y, de hecho, los saltos de cardinalidad en los niveles L_α sólo se producen cuando α es un cardinal, puesto que $|L_\alpha| = |\alpha|$ para todos los ordinales infinitos α [76, p. 150]. L se llama el *universo constructible* y el *axioma de constructibilidad* $V = L$ postula que todos los conjuntos del universo son constructibles, de modo que L es un modelo de la teoría ZF + $(V = L)$. Gödel demostró que el axioma de elección y la hipótesis del continuo generalizada son teoremas de esta teoría, lo que prueba la consistencia de ambas con ZF (por ejemplo, CH se deduce del hecho de que los subconjuntos constructibles de ω se construyen todos en algún nivel numerable, de modo que $\mathcal{P}(\omega) \subset L_{\aleph_1}$, cf. [76, p. 161] o [66, p. 175]). Sin embargo, pocos especialistas consideran esta solución satisfactoria, porque creen que el axioma de constructibilidad es *demasiado restrictivo* y que L no agota V (y el propio Gödel así lo creía también).[31]

Otro argumento que ha sido usado en favor de CH es la existencia de resultados parciales en *teoría de conjuntos descriptiva*. Una formulación alternativa de CH es que no existen cardinalidades intermedias entre la de los conjuntos numerables y la del continuo, es decir, que todo subconjunto no numerable de $\mathbb{R}$ tiene la potencia del continuo. Más generalmente, dada una familia de subconjuntos de $\mathbb{R}$, se dice que satisface CH cuando todo conjunto no numerable de dicha familia tiene la potencia del continuo. Por ejemplo, los subconjuntos cerrados de $\mathbb{R}$ (por el teorema de Cantor-Bendixson) y, más generalmente, los conjuntos analíticos —y, en particular, los conjuntos de Borel— satisfacen CH en este sentido [85]. Sin embargo, los métodos usados para demostrarlo no tienen generalización satisfactoria y hoy en día no se considera que este argumento sea relevante. Otros argumentos favorables son la efectividad de GCH, que permite resolver de manera inmediata casi todas las cuestiones relativas a la aritmética de cardinales y también el hecho de que $\neg$GCH es restrictiva en cierto sentido surgido de la teoría del *"forcing"*,[32] que tampoco explicaré. Sin embargo, se han formulado muchos más argumentos en contra de la validez de CH y la mayoría de los expertos se inclinan en este sentido.

Entre los argumentos en contra se pueden mencionar algunas consecuencias contra-intuitivas de CH que ya fueron observadas por Gödel y también la verificación de CH en el universo constructible, que algunos interpretan negativamente dado el carácter restrictivo de dicho universo. Otro argumento en contra es la intuición de que el axioma de partes es más fuerte que el de reemplazo, una postura que fue defendida por Cohen a pesar de su formalismo [22]:

[31] La teoría de conjuntos se simplificaría muchísimo si se trabajase en el contexto de ZF + $(V = L)$ pues no sólo AC y GCH serían teoremas sino que, por resultados de Jensen [61], el universo constructible tiene una "estructura fina" que hace que casi todas las cuestiones sobre L sean decidibles. Esto es, precisamente, lo que hace el axioma de constructibilidad poco atractivo pues, en palabras de H.M. Friedman [40]: *"El especialista en conjuntos busca fenómenos conjuntistas profundos, y así $V = L$ es anatema puesto que restringe el universo conjuntista tan drásticamente que todo tipo de fenómenos está demostrablemente ausente"*. Por otra parte, dado que $V = L$ implica GCH y $\neg$GCH es consistente con ZFC, se deduce que $\neg(V = L)$ es consistente con ZFC.

[32] El "forcing" fue el método empleado por Cohen en su demostración de la independencia de CH. La idea básica de este método consiste en extender modelos de forma controlada, lo que permite que las sentencias verdaderas en el modelo extendido sean precisamente las que son "forzadas" a serlo.

El conjunto C (el continuo) es mayor que $\aleph_n$, $\aleph_\omega$, $\aleph_\alpha$, donde $\alpha = \aleph_\omega$, etc., pues está dado por un atrevido nuevo axioma (el de partes) que no puede ser aproximado por ningún proceso de construcción por pasos (el axioma de reemplazo).

Un argumento curioso contra GCH es el proporcionado por lo que Maddy llama la "identidad caprichosa" ("whimsical identity"). La identidad $n+1 = 2^n$ sólo se cumple para $n = 0, 1$. Por tanto, si GCH se verifica, entonces $\aleph_0$ se podría definir como el cardinal antes del cual GCH es falsa (exceptuando 0 y 1) y después del cual GCH es verdadera. Este argumento se basa en la creencia en que el universo de la teoría de conjuntos debería de ser lo suficientemente rico para descartar estas "identidades accidentales". Además, tal identidad contradeciría el *principio de uniformidad* que muchos defienden como una *regla heurística* válida para la teoría de conjuntos. Este principio se puede formular así: *"El universo de los conjuntos no cambia su carácter sustancialmente cuando se pasa de cardinales más pequeños a cardinales o conjuntos mayores, es decir, los mismos o similares patrones reaparecen repetidamente (quizá en versiones más complicadas)"* [108]. Esta singularidad de $\aleph_0$ iría en contra de dicho principio.

Un argumento persuasivo contra CH ha sido formulado por C. Freiling en [46] (véanse también [32, 87]). Consideremos una competición entre dos personas A y B que arrojan dardos a una diana de forma completamente aleatoria e independiente. Supongamos que los puntos de la diana se han puesto en correspondencia biunívoca con los números reales, de modo que lanzar un dardo a la diana es, simplemente, generar un número real aleatoriamente. Para decidir el ganador, se fija una buena ordenación de $\mathbb{R}$ y gana el competidor que lance el dardo a un punto con el número mayor en esta ordenación. Supongamos además que CH es verdadera. Entonces la buena ordenación de $\mathbb{R}$ se puede haber elegido de forma que el conjunto ordenado resultante sea orden-isomorfo a $\aleph_1$ y, como este es el primer ordinal no numerable, se deduce que todos los segmentos iniciales $\mathbb{R}_x = \{r \in \mathbb{R} \mid r \leq x\}$ son numerables, es decir, para cada punto P de la diana, el conjunto $S_P = \{Q \mid Q \leq P\}$ es numerable. En consecuencia, dado que un conjunto numerable tiene medida nula, si A lanza primero y su dardo se clava en P, la probabilidad de que el dardo de B caiga en un punto de S_P es cero y, por tanto, con probabilidad 1, B gana. Pero como los lanzamientos eran independientes, se puede suponer también, sin variar para nada la competición, que es B quien ha lanzado primero. En este caso, por el razonamiento simétrico, es A quien gana con probabilidad 1. Se llega así a una contradicción que muestra que CH es falsa. El problema es que, si se trata de hacer riguroso el argumento en el contexto de la teoría de la medida, es necesario demostrar que el grafo de la buena ordenación utilizada es medible, cosa que no se ha justificado en absoluto. Sin embargo, esto parece proporcionar evidencia intuitiva bastante plausible en contra de CH y, en apoyo de esta aseveración, citaré unas palabras de David Mumford en [87]:

Esto nos lleva al pasmoso resultado de Christopher Freiling (1986): usando la idea de lanzar dardos, podemos refutar la hipótesis del continuo. Desconozco la razón por la que este teorema no es universalmente cono-

> *cido y considerado al nivel de los resultados de Gödel y Cohen. [...] Así, ¿rechazaremos la demostración? Freiling usó el argumento para motivar un nuevo axioma de la teoría de conjuntos que refuta la hipótesis del continuo. Creo que deberíamos ir mucho más lejos: su 'demostración' muestra que si hacemos de las variables aleatorias uno de los elementos básicos de las matemáticas, se deduce que CH es falsa y nos libraremos de uno de los acertijos sin significado de la teoría de conjuntos.*

Freiling enmarcó su argumento en un axioma "de simetría" que es intuitivamente muy plausible y formalmente equivalente (en ZFC) a $\neg$CH. Este axioma, $\mathrm{A}_{\aleph_0}$ postula que para toda función $f : \mathbb{R} \to \mathbb{R}_{\aleph_0}$ que asigna a cada número real un conjunto numerable de números reales, existen $x_1, x_2 \in \mathbb{R}$ tales que $x_1 \notin f(x_2)$ y $x_2 \notin f(x_1)$. La razón por la que $\mathrm{A}_{\aleph_0}$ implica $\neg$CH es justo la que vimos en la discusión precedente: si suponemos CH, podemos considerar una buena ordenación de $\mathbb{R}$ con segmentos iniciales numerables y la función que a cada número real le hace corresponder el segmento inicial correspondiente no satisface $\mathrm{A}_{\aleph_0}$. La plausibilidad de $\mathrm{A}_{\aleph_0}$ procede de que podemos imaginar que x_1 y x_2 se pueden encontrar lanzando independientemente dos dardos aleatorios y, de hecho, como Freiling observa, $\mathrm{A}_{\aleph_0}$ es incluso más débil que nuestra intuición porque lo único que afirma es que lo que heurísticamente va a ocurrir siempre, es posible que ocurra, de modo que, si, por un milagro, $x_2 \in f(x_1)$, siempre podríamos lanzar el dardo de nuevo.

Una objección al argumento de Freiling consiste en la observación de que es posible modificarlo para dirigirlo contra el axioma de elección (AC). Se puede pensar que el argumento se basa en que un subconjunto numerable de los reales tiene un complemento de cardinalidad mayor y así es infinitamente más probable que dicho complemento sea alcanzado por un dardo. Esta idea es plausible y lleva a considerar, de forma totalmente análoga, el axioma $\mathrm{A}_{<2^{\aleph_0}}$, similar a $\mathrm{A}_{\aleph_0}$, con la única diferencia de que se refiere a funciones $f : \mathbb{R} \to \mathbb{R}_{<2^{\aleph_0}}$ de los reales a conjuntos de reales con cardinalidad menor que la del continuo. Como en el razonamiento anterior, este axioma implica que $\mathbb{R}$ no puede ser bien ordenado y es, por tanto, inconsistente con ZFC (pues contradice AC). Sin embargo, Freiling aduce que la evidencia contra el axioma de elección no es tan fuerte pues la idea de que los conjuntos de cardinalidad $< 2^{\aleph_0}$ tienen probabilidad cero parece sólo una intuición sin ningún argumento sólido que la soporte: la razón por la que un dardo aleatorio no caerá en un subconjunto numerable predeterminado no es que dicho conjunto tiene cardinalidad menor que la de $\mathbb{R}$, sino que tiene medida de Lebesgue 0. Por otra parte, se podría argumentar también que, con independencia de que CH sea o no cierta, $\mathbb{R}$ tiene un subconjunto X de cardinalidad $\aleph_1$, el cual, de manera similar, no podría ser bien ordenado, contradiciendo AC. Pero este argumento es diferente del considerado por Freiling pues aquí la intuición física que nos permitía tomar un número real aleatoriamente ya no nos acompaña. Si la cardinalidad de $\mathbb{R}$ es mayor que $\aleph_1$, no tenemos ni idea de cómo sería el conjunto X y ¿cómo podríamos entonces lanzarle un dardo?

El experimento mental de Freiling, aun siendo bastante persuasivo para algunos matemáticos, no es, en general, aceptado como una solución a CH y persiste la idea de tratar de hallar esta solución a través de nuevos axiomas. Entre los nuevos axiomas que se han introducido, destacan los ya mencionados axiomas de cardinales grandes, que aseguran la existencia de infinitos de orden superior, que van más allá de los infinitos más pequeños de la misma forma que el infinito va más allá de lo finito. Su estudio es una de las principales ramas de la teoría de conjuntos a partir de los años 1970 [29] y su justificación proviene tanto de su contenido intuitivo y su armonía con el llamado *principio de reflexión* —una regla heurística que goza de gran aceptación en teoría de conjuntos—[33] como de su éxito para decidir un gran número de enunciados que ZFC no puede probar [64]. Por todo ello existe un cierto consenso entre los especialistas en conjuntos para aceptarlos. Por ejemplo, un cardinal κ se dice (fuertemente) *inaccesible* si es no numerable, regular (es decir, no existe una aplicación cofinal $f : \alpha \to \kappa$, donde α es un ordinal menor que κ o, en otras palabras, κ no es la unión de menos de κ conjuntos de cardinalidad menor que κ), y verifica que, para todo cardinal $\mu < \kappa$, $2^\mu < \kappa$ [66, p. 32]. Si κ es un cardinal inaccesible, entonces V_κ es un modelo de ZFC (las propiedades de V se reflejan en V_κ). Esto muestra que la existencia de un inaccesible κ es independiente de ZFC pues, en caso contrario, la demostración de que V_κ es un modelo de ZFC se podría formalizar en ZFC, probando su consistencia, lo que contradice el teorema de incompletitud de Gödel si, como suponemos, ZFC es consistente[34] (cf. [57, 98]).

Los inaccesibles (junto con los *débilmente inaccesibles*) fueron los primeros cardinales grandes que se consideraron y su existencia no sólo implica la consistencia de ZFC sino que (ZFC + "Existe un inaccesible") es *equiconsistente* —en el sentido de que la consistencia de una de estas teorías implica la de la otra— con (ZF + "Todos los subconjuntos de $\mathbb{R}$ son medibles Lebesgue"). Este resultado tiene una cierta asimetría al aparecer en él ZF, debido a que el axioma de elección garantiza la existencia de conjuntos no medibles, pero la cosa no termina aquí sino que parece ser también que cada extensión natural de ZFC (determinada, por ejemplo, añadiendo a ZFC alguna propiedad interesante de teoría de conjuntos descriptiva) es equiconsistente con una extensión axiomatizada por algún axioma de cardinales grandes. Por ejemplo, mencionaré sin dar las definiciones que (ZFC + "Existe una extensión total de la medida de Lebesgue") es equiconsistente con (ZFC + "Existe un cardinal medible"),[35] y resultados similares existen para muchos otros cardinales grandes. Además, las "fuerzas de consistencia" correspondientes a los cardinales grandes parecen estar bien ordenadas (la consistencia de la existencia de los más grandes implica la de la existencia de los más pequeños) mostrando una especie de "camino hacia arriba" marcado por los axiomas de cardinales grandes. Esto hace que estos axiomas sean considerados generalmente como la forma más natural y fructífera de extender ZFC ([58, 64, 71]) y refuerzan la idea de que la adición de nuevos axiomas es legítima. Sin embargo, los axiomas habituales de cardinales grandes no

[33]En palabras de P. Maddy, [71]: *"el universo de los conjuntos es tan complejo que no puede ser descrito completamente; por tanto, algo que es cierto en todo el universo tiene que ser ya cierto en algún segmento inicial suyo. En otras palabras, cualquier intento de describir únicamente V también se aplica a algún V_α más pequeño que 'refleja' la propiedad atribuida a V".*

[34]Más concretamente, el segundo teorema de incompletitud [50], según el cual ZFC —y, en general, cualquier extensión recursiva de la aritmética de Peano— no puede probar su propia consistencia a menos que sea inconsistente.

[35]Este es un resultado de Solovay [105].

dicen nada sobre la hipótesis del continuo. A pesar de ello, estos axiomas juegan un papel relevante en los intentos de resolver CH puesto que, por una parte, su éxito sugiere que la adición de nuevos axiomas también es el camino natural para intentarlo y, por otra, que los axiomas que se añadan deberán ser compatibles con la existencia de cardinales grandes. Estos son los principios básicos que han guiado a W.H. Woodin en el intento de resolver —negativamente— CH que ha desarrollado en años recientes. En lugar de buscar un axioma concreto que lleve al resultado deseado, ha estudiado las condiciones que un tal axioma debería cumplir, lo que le ha llevado a la siguiente conjetura [29]:

> *Toda teoría obtenida añadiendo a ZFC un axioma que es compatible con la existencia de cardinales grandes y hace que las propiedades de conjuntos con cardinalidad hereditaria a lo sumo $\aleph_1$ sean invariantes bajo "forcing", implica que la hipótesis del continuo es falsa.*

Los resultados de Woodin se acercan mucho a resolver esta conjetura, mostrando que se verifica para una parte sustancial de la jerarquía de los cardinales grandes. Woodin se ha apoyado en estos resultados para defender la tesis —opuesta a la de Feferman— de que el concepto de conjunto arbitrario no es "inherentemente vago" y de que los resultados de independencia sobre CH (independencia no sólo de ZFC sino también de ZFC junto con axiomas de cardinales grandes), lo único que hacen es mostrar que CH es un problema muy difícil. Aunque no puede afirmarse que esta sea "la" solución definitiva a la hipótesis del continuo, sí se puede decir que proporciona "una" solución negativa a la misma bajo unas hipótesis que a los expertos en teoría de conjuntos les parecen muy plausibles. Para una discusión detallada de la conveniencia de añadir nuevos axiomas a ZFC y, en particular, de los resultados de Woodin se pueden ver [4, 28, 29, 111].

Entre los especialistas que han mostrado cierta simpatía por la hipótesis del continuo hay uno muy importante, pues es una persona que ha hecho contribuciones fundamentales en la mayor parte de los aspectos de la teoría de conjuntos.[36] Se trata de Saharon Shelah quien, en [103], ha seguido un camino diferente al consistente en buscar nuevos axiomas y ha reformulado GCH mediante una redefinición de la exponenciación de cardinales, probando un teorema que tiene consecuencias similares a GCH. Sin embargo, a pesar del indudable interés de este resultado, pocos creen que que sea un sustituto válido a una solución de "la verdadera GCH".

La hipótesis del continuo es el problema más conocido entre los que son indecidibles en ZFC. Sin embargo, no es ni mucho menos el único con esta característica y también existen muchas cuestiones indecidibles situadas fuera del ámbito de la teoría de conjuntos propiamente dicha. Los métodos conjuntistas tienen, en particular, muchas aplicaciones en análisis, en topología, en la teoría de grupos abelianos y en álgebra homológica. S. Shelah también ha tenido que ver con muchas de estas aplicaciones y, en particular, como se indica en [36], la utilización moderna de métodos conjuntistas en álgebra comenzó el 11 de julio de 1973, cuando Shelah, que

[36] Otro especialista que ha postulado una "solución" alternativa a la de Woodin es M. Foreman [43]. Dicha solución se basa en los llamados *cardinales grandes generalizados*, que permiten resolver afirmativamente CH.

entonces era muy joven, tomó prestado un ejemplar del libro de Lázsló Fuchs *Infinite abelian groups* en la biblioteca de la Universidad Hebrea de Jerusalén y se interesó por el *problema de Whitehead*. Este problema había sido planteado por J.H.C. Whitehead en 1952 y preguntaba si un grupo abeliano A que satisface la condición $\mathrm{Ext}(A, \mathbb{Z}) = 0$ (en otras palabras, $\mathbb{Z} \subseteq B$ y $B/\mathbb{Z} \cong A$ implican $B \cong \mathbb{Z} \oplus A$) ha de ser necesariamente libre. Shelah tuvo la idea de abordar el problema investigando los conjuntos subyacentes y probó que, incluso para grupos de cardinalidad $\aleph_1$, el problema de Whitehead es indecidible en ZFC.

Para empezar, Shelah consideró el universo constructible L y demostró que, en él, si un grupo abeliano A satisface la condición $\mathrm{Ext}(A, \mathbb{Z}) = 0$, entonces A es libre. Por otra parte, consideró el *axioma de Martin* (MA) [36, p. 170], el cual procede de la teoría del "forcing". MA no se verifica en el universo constructible, pero MA + ¬CH es consistente con ZFC y Shelah probó que en la teoría ZFC + MA + ¬CH hay grupos abelianos que satisfacen $\mathrm{Ext}(A, \mathbb{Z}) = 0$ pero no son libres (cf. [36, Theorem XII.2.5] o el trabajo original de Shelah [101]). En consecuencia, se puede decir que, en la teoría ZFC, el problema de Whitehead es indecidible y, pocos años después, Shelah demostró incluso que también es indecidible en ZFC + GCH. El resultado de Shelah fue completamente inesperado pues, aunque ya se conocían muchos ejemplos de cuestiones indecidibles, todas ellas estaban enmarcados en la teoría de conjuntos y este fue el primer problema puramente algebraico que también resultó serlo. Como consecuencia del impacto causado por este resultado, el uso de métodos conjuntistas en otras partes de las matemáticas y, en particular, en álgebra, recibió un gran impulso. Una muestra representativa de la aplicabilidad de estos métodos al álgebra la proporciona el libro [36].

El trabajo de S. Shelah abarca casi toda la teoría de conjuntos moderna y puede servir de ejemplo para mostrar cómo esta se ha desarrollado como una rama de las matemáticas con total independencia de los aspectos fundacionales (a los que Shelah apenas ha contribuido). Es muy interesante el artículo [102], donde Shelah expresa no sólo sus ideas sobre la evolución futura de la teoría de conjuntos sino también su percepción actual de la misma. Por ejemplo, establece una serie de aspectos que motivan su trabajo, atribuyendo a cada uno de ellos una puntuación expresada por un cierto número de signos de admiración. Así, la *belleza* es su máxima motivación con nueve signos —en la estela de Hardy: *"Beauty is the first test."*—, seguida de la *generalidad* con seis y la *"demostración con 'huesos' o, al menos, 'carne'"* (sic) con cinco, mientras que, en contraste, las *aplicaciones a las matemáticas* sólo reciben tres signos y los *fundamentos y las aplicaciones a la filosofía* un único signo. Sobre este último aspecto comenta:

> *Muchos ponen gran énfasis en el papel de los fundamentos y la filosofía. No tengo ninguna objeción a esos aspectos en sí, pero desconfío de ellos. Mi impresión puede ser similar a la de muchos autores que, aun reconociendo el papel de los críticos literarios en la vida cultural, piensan que seguir sus dictados llevará a obras aburridas —pero que las suyas, claro está, brillarán eternamente a causa de su belleza intrínseca.*[37]

[37] La reticencia de Shelah hacia las cuestiones fundacionales no es menor que la de muchos

CÍRCULOS VICIOSOS

Il y a plus affaire á interpreter les interpretations qu'á interpreter les choses, et plus de livres sur les livres que sur autre subject: nous ne faisons que nous entregloser.

(Montaigne, Les Essais, De l'Experience.)

En las secciones precedentes hemos analizado la cuestión de si los conjuntos son objetos matemáticos muy fáciles de comprender y, como hemos visto, esta presunción no está del todo justificada pues, ya al considerar los subconjuntos del conjunto de los números naturales, surgen problemas muy difíciles que permanecen sin una solución satisfactoria y que, en ocasiones, dan lugar a la existencia de respuestas incompatibles entre sí, pues dependen de la concepción filosófica que se adopte. A pesar de todo, muchos sostienen que el universo V, del que tenemos una fuerte intuición, encarna todos los aspectos esenciales del concepto de conjunto. Sin embargo, como vamos a ver, también hay razones de peso para dudar de esta premisa. El universo V está formado por conjuntos bien fundados, es decir, por conjuntos tales que todo subconjunto no vacío contiene un elemento que es *minimal* en el sentido de que tiene intersección vacía con el propio subconjunto. El axioma de ZFC que permite identificar "el universo" de la teoría de conjuntos con V es el de fundación.[38] Este axioma es equivalente a la no existencia de $\in$-cadenas descendentes infinitas y, en consecuencia, no permite la existencia de "conjuntos circulares" como $x = \{x\}$ ni la existencia de ciclos de la forma $x_1 \in x_2 \in \cdots \in x_n \in x_1$. Sobre estos conjuntos dice K. Kunen [66, p. 94, p. 101]:

Segunda cuestión irrelevante. ¿Existe un x tal que $x = \{x\}$? [...] nuestra adopción del axioma de fundación no dice nada sobre si existe realmente *(con independencia de lo que esto signifique) algún x tal que $x = \{x\}$; simplemente nos abstenemos de considerar un tal x. [...] A diferencia de los otros axiomas de ZFC, el de fundación no tiene aplicación a las matemáticas ordinarias, pues su aceptación equivale a restringir nuestra atención a la clase de los conjuntos bien fundados, donde todas las matemáticas se desarrollan.*

Esta opinión de Kunen es bastante representativa: la adopción del axioma de fundación no es un asunto fundamental sino sólo una cuestión de higiene que lo único que hace es evitar el uso de conjuntos "extraños" que no son necesarios para las matemáticas. Sin embargo, en los últimos 20 años se ha explorado la posibilidad de que, después de todo, es posible que existan conjuntos que, sin ser bien fundados, sean no obstante útiles para modelar ciertos fenómenos de interés, sobre todo en informática. En este ámbito ya he mencionado la idea de modelar los flujos como

---

matemáticos que trabajan en campos mucho más alejados de estas; quizá trata de destacar así la autonomía de la teoría de conjuntos como una parte de pleno derecho de las matemáticas.

[38] Este axioma se expresa a veces mediante la igualdad $V = WF$, donde V denota el universo de los conjuntos y WF el de los conjuntos bien fundados (por ejemplo, en [66]). En la definición antes dada de V ya se suponía la verificación del axioma de fundación, por lo que dicha definición es realmente la de WF.

pares ordenados y también un ejemplo concreto definido por $f = (a, (b, f))$. Esta idea se acomoda bien a nuestra intuición pero tiene un pequeño inconveniente. Supongamos que definimos, en general, un flujo f como un par ordenado $f = (a, f')$, donde $a \in A$ (A es un alfabeto) y f' es otro flujo. Entonces es natural definir el conjunto $\mathrm{Fl}(A)$, de flujos sobre A como el mayor conjunto que satisface la condición siguiente: si $f \in \mathrm{Fl}(A)$, entonces $f = (a, f')$ para algún $a \in A$ y algún $f' \in \mathrm{Fl}(A)$ [7]. El problema es que, siendo $f = (a, f') = \{\{a\}, \{a, f'\}\}$, se tiene que $f' \in \{a, f'\} \in f$ o, en otras palabras, f' pertenece a la clausura transitiva de f (el menor conjunto transitivo que contiene a f). Como $f' = (b, f'')$, etc., se obtiene una $\in$-cadena descendente infinita, que está prohibida por el axioma de fundación. Por tanto, dicho axioma tiene como consecuencia que $\mathrm{Fl}(A) = \emptyset$. Esto proporciona una buena motivación para prescindir del axioma de fundación y admitir en nuestro universo conjuntos que no son bien fundados. Estos son los conjuntos b para los que existe una cadena descendente infinita:

$$\cdots \in a_{n+1} \in a_n \in \cdots \in a_1 \in b$$

y se les suele llamar también, siguiendo a [8], *hiperconjuntos*. Un ejemplo sencillo de hiperconjunto es $x = \{0, \{0, \{0, \{0, \ldots\}\}\}\}$, puesto que $x \in x$. Intuitivamente, este hiperconjunto está definido por la ecuación $x = \{0, x\}$ pero el manejo de ecuaciones de este tipo plantea algunos problemas que es necesario resolver. La pregunta más básica es si así estamos definiendo un nuevo conjunto y también podemos preguntarnos si el conjunto $y = \{0, y\}$ es igual al conjunto x anterior. El axioma de extensionalidad no es suficiente para aclarar esto, pues simplemente nos dice que "x es igual a y si y sólo x es igual a y", lo cual no es de mucha ayuda. Aunque tenemos la intuición clara de que x e y deben ser iguales, es necesario aclarar estas cuestiones y, para ello, será útil pensar en los conjuntos de una forma diferente a la que estamos acostumbrados.

Aunque la relación $\in$ sólo está sujeta a lo especificado por los axiomas de la teoría de conjuntos, la imagen habitual que tenemos es la de un conjunto como una caja o un contenedor, donde se encuentran los elementos, que pertenecen a él. Esta idea ya la tenía Cantor, quien definió un conjunto como una "colección" de objetos, y es la intuición que motiva la jerarquía acumulativa y el axioma de fundación. Pero, como ya he indicado anteriormente, también existe la posibilidad de pensar en los conjuntos como objetos matemáticos que se obtienen a partir de otros más complejos "olvidando la estructura". Una imagen que ha sido decisiva para el desarrollo de la teoría de hiperconjuntos es que cada conjunto b puede ser representado por un grafo dirigido. Para ello, consideremos el grafo cuyos vértices son b y los elementos de la clausura transitiva de b, en el cual hay una arista del vértice x al vértice y precisamente cuando $y \in x$. De esta forma, el grafo representa la estructura de pertenencia hereditaria de b. Los grafos resultantes se suelen llamar *grafos punteados accesibles* [7] (abreviadamente gpa), pues son grafos dirigidos junto con un vértice distinguido p (que, en la representación descrita, corresponde al propio conjunto) que tiene la propiedad de que cualquier vértice distinto de él se puede alcanzar mediante un camino finito que parte de p. Esta idea de asociar grafos con conjuntos es mucho más fructífera y profunda de lo que parece a primera vista si se piensa en los conjuntos como objetos obtenidos olvidando la estructura, es decir, si consideramos los grafos como objetos *preexistentes* a los conjuntos que representan. Esta fue la idea que guió a Peter Aczel [2] para desarrollar su teoría de conjuntos *no bien fundados* (hiperconjuntos). En efecto, se puede demostrar en ZFC$^-$ (ZFC sin el axioma de fundación) que todo gpa sin cadenas descendentes infinitas (que se puede llamar bien fundado) representa un único conjunto y, naturalmente, en ZFC se tiene que sólo los gpa bien fundados pueden representar conjuntos (que, en presencia del axioma de fundación, tienen que ser bien fundados). La intuición de Aczel fue que deberíamos pensar en los conjuntos como los objetos que se pueden representar por un gpa arbitrario. Precisando un poco más, se puede definir una *decoración* de un grafo dirigido como una función d cuyo dominio es el conjunto de los vértices y cuyos valores son conjuntos, satisfaciendo que para cada vértice n, $d(n) = \{d(m) \mid n \to m\}$, donde $n \to m$ significa que "m es un hijo de n", o sea, que hay una arista del vértice n al vértice m. Se dice entonces que un gpa G con punto distinguido p representa el conjunto b cuando existe una decoración d de G tal que $d(p) = b$. La idea de Aczel es capturada por el *Axioma de Anti-Fundación*, que ya había sido considerado previamente por Forti y Honsell [44]:

AFA: *Todo gpa representa un conjunto único.*

Alternativamente, AFA se puede también enunciar de la forma siguiente: *Todo gpa tiene una única decoración.* La colección de axiomas ZFC$^-$ + AFA se denota por ZFA y los elementos del universo que describe son precisamente los hiperconjuntos. Observemos que AFA tiene dos vertientes, por una parte proporciona la existencia de hiperconjuntos y, por otra, resuelve el problema de cuándo dos hiperconjuntos deben considerarse iguales. Por ejemplo, el gpa consistente en un único vértice p y una única arista (un bucle) de p a p define el hiperconjunto más sencillo (llamado, a veces, *átomo de Quine* o también *conjunto reflexivo* [55]) $\Omega = \{\Omega\}$. Este hiperconjunto es único y la unicidad también muestra que los hiperconjuntos $x = \{0, x\}$ e $y = \{0, y\}$ anteriormente considerados son, en realidad, el mismo.

La relación entre ZFA y ZFC es la siguiente: Si ZFC$^-$ es consistente, entonces también lo es ZFA. De hecho, se puede extender de forma canónica un modelo de ZFC$^-$ para obtener un modelo de ZFA. Esto muestra que ZFA es una extensión de ZFC$^-$ que no cambia las matemáticas que se desarrollan en este último ámbito, pues no puede dar lugar a nuevos resultados referidos sólo a conjuntos bien fundados. Se tiene así una situación que, como se observa en [7], es semejante a la que se produce cuando se extienden los números reales para dar lugar a los complejos, pues se gana la posibilidad de resolver ciertas ecuaciones mediante los nuevos objetos introducidos sin perder ninguno de los objetos originales. La analogía con las ecuaciones no es meramente formal sino que, de hecho, AFA puede ser formulado en términos de sistemas de ecuaciones. Consideremos, por ejemplo, el sistema formado por las ecuaciones siguientes, donde x, y, z son las variables: $x = \{y, z\}$; $y = \{2, z\}$; $z = \{2, \Omega, y\}$. Entonces, está claro intuitivamente que se puede construir un grafo que representa la relación de pertenencia en una posible solución del sistema. Si se aplica AFA a este grafo, se obtienen conjuntos X, Y, Z, que resuelven el sistema de ecuaciones en las variables x, y, z; cf. [7, 31, 8] para los detalles. De hecho, el llamado *Lema* *de la Solución* [8] proporciona la existencia de solución única para ciertos tipos de sistemas de ecuaciones como el anterior y, en presencia de ZFC$^-$, es equivalente a AFA. Este lema permite concluir, por ejemplo, que el sistema $x = (a, y)$; $y = (b, x)$, en las variables x e y (donde (a, y) denota el conjunto $\{\{a\}, \{a, y\}\}$ correspondiente al par ordenado) tiene por solución dos hiperconjuntos f y f' que representan flujos, de modo que, en presencia de AFA, el conjunto $\mathrm{Fl}(A)$, que era vacío en ZFC, ya ha dejado de serlo.

De esta forma, hemos conseguido modelar los flujos como pares ordenados aunque, claro está, en ZFC también pueden modelarse los flujos como funciones $f : \mathbb{N} \to A$. Estamos así en presencia de otro episodio de la batalla entre conjuntos y sucesiones para modelar los conceptos básicos de la informática. En [8], se argumenta que el modelo proporcionado por los pares (y, en consecuencia, por los hiperconjuntos), es más natural.[39] Además, existe otra alternativa para modelar fenómenos circulares, y es la proporcionada por la teoría de categorías, que ha encontrado muchas aplicaciones en la informática teórica (véase, por ejemplo, [6, 75], y también [52] para una visión general de las aplicaciones de las categorías a la informática). En este contexto, aspectos como la coinducción y la correcursión, que juegan un papel muy importante en la teoría de hiperconjuntos, se han desarrollado, a través de la utilización de las *coálgebras finales*, más allá de lo que permite el estricto marco conjuntista [60, 86]. Pero, en cualquier caso, está claro que la teoría de hiperconjuntos proporciona una forma nueva y enriquecedora de modelar los fenómenos circulares, y la constatación de este hecho y de la existencia de los “conjuntos extraños” que se utilizan para ello sirve, una vez más, para arrojar nuevas dudas sobre nuestra hipótesis inicial relativa a la sencillez del concepto de conjunto.

Los fenómenos circulares modelados por ZFA han gozado de mala reputación a lo largo de todo el siglo XX.[40] El origen de esta mala reputación se remonta a la aparición de las paradojas en la teoría de conjuntos de Cantor y, en particular, la paradoja —o antinomia— de Russell. Esta surge al considerar el conjunto r formado por todos aquellos conjuntos que no son elementos de sí mismos, $r = \{x \mid x \notin x\}$, para el cual se obtiene inmediatamente que $r \in r$ si y sólo si $r \notin r$, lo cual es una contradicción. Esto se puede considerar simplemente como una demostración por reducción al absurdo de que el conjunto r no puede existir, lo cual soluciona la paradoja, pero está en franca contradicción con la hipótesis básica de Cantor sobre existencia de conjuntos: *“un conjunto es cualquier colección de objetos de nuestra intuición o nuestro pensamiento. . . ”* (o, en otras palabras, cualquier condición determina un conjunto, formado por los elementos que satisfacen dicha condición). Esta idea tuvo que ser abandonada y sustituida en las teorías axiomáticas por el axioma de subconjuntos o de separación, que es más débil pues sólo postula la existencia del *subconjunto* de un conjunto dado formado por los elementos que satisfacen una

[39] Esto es muy discutible porque el concepto de sucesión parece estar fuertemente enraizado en nuestra intuición, de modo previo al modelo proporcionado por las funciones sobre los números naturales.

[40] Quizá convendría precisar que esto ha sido así en la filosofía occidental, pero no en las orientales. En particular, el budismo no considera que la vida sea lineal, sino circular, recorriendo un ciclo que no termina nunca.

condición determinada. Como casi todas las paradojas, la de Russell se origina por la interacción de la circularidad con la negación. La perspectiva logicista, bajo la cual los conjuntos habrían de ser “definidos” en términos de la lógica, llevó a Russell a declarar la ilicitud de la circularidad: *Lo que involucra a toda una colección no puede ser uno de la colección* (cf. [8, p. 80]). Esta idea ha permanecido omnipresente en la lógica y también se manifiesta en el lenguaje ordinario, donde se habla de *círculos viciosos* para referirse al razonamiento circular. Sin embargo, la circularidad, por sí sola, no es la culpable de los problemas causados por las paradojas y es fácil ver que en el contexto de la teoría de hiperconjuntos la paradoja de Russell no plantea ningún problema adicional [7, 8].[41]

Las paradojas relacionadas con la circularidad surgieron mucho antes de que se hablara de conjuntos y de la paradoja de Russell. Con anterioridad a las paradojas lógicas como esta, se conocían ya algunas de las que, más tarde, fueron llamadas *paradojas semánticas* porque hacen referencia al “significado” o a la “verdad” de expresiones del lenguaje. La que se podría llamar la *madre de todas las paradojas semánticas* es la *paradoja del mentiroso*[42] que, en su formulación más sencilla —aunque no la más precisa— consiste en la sentencia siguiente: *“Esta sentencia es falsa”*.[43] Durante la crisis fundacional que afectó a la teoría de conjuntos de Cantor surgieron muchas otras paradojas semánticas y, en esos momentos, la opinión predominante entre los matemáticos era la que expresó Peano, refiriéndose a la *paradoja de Richard* [45]: *“Exemplo de Richard non pertine ad mathematica, sed ad linguistica”*. Sin embargo, pronto se iba a ver que las paradojas semánticas sí tenían relación con las matemáticas —a través de la lógica— y, de hecho, la paradoja del mentiroso sirvió de inspiración a Gödel [50] para demostrar su (primer) teorema de incompletitud mediante la construcción, en cualquier sistema formal recursivamente axiomatizable que contenga a la aritmética, de una sentencia que —en un cierto sentido que no precisaré, cf. [76] para los detalles— afirma su propia indemostrabilidad y, por tanto, en caso de ser el sistema consistente, es verdadera (en el modelo estándar de la aritmética) pero no demostrable.[44]

La paradoja del mentiroso también sirvió de inspiración a Tarski para demostrar su *teorema de indefinibilidad de la verdad* [76, p. 79], según el cual no existe una fórmula de la lógica de primer orden que sirva para definir la verdad de todas

[41] La idea de que la paradoja de Russell impide, de alguna forma, desarrollar una teoría de conjuntos no bien fundados, es completamente errónea. Si x es bien fundado, entonces el conjunto $r_x = \{y \in x \mid y \notin y\}$ satisface que $r_x = x$ (y, en particular, $r_x \notin x$). Si, por el contrario, x no es bien fundado, el axioma de separación también nos proporciona $r_x = \{y \in x \mid y \notin y\}$ y lo único que se puede concluir en este caso es que $r_x \notin x$ pues, de no ser así, se tendría que $r_x \in r_x$ si y sólo si $r_x \notin r_x$.

[42] Esta paradoja se remonta al menos al siglo IV antes de Cristo y la atribución más antigua señala que fue incluida por Eubulides de Mileto en una lista de siete acertijos.

[43] Una variante es la versión “reforzada” del mentiroso: *“Esta sentencia no es verdadera”*; esta forma dificulta la “solución” consistente en suponer que la sentencia del mentiroso no es verdadera ni falsa.

[44] Aunque formalistas, como Nelson, que creen que las matemáticas son pura sintaxis, niegan cualquier relación entre el teorema de Gödel y la paradoja del mentiroso. Es cierto que el contenido del teorema de Gödel es sintáctico, pero el propio Gödel reconoció la inspiración proporcionada por la paradoja.

las sentencias de la lógica, es decir que sea satisfecha por las sentencias verdaderas y no lo sea por las demás (en otras palabras, la lógica de primer orden no es un lenguaje *semánticamente cerrado*). Para definir el concepto de verdad en un lenguaje formalizado Tarski propuso considerar una jerarquía de lenguajes. En el nivel más bajo está el *lenguaje objeto* que sólo contiene "expresiones ordinarias" pero no nombres de estas expresiones ni términos semánticos. Para poder referirnos a las expresiones del lenguaje objeto hay que recurrir al siguiente nivel (*metalenguaje*), que ya permite hacerlo y, además, contiene predicados para afirmar la veracidad o la falsedad de una expresión del lenguaje objeto. Si queremos hablar sobre expresiones del metalenguaje tenemos que ir al nivel inmediatamente superior (algo así como al "metametalenguaje") y así sucesivamente, dando lugar a una jerarquía infinita de metalenguajes (esta idea de una estructura jerárquica ya la tuvo Russell al desarrollar la teoría de conjuntos libre de contradicciones mediante la *teoría de tipos*). Como consecuencia de esto, Tarski llegó a la conclusión de que no es posible definir satisfactoriamente el concepto de verdad en los lenguajes naturales, pues en caso de ser semánticamente cerrados serían contradictorios. Sin embargo, sus ideas han inspirado la solución más conocida de la paradoja del mentiroso, que consiste en establecer una estructura jerárquica en el lenguaje natural. Esta línea de razonamiento fue seguida por Quine [95], quien llegó a la conclusión de que la sentencia del mentiroso no está bien formada o, en todo caso, carece de significado, pues tendría que residir simultáneamente en más de un nivel: la frase "es falsa" tendría que aplicarse a sentencias en un lenguaje inferior en la jerarquía y no a la propia sentencia en la que aparece.[45] Pero esta solución de la paradoja no es universalmente aceptada y una alternativa importante surgió en 1975 con la publicación del artículo de S. Kripke *"Outline of a theory of truth"* [65]. Kripke mostró que el razonamiento circular es mucho más frecuente de lo que se suponía y que el que una sentencia sea paradójica puede depender de hechos empíricos, no lingüísticos. Kripke puso un ejemplo famoso de esto mediante las dos sentencias siguientes:

(1) *La mayoría de las declaraciones de Nixon sobre Watergate son falsas.*

(2) *Todo lo que Jones dice sobre Watergate es verdadero.*

Ninguno de estos dos enunciados es intrínsecamente paradójico y hay muchas circunstancias plausibles en las que ambos podrían ser verdaderos sin ningún problema (lo que significa que, aun tomadas conjuntamente, dichas afirmaciones no son intrínsecamente o, si se quiere, lingüísticamente, paradójicas). Pero, como observó Kripke, también hay circunstancias que hacen que ambos enunciados juntos creen una paradoja. Por ejemplo, supongamos que Jones solo afirma (1) sobre Watergate pero Nixon afirma (2) junto con otras dos afirmaciones sobre Watergate, de las cuales una es verdadera y la otra falsa. Parece entonces que (2) es verdadera si y sólo si no es verdadera y esto es así como consecuencia de factores contextuales ajenos a ambas sentencias, como son las otras dos afirmaciones que Nixon hizo sobre Watergate. Por otra parte, Kripke rechazó la estructura jerárquica pues ¿Cómo asignar un nivel a la sentencia (1) de modo que sea superior en una unidad a las declaraciones de Nixon

[45] Algo así como "Si p habla sobre q, q no puede hablar sobre p, luego p no puede hablar sobre p".

sobre Watergate, antes de conocer los niveles de estas? Y si se hubiese asignado este nivel, al hacer Nixon su declaración (2) rompería completamente la estructura jerárquica.

Kripke propuso una teoría de la verdad que no presupone la jerarquía sintáctica de metalenguajes y permite a un lenguaje contener un predicado de verdad aplicable a sus propias sentencias siendo, al mismo tiempo, consistente. Para ello es necesario permitir que algunas sentencias, aun siendo significativas, carezcan de valor de verdad (es decir, no sean verdaderas ni falsas) y la sentencia del mentiroso es una de ellas. El criterio para decidir qué sentencias carecen de valor de verdad no puede ser simplemente el de no atribuirles ese valor cuando den lugar a paradojas y, para obtenerlo, Kripke hizo algo así como establecer una "jerarquía semántica", considerando un lenguaje objeto único que está sujeto a una jerarquía infinita de interpretaciones parciales. Los detalles de la teoría de la verdad de Kripke se pueden ver en [65], pero lo que aquí nos interesa es resaltar el hecho de que mostró que es posible formular un concepto de verdad coherente en un lenguaje con autorreferencia.

En [8], Barwise y Moss se inspiran en Kripke pero proponen, en el contexto de la teoría de modelos basada en hiperconjuntos, una explicación de la paradoja que no implica abandonar la hipótesis de que cualquier afirmación es verdadera o no lo es. Según esta explicación, contenida en [8, Theorem 13.10], lo que parece llevar a una paradoja en el razonamiento es el hecho de que no se tiene en cuenta que la afirmación del mentiroso provoca un cambio pragmático de contexto que hace que este no sea el mismo antes de la afirmación que después de ella (cf. [8, p. 188] para los detalles).

Para concluir, mencionaré que en [8] se consideran muchas otras aplicaciones de los hiperconjuntos, la mayoría de ellas fuera de las matemáticas.[46] Esto nos da una muestra más de la gran versatilidad de los conjuntos y también del hecho de que su aplicabilidad va más allá de las cuestiones fundacionales y de ser un lenguaje básico para las matemáticas.

¿Es posible reducir las matemáticas a la teoría de conjuntos?

De las dos hipótesis iniciales que hemos considerado, la que establece la relevancia de los conjuntos para los fundamentos de las matemáticas es la que postula que estas se pueden reducir a la teoría de conjuntos, la cual se supone que proporciona una base firme para poder desarrollar rigurosamente las matemáticas. Pero incluso la necesidad y la existencia de tales fundamentos es una cuestión discutida sobre la que hay opiniones muy divergentes. El punto de vista clásico, que establece un contraste entre las exigencias de rigor de las matemáticas y las de las otras ciencias, se manifiesta claramente en la Sección 1.1 del libro de J.P. Mayberry [82], titulada

[46] La razón principal de que esta teoría no se haya desarrollado mucho antes es, probablemente, el hecho de no ser necesaria para las matemáticas y que las aplicaciones a la informática no podían haber existido hasta tiempos recientes.

"Why mathematics needs foundations" donde, ya en la primera frase, su autor hace una declaración explícita de esta necesidad [82, p. 3]:

> *Las matemáticas difieren de todas las otras ciencias en el requerimiento de que sus proposiciones han de ser demostradas.*

Por el contrario, Manin dice, al analizar el concepto de demostración en [76, p. 48]:

> *Una demostración sólo llega a ser una demostración después del acto social de 'ser aceptada como tal'. Esto es tan cierto para las matemáticas como para la física, la linguística o la biología.*

Esta declaración es congruente con el escepticismo que Manin muestra sobre la necesidad de fundamentos, expresado en el siguiente comentario sobre el contenido de su libro: *"Los problemas de fundamentos son, en su mayor parte, dejados en silencio. Muy probablemente, la lógica no puede justificar las matemáticas en mayor medida que la biología puede justificar la vida".* Aún mucho más explícito en su rechazo a la necesidad de los fundamentos fue Hilary Putnam en [94]: *"No creo que las matemáticas sean poco claras; tampoco creo que las matemáticas tengan 'fundamentos' ni que los necesiten".* Lo que aquí está rechazando Putnam son los "fundamentos" en el sentido de los medios que tratan de justificar que el conocimiento matemático es *a priori* y, en consecuencia, tratan de proporcionar a las matemáticas un rigor absoluto, en oposición a las ciencias empíricas, que carecen de él (una posición implícitamente defendida en la cita anterior de Mayberry).

En cualquier caso, está muy extendida la idea de que los conjuntos parecen proporcionar un lenguaje común que eventualmente podría permitir obtener demostraciones de teoremas matemáticos que fuesen mecánicamente verificables. Este es el punto de vista defendido por los autores de [13], donde se insiste en que es muy importante la posibilidad de traducir las matemáticas a conjuntos pues si alguien afirma haber demostrado un teorema importante y uno no comprende algunas de las nociones manejadas, le podría pedir al demostrador que las defina de modo preciso, hasta reducir la demostración a ZFC, de modo que se convierta en mecánica. Aquí hay varios aspectos discutibles. En primer lugar, es muy probable que no sea *factible* en la mayoría de los casos hacer esa traducción pero, además, dejando por el momento a un lado esta dificultad, se puede argumentar que aun en los casos en que sea posible, no parece que sea deseable o, al menos, no lo sería por la razón que se acaba de exponer, es decir, dicha traducción no serviría para convencer mejor a otros seres humanos de la validez de la demostración. En efecto, la creencia en que una deducción formal puede ser comprobada fácilmente por una persona[47] no parece estar justificada y existen muchos indicios de que, por el contrario, la mente humana no está bien capacitada para el análisis de textos formales, los cuales, por otra parte, rara vez se usan en la comunicación entre matemáticos, salvo quizá en contextos estrechamente relacionados con la lógica. No discutiré aquí en detalle esta cuestión y me limitaré a referirme a los comentarios de Manin [76] en este sentido.

[47] En [76, p. 38] se cita la opinión de J.B. Rosser en el sentido de que *"una vez que una demostración es descubierta y enunciada en lógica simbólica, puede ser comprobada por un imbécil".*

La dificultad humana para analizar y comprender textos formales sugiere la hipótesis plausible de que la única justificación real de un intento de formalizar todas las matemáticas o, al menos, gran parte de ellas, sería el hacer que el conocimiento matemático fuese directamente accesible a los ordenadores, con la esperanza de poder explotar las capacidades de estos para tratar de incrementar dicho conocimiento o para obtener aplicaciones de métodos y resultados matemáticos ya conocidos. En la actualidad existen diversos ámbitos en los que se trabaja en esta dirección, lo cual implica casi siempre hacer uso más o menos explícito de la teoría de conjuntos (y, por supuesto, de la lógica, cf. [90], donde se describen algunas de sus aplicaciones más importantes a la informática). Un área que utiliza con éxito los métodos conjuntistas es la *verificación formal*, que trata de obtener, mediante el uso de métodos formales, demostraciones rigurosas de que sistemas de hardware o de software cumplen una serie de especificaciones.[48]

La verificación formal del software tiene conexiones con otra actividad de este tipo que es mucho más ambiciosa: la demostración automática de teoremas, la cual, a su vez, es un caso particular de lo que se suele llamar *razonamiento automático*. El objetivo de los sistemas denominados *demostradores automáticos de teoremas* es permitir que los ordenadores puedan encontrar, por sí solos, demostraciones de teoremas matemáticos. Dado que los ordenadores son muy aptos para la manipulación sintáctica, esta idea está bastante ligada a la concepción de que las matemáticas son esencialmente lógica, pero no es demasiado popular entre los matemáticos.[49] El fin último sería realizar el sueño de Leibniz de obtener un sistema de cálculo automático que permitiera reducir el razonamiento a computación y algunos han imaginado que, finalmente, todas las matemáticas podrían ser subsumidas en este contexto.

Antes de comentar las dificultades para obtener demostraciones automáticas de teoremas, es necesario señalar que, incluso en el caso de que este programa tuviese éxito, estaríamos muy lejos de poder enmarcar toda la actividad matemática en este ámbito. En efecto, como señala acertadamente Corfield en [23], la investigación matemática comprende, además de la demostración de teoremas, al menos otros dos aspectos muy importantes: la formulación de conjeturas y la formación de conceptos.

[48] Un ejemplo del uso de métodos conjuntistas en este contexto lo proporciona el lenguaje de especificación Z, que está basado en la teoría de conjuntos de Zermelo-Fraenkel y en la lógica de primer orden [112].

[49] Al menos, entre los que no son formalistas. Por otra parte, entre los que trabajan en informática teórica —que, como acertadamente sostiene S. Kahrs en su defensa del formalismo [63], es una subdisciplina de las matemáticas— el formalismo es una opción muy natural y, probablemente, mayoritaria. Por ejemplo, es bien conocida la postura que tenía E.W. Dijkstra, quien en [33] llama "informalistas" a los matemáticos no formalistas y tituló uno de sus manuscritos *"A formula is worth a thousand pictures"*. En el ámbito de la matemática más tradicional, también se observa cómo el área concreta de trabajo puede influir en la concepción filosófica de las matemáticas. Compárese, por ejemplo, la defensa del formalismo hecha por Dales en [24], quien habla desde el punto de vista del "análisis abstracto y el álgebra" con el realismo de V.F.R. Jones [62], quien usa problemas de topología de baja dimensión para describir la "verdad" matemática en términos de la intuición física y de la experiencia espacial. Quizá estas sean manifestaciones de los modos de pensar correspondientes al hemisferio izquierdo y al hemisferio derecho del cerebro, respectivamente, que, como observa Manin en [79], matemáticamente corresponden, aproximadamente, a las dicotomías álgebra/geometría, deducción formal/visión, etc. Todo esto sugiere que la complejidad y diversidad de las matemáticas hacen difícil capturar su esencia en una idea filosófica sencilla.

Además, como argumentó brillantemente Lakatos en [67], estos tres aspectos están estrechamente interrelacionados y ninguno de ellos se puede desarrollar plenamente en ausencia de los otros. La importancia de las conjeturas no puede ser subestimada y se podría decir, contra los que aventuran la tesis reduccionista de que las matemáticas consisten en resolver problemas, que no puede haber buenas respuestas si con anterioridad no ha habido buenas preguntas. Por citar un ejemplo histórico concreto, no es exagerado decir que, además de haber demostrado muchos teoremas importantes, una de las grandes contribuciones que Hilbert hizo a las matemáticas fue la formulación de su famosa lista de problemas en el Congreso Internacional de Matemáticos del año 1900. Muchas de estas cuestiones ya habían sido formuladas o consideradas por otros matemáticos pero fue muy importante la selección y sistematización que Hilbert hizo, pues estos problemas marcaron el desarrollo de gran parte de las matemáticas del siglo XX y algunas de ellas seguirán teniendo impacto (al menos) durante el siglo XXI (por ejemplo, la Hipótesis de Riemann, que permanece abierta).

En cuanto a la formación de conceptos me limitaré también a citar un ejemplo muy claro. El problema de la resolución por radicales de ecuaciones algebraicas de grado 5 o superior, al ser atacado por Galois y Abel, trajo como consecuencia la introducción del concepto de grupo, que es central en matemáticas, con una influencia que se extiende desde la teoría de números y la geometría algebraica a las aplicaciones a la física. La entrada de este concepto en las matemáticas tiene una importancia incomparablemente mayor que la resolución del problema sobre ecuaciones que lo originó.

Hasta la fecha, el mayor éxito en el campo de la demostración automática fue la solución, en 1996, del *problema de Robbins* [83]. El resultado tuvo una cierta repercusión mediática e incluso mereció un artículo en el *New York Times*. El problema preguntaba si un álgebra, con una operación binaria denotada $+$ y una operación unaria n tales que $+$ es conmutativa y asociativa, y que, además, verifica la *ecuación de Robbins*, $n(n(x) + y) + n(x + n(y))) = x$, es un álgebra de Boole (el recíproco ya era conocido). El problema de Robbins fue resuelto afirmativamente por W. McCune con el programa demostrador EQP. El resultado no es trivial (Tarski y algunos de sus estudiantes le dedicaron atención sin conseguir resolverlo) pero lo que un matemático se preguntaría para tratar de discernir su posible interés es si nos ayuda a comprender mejor las álgebras de Boole o, simplemente, si tiene aplicaciones (que, valga la circularidad, deberían de ser "interesantes" para ser tenidas en cuenta).

La ecuación de Robbins no tiene un gran contenido intuitivo y el propio McCune reconoce que el resultado carece de aplicaciones. Por otra parte, parece claro que usar estos axiomas en lugar de los habituales no traería sino inconvenientes, por lo que no es aventurado concluir que, en términos estrictamente matemáticos, el resultado carece de utilidad. Lo mismo puede decirse de muchos otros resultados obtenidos por demostradores automáticos, gran parte de los cuales consisten en encontrar "sistemas minimales de axiomas" o, incluso, axiomas que utilizan un número menor de símbolos que otros ya conocidos. Los resultados de este tipo probablemente se han elegido porque sus demostraciones están muy próximas a las manipulaciones sintácticas que pueden realizar los programas demostradores pero su interés matemático es dudoso.

Por ejemplo, es conocido que los grupos se pueden axiomatizar con un único axioma en términos de una única operación binaria (como demostraron Higman y Neumann en 1952), pero este axioma también carece del significado intuitivo que tienen los usuales y tratar de usarlo en la práctica sería desventajoso. Por eso, el verdadero test para la demostración automática no reside en la obtención de resultados no triviales sino en la de resultados interesantes (en el sentido matemático del término) y parece claro que este test no ha sido superado aún. Pero esto no significa, ni mucho menos, que la demostración automática de teoremas carezca de interés. En primer lugar, el diseño de demostradores y el análisis de los procesos que se pueden utilizar para ello, así como de los resultados obtenidos al atacar problemas concretos, pueden arrojar luz sobre las formas de razonar en matemáticas y, en segundo lugar, es prudente considerar que lo obtenido hasta la fecha son sólo los primeros pasos de un camino que puede ser muy largo. Quizá los demostradores automáticos no lleguen a hacer matemáticas importantes por sí mismos, pero se puede entrever la posibilidad de que lleguen a ser de mucha ayuda para los matemáticos humanos, posiblemente actuando en forma interactiva. Ya hace tiempo que los ordenadores se usan en matemáticas para obtener datos que puedan arrojar luz sobre la viabilidad de conjeturas, y con el desarrollo de los programas de cálculo simbólico se abren perspectivas prometedoras que pueden ir mucho más allá de la simple generación de datos numéricos. Una línea de trabajo interesante, en esta dirección, es la propuesta por el proyecto CALCULEMUS [20], cuyo objetivo es conseguir la integración de los sistemas de deducción automática con los de álgebra computacional.

En cuanto a los otros aspectos mencionados de la actividad matemática, la generación automática de conjeturas parece algo todavía mucho más lejano. No hay indicios de que lo que se podría llamar *inducción mecánica* vaya a ser realizable (y, después de todo, el razonamiento inductivo humano tampoco es universalmente aceptado; recuérdese la declaración de Popper de que "la inducción es un mito"). Por otra parte, aunque una máquina pueda generar conjeturas matemáticas, es difícil de imaginar cómo podría seleccionar las que fuesen interesantes. La posibilidad de que las máquinas puedan llegar a generar conceptos interesantes no debe ser descartada pero parece aún más lejana.

Después de haber discutido la conveniencia de la traducción de las demostraciones matemáticas al lenguaje conjuntista, me detendré un poco a analizar si dicha traducción es factible. Aquí se pueden apreciar dos tipos de dificultades. Una es de tipo puramente práctico y se puede ilustrar recurriendo a los *Principia Mathematica* [99], que fue escrito con la idea de mostrar la viabilidad del *logicismo*, según el cual las matemáticas serían reducibles a la lógica, sin que su desarrollo formal permitiera la aparición de paradojas como las que surgían en la teoría de conjuntos de Cantor. El sistema lógico (*teoría de tipos*) de los *Principia* permitió vislumbrar que, en principio, sería posible desarrollar de esta forma los conceptos básicos de la teoría de conjuntos y, por extensión, de las matemáticas, pero mostró también que lo que era posible, en principio, no sería factible en la práctica. En la edición española de los *Principia* [99], se menciona, en la página 423, después de *54.43:

> *A partir de esta proposición, una vez introducida la suma aritmética, se podrá demostrar que 1+1 = 2.*

Esto significa que Russell y Whitehead no llegaron siquiera a demostrar formalmente este hecho básico sino sólo a indicar *como podría ser demostrado.* Otra ilustración de la distancia entre la matemática formalizada y la matemática real la proporciona la siguiente notación abreviada del término “uno” que —en palabras de Manin [76]— fue imprudentemente introducida por Bourbaki:

$$\tau_Z((\exists u)(\exists U)(u = (U, \{\emptyset\}, Z) \wedge U \subset \{\emptyset\} \times Z \wedge (\forall x)((x \in \{\emptyset\})$$
$$\Rightarrow (\exists y)((x,y) \in U)) \wedge (\forall x)(\forall y)(\forall y')(((x, y \in U \wedge (x,y') \in U)$$
$$\Rightarrow (y = y')) \wedge (\forall y)((y \in Z) \Rightarrow (\exists x)((x,y) \in U)))))$$

Según el propio Bourbaki, escribir este término completamente requeriría decenas de miles de símbolos pero un cálculo más preciso revela que serían más de $4 \cdot 10^{12}$ [81]. Aun usando un formalismo más económico no tendría sentido plantearse la traducción formal de, por ejemplo, la demostración del último teorema de Fermat, con vistas a facilitar su comprensión a otras personas. Requiriría un trabajo gigantesco y el resultado final sería esencialmente incomprensible para los humanos.

Pero, además de la dificultad práctica, hay otro obstáculo muy serio a la posible formalización de todas las matemáticas. El problema surge al considerar lo que es una demostración matemática. En los estudios fundacionales hay una tendencia clara a identificar las demostraciones con deducciones formales en una lógica especificada y, desde este punto de vista, el objetivo de una demostración sería fundamentalmente el de servir como verificación de un resultado. Sin embargo, aun cuando este aspecto es, sin duda, importante, entre los matemáticos está también muy extendida la idea de que hay otro que, probablemente, lo sea incluso más. La idea es que una demostración debe de ser, ante todo, una explicación y que lo que la legitima, más que su estructura formal, es su capacidad de hacernos *comprender* los hechos matemáticos.[50]

En años recientes, diversos autores han insistido en esta idea. Por ejemplo, Manin en [77]:

> *Los axiomas, definiciones y teoremas son lugares en un paisaje matemático, atracciones locales y cruces de carreteras. Las demostraciones son las propias carreteras, los caminos y las autopistas. Todo itinerario tiene sus propias cualidades paisajísticas, que pueden ser más importantes que el hecho de que lleva de A a B.*

Por su parte, Y. Rav [96] abunda en la misma idea:

> *Los teoremas son, en un sentido, sólo etiquetas para las demostraciones, resúmenes de información, titulares de noticias, recursos editoriales...*

[50]Hace ya algunos años tuve la oportunidad de asistir a una conferencia en la que la tesis principal del conferenciante era que *“En matemáticas lo importante son (los enunciados de) los teoremas. Las demostraciones son como las garantías que nos dan cuando compramos electrodomésticos. Como estas, en circunstancias normales sirven solamente para tranquilizarnos y podemos guardarlas en un cajón, de donde sólo las sacaremos si vemos que algo va mal”*. En aquella ocasión no pude dejar de manifestar mi radical discrepancia con esta interpretación, en la línea de que una demostración debe de ser más que una justificación y que, en consecuencia, cabe exigirle mucho más que el que nos tranquilice; según Manin [76, p. 51], si es una buena demostración, debería hacernos más sabios.

> *Pensemos en las demostraciones como una red de carreteras en un sistema de transporte público, y consideremos los enunciados de los teoremas como paradas de autobús; el lugar de las paradas es simplemente un asunto de conveniencia.*[51]

En la misma línea, podríamos también imaginar que las demostraciones son viajes. Pensemos, por ejemplo, en el último teorema de Fermat. Sin duda, su gran importancia histórica proviene, más que del resultado en sí, del largo camino que ha habido que recorrer para demostrarlo.[52] Este camino está jalonado de gran cantidad de ideas y métodos importantes que se fueron introduciendo con el afán de demostrarlo, pero que van mucho más allá y en múltiples direcciones. De hecho, la demostración del teorema de Fermat se puede ver como una pequeña etapa de un gran viaje colectivo que comenzó Galois estudiando la resolubilidad por radicales de las ecuaciones algebraicas, y que continúa en la actualidad con muchas ramificaciones, pudiendo ser observado, por ejemplo, en el *Programa de Langlands* [11].[53] Este programa es un conjunto de profundas conjeturas que se puede interpretar como una *gran unificación* en matemáticas, puesto que postula una estrecha relación entre las representaciones de Galois (enmarcadas en el contexto del álgebra) y las formas automorfas (en el análisis); el último teorema de Fermat y, más en general, la conjetura de Taniyama-Shimura, de la cual es consecuencia, se pueden ver como una pequeña parte del programa de Langlands. El origen de este programa fue una carta manuscrita de 17 páginas que Langlands escribió a André Weil en 1967, donde esbozaba estas sorprendentes conexiones. Los antecedentes históricos se remontan, al menos, a la *ley de reciprocidad cuadrática* que demostró Gauss, la cual fue seguida por otras muchas leyes de reciprocidad que fueron probadas en la segunda mitad del siglo XIX, y en las que es un ingrediente importante la *teoría de Galois*. Posteriormente se desarrolló, durante la segunda mitad del siglo XIX y la primera del XX, la teoría de cuerpos de clases, que busca describir ciertas extensiones de cuerpos que tienen grupo de Galois abeliano. En el marco de esta teoría, Emil Artin obtuvo en 1927 una ley de reciprocidad general (reciprocidad de Artin), que engloba todas las leyes de reciprocidad precedentes. A partir de aquí, era natural tratar de extender la teoría de cuerpos de clases al caso en que el grupo de Galois no es abeliano, y Langlands conjeturó que debería de existir una correspondencia biunívoca entre ciertas representaciones de dimensión n del grupo de Galois de una extensión de un cuerpo K y ciertas representaciones llamadas automorfas del grupo lineal general

[51] El título del artículo de Rav ha sido parafraseado por John Dawson, quien ha presentado una charla titulada *"Why do we re-prove theorems?"*, en la que sugiere acertadamente que la necesidad que a menudo sentimos de dar demostraciones nuevas de resultados ya conocidos apoya la tesis de que son las demostraciones las portadoras del conocimiento matemático.

[52] Esto nos recuerda las palabras de Cavafis en su poema *Itaca*, insistiendo en que es más importante recorrer el camino que llegar al destino: *"Cuando emprendas el viaje hacia Itaca ruega que tu camino sea largo y rico en aventuras y en descubrimientos... Itaca te ha dado un bello viaje. Sin ella nunca lo hubieras emprendido; pero no tiene más que ofrecerte".*

[53] Se vislumbra aquí la posibilidad de un viaje que no termina nunca, como en la secuela moderna de la *Odisea*, de Nikos Kazantzakis, donde Ulises, después de regresar a Itaca, se siente insatisfecho y reemprende el viaje.

$GL(n, K)$.[54] En 2002, Laurent Lafforgue recibió la medalla Fields por su demostración de la correspondencia de Langlands para cuerpos de funciones, pero el caso más importante y más difícil, que es el de los cuerpos de números algebraicos, permanece abierto.

La importancia del programa de Langlands reside fundamentalmente en la unificación que propone, pues es generalmente admitido que el hecho de llegar a observar que objetos muy distintos aparecen como aspectos diferentes de objetos más generales lleva a una comprensión mucho más profunda de los contextos en que dichos objetos aparecen; el objetivo principal aquí es esta comprensión más profunda y no la mera obtención de respuesta a algunas cuestiones.

En el polo opuesto a las demostraciones explicativas se encuentran las demostraciones que se limitan a dar una respuesta sí/no; un ejemplo extremo es la demostración, obtenida en 1988, de que no existen planos proyectivos finitos de orden 10, la cual fue realizada mediante una búsqueda por ordenador [68]. El problema con esta demostración no es tanto que pueda contener errores sino que no da la menor idea de la razón por la que no existen planos proyectivos de este orden ni sobre la existencia o no de planos proyectivos de otros órdenes. No se conoce ningún plano proyectivo finito cuyo orden no sea una potencia de un número primo y, por ejemplo, no se sabe si existe o no un plano proyectivo de orden 12; la demostración del caso de orden 10 no arroja absolutamente ninguna luz sobre lo que puede ocurrir para orden 12. En este caso, y en otros parecidos, el ordenador ha actuado como un oráculo y, como se argumenta en [96], incluso si dispusiésemos de un oráculo (que Rav imaginó como una máquina fantástica llamada Pythiagora que nos respondería sobre la verdad o falsedad de cualquier conjetura), seguiríamos necesitando demostraciones para tener explicaciones. Corfield [23, p. 51] menciona que el oráculo podría ser útil porque le podríamos plantear posibles lemas y el conocimiento de su verdad o falsedad podría ayudarnos a obtener una estrategia para la demostración. Esto es cierto pero no invalida el fondo de la argumentación de Rav. Podemos pensar en una versión más débil del oráculo que no cumpliría esa función: un libro de matemáticas con resultados clásicos que han venido siendo abundantemente utilizados en la literatura, pero que contuviese solamente los enunciados de los axiomas, las definiciones y los teoremas, pero sin demostraciones, ni tampoco imágenes ni comentarios adicionales (que se pueden considerar parte de las demostraciones informales). Este tipo de libros no existe y la causa no es que los posibles lectores fuesen a desconfiar de la validez de los resultados; uno no lee la demostración de un resultado clásico con la esperanza de encontrar un fallo y demostrar que el resultado es falso, sino con la esperanza —y casi diría que con la certeza— de que va a aprender algo.

Una de las razones de la preponderancia que se ha venido atribuyendo a la teoría de conjuntos en los estudios fundacionales reside, probablemente, en el hecho de que estos últimos permanecen centrados en las matemáticas de comienzos del siglo XX y en la propia teoría de conjuntos, ignorando en gran medida la investigación matemática de los últimos 70 años. Esta es la tesis inicial del libro de D. Corfield [23], donde

[54]Explicar esto con precisión exigiría muchas páginas y está fuera del alcance de estas notas. La versión general de la *correspondencia de Langlands*, también llamada *principio de funtorialidad*, es aún mucho más complicada, véase el libro [11] y los artículos [106, 47].

se sostiene la idea de que la filosofía de las matemáticas debe de prestar más atención a las cuestiones que surgen en la práctica matemática actual, incluyendo el papel de los ordenadores en matemáticas, el razonamiento por analogía, el razonamiento plausible y el desarrollo histórico de las matemáticas basado en estudios concretos sobre la emergencia de nuevos conceptos y su importancia para nuestra percepción de las matemáticas y su posible desarrollo futuro. Ni que decir tiene que en este enfoque la teoría de conjuntos no juega, ni mucho menos, el papel prominente que se le reserva en los estudios fundacionales tradicionales y el autor destaca más el papel de la teoría de categorías (y sus variantes, como, por ejemplo las n-categorías) en el desarrollo de las matemáticas. En relación con el papel de la teoría de conjuntos dice:

> *Aunque la teoría de conjuntos muestra ciertas virtudes "fundacionales", tenemos que reconocer que reformular una pieza de matemáticas de esa forma puede ir contra su esencia [...] El precio a pagar por la universalidad es la falta de naturalidad. En lugar de ver los entes y las construcciones de las matemáticas meramente como formados, en último término, por polvo conjuntista, deberíamos tener en cuenta consideraciones estructurales, de la misma forma que un estudiante de anatomía gana poco al ver el esqueleto humano como un mero depósito de calcio.*

El reconocimiento de que los conjuntos proporcionan muy buenos modelos para los conceptos matemáticos básicos no implica admitir la tesis reduccionista subyacente a muchos estudios fundacionales según la cual "las matemáticas son teoría de conjuntos". Como indican Barwise y Moss en [8, p. 5], *"el hecho de que la teoría de conjuntos pueda modelar tantas cosas no significa que los modelos resultantes tengan que ser los mejores modelos"*. Por eso insisten en que los éxitos de la teoría de conjuntos no los impelen a tomarla como "la fundamentación" de las matemáticas y dicen:

> *El saber que cosas como los números reales, funciones, relaciones, etc., pueden ser fielmente representados en la teoría de conjuntos no significa que* sean *conjuntos, de la misma forma que los aviones en que volamos no son los modelos a escala que fueron probados en los túneles de viento.*

Abundando en esta idea, es claro que la descripción conjuntista de los pares ordenados no significa que estos sean precisamente esos conjuntos específicos, entre otras razones, porque la representación conjuntista dista mucho de ser única. En la misma línea, Benacerraf [9] argumentó que los números no pueden ser conjuntos pues, por ejemplo, no puede ser simultáneamente correcto que $2 = \{\emptyset, \{\emptyset\}\}$[55] (considerado como un ordinal en el sentido de Von Neumann, que es el utilizado en estas notas) y que $2 = \{\{\emptyset\}\}$ (considerado como un ordinal en el sentido de Zermelo).[56] Sin embargo, se puede argumentar que la definición conjuntista de Kuratowski y los ordinales

[55] En muchas de sus conferencias, Saunders MacLane solía plantear la siguiente pregunta a sus oyentes: *¿Hay alguien que crea, seriamente, que $2 = \{\emptyset, \{\emptyset\}\}$?*

[56] Esto llevó a Benacerraf a la hipótesis de que las propiedades de los números son esencialmente *estructurales*.

de Von Neumann finitos proporcionan modelos muy satisfactorios de los pares ordenados y de los números naturales, respectivamente. Esta es una razón básica por la que los conjuntos son muy importantes para las matemáticas: permiten modelar de manera clara y precisa muchos conceptos que, de otra forma, serían más difíciles de manejar con el rigor requerido. Por ejemplo, el concepto de aplicación se define a veces de manera no muy precisa indicando que es una regla que a un elemento genérico le hace corresponder otro elemento mediante ciertas operaciones matemáticas. Esto puede dar lugar a una situación ambigua si, por ejemplo, no se hace explícito cuál es el codominio de la aplicación, que es un dato importante en muchas situaciones matemáticas donde es necesario considerar las aplicaciones globalmente y no como meras reglas que van actuando sobre los elementos uno a uno. La definición conjuntista precisa todos los detalles y no deja lugar a la ambigüedad, aunque en contextos concretos, como los lenguajes de programación, esta ambigüedad pueda ser incluso beneficiosa al permitir una mayor versatilidad de los mismos. Por otra parte, además de servir como soporte básico para modelar muchos conceptos matemáticos —y, en gran medida, precisamente como consecuencia de ello— la teoría de conjuntos tiene aplicaciones a otras partes de las matemáticas, no relacionadas con cuestiones "fundacionales" (sin olvidar que también tiene sus propios problemas que, sin duda, forman parte de las matemáticas). Por todas estas razones se puede concluir que, aunque las matemáticas no "sean" teoría de conjuntos, los conjuntos son muy importantes para las matemáticas.

La objetividad, el rigor y la comprensión

> *"Curiouser and curiouser!" cried Alice.*
> (Lewis Carroll, *Alice's Adventures in Wonderland.*)

En relación con los comentarios anteriores, merece la pena señalar explícitamente que las observaciones sobre la insuficiencia del concepto de deducción formal para capturar la idea de demostración no deben ser interpretadas como un argumento en favor de una disminución del rigor en matemáticas. La experiencia muestra, fuera de toda duda, que la formalización no es una condición necesaria para alcanzar un nivel de rigor muy alto y las demostraciones matemáticas informales efectivamente lo alcanzan (aunque, claro está, el "rigor absoluto" no existe en la práctica).[57] En la comunidad matemática rara vez hay discrepancias de fondo sobre la validez de una demostración y, cuando surgen, terminan resolviéndose más pronto que tarde, sin necesidad alguna de recurrir a la formalización. Más aún, cuando las ideas de una demostración son correctas, ni siquiera la aparición de errores concretos es un asunto grave, pues lo habitual es que terminen subsanándose rápidamente. Por ejemplo, es bien sabido que la versión original de la demostración de Wiles del último teorema de Fermat tenía un error, pero pocos dudaron de que la estructura general era correcta y, como era de suponer, la dificultad se superó rápidamente.

[57] René Thom mencionó en [97] que la palabra "rigor" le recuerda el "rigor mortis", pero es posible rechazar la visión formalista de las matemáticas sin renunciar a los niveles de rigor habituales.

Un ejemplo de discrepancia entre matemáticos lo proporcionan las afirmaciones de Louis de Branges (un matemático conocido por haber demostrado la *conjetura de Bieberbach*) de haber demostrado la Hipótesis de Riemann. La gran mayoría de los expertos no considera que sea así y la demostración no ha sido, por el momento, aceptada por la comunidad matemática. A otro nivel, es también frecuente la aparición de "demostraciones" de resultados matemáticos importantes por parte de aficionados que habitualmente carecen de los conocimientos mínimos imprescindibles para llevar a cabo un trabajo coherente. Una vez que el teorema de Fermat ha sido demostrado, el problema favorito en este ámbito parece ser la conjetura de Goldbach, probablemente debido a la sencillez de su enunciado. El medio de difusión habitual de estas pretendidas "demostraciones" suele ser Internet (e-mail, grupos de noticias, páginas web, etc.), pero ninguna de ellas pasa el filtro impuesto por las revistas matemáticas serias.[58] También puede haber discrepancias sobre la validez de una demostración, debidas a la existencia de diferentes ideas sobre qué métodos son aceptables. Por ejemplo, ya se ha mencionado que una pequeña minoría de matemáticos sólo aceptan métodos constructivos. Sin embargo, estas diferencias están usualmente explicitadas de forma clara, de modo que no dan lugar a discusión ni a incertidumbre (aparte, claro está, de posibles discusiones filosóficas). Un matemático constructivista no aceptaría como válida una demostración que utiliza principios existenciales como el axioma de elección pero, a pesar de ello, tendría perfectamente claras las razones por las que otros matemáticos no constructivistas sí la consideran válida.

El gran consenso existente en la comunidad matemática sobre lo que constituye una demostración válida proporciona una gran objetividad a los resultados matemáticos. Ha habido episodios en la historia de las matemáticas en los que algunos de los métodos utilizados eran dudosos. Un ejemplo es el uso de infinitésimos, en los siglos XVII y XVIII que, a pesar de todo, cuando eran usados por matemáticos destacados, rara vez daban lugar a resultados erróneos y, andando el tiempo, fueron vindicados cuando Abraham Robinson desarrolló el *análisis no estándar*. Después de la rigorización que se llevó a cabo en el siglo XIX no ha vuelto a haber episodios históricos similares, ni tampoco fracturas importantes en la comunidad matemática como, por ejemplo, la producida en biología por el lysenkoismo.[59]

A pesar de los comentarios anteriores, hay un campo fronterizo entre la física y las matemáticas donde se ha producido recientemente un episodio que ilustra elo-

[58] Sin embargo, en ocasiones, estas "demostraciones" alcanzan cierta repercusión mediática (usualmente a nivel local). Yo he tenido ocasión de encontrarme con numerosas "demostraciones" elementales del último teorema de Fermat y de la conjetura de Goldbach. En una ocasión tuve una extensa charla con un periodista sobre una persona que, entre otras cosas, pretendía haber demostrado la racionalidad de π. El periodista trataba de averiguar lo que había de cierto en las afirmaciones de este señor (considerado, por algunos, un genio incomprendido) y estaba bastante predispuesto en su favor. Durante una media hora traté de hacerle ver la magnitud de los disparates que figuraban en los escritos de aquel hombre pero el periodista, alegando que él era "de letras", se mostraba refractario a mis argumentos y, al final, terminó preguntándome: *"¿y no estaremos ante otro caso como el de Galileo?"*.

[59] Esta fue una teoría científica que, amparada por el régimen soviético, dominó la biología en la URSS entre los años 30 y los años 60. El lysenkoismo rechazaba la idea darwiniana de la evolución y la genética de Mendel.

cuentemente la imperiosa necesidad de mantener los estándares de rigor existentes. Me refiero al llamado "caso Bogdanoff", que surgió en 2002, cuando comenzaron a circular rumores de que dos hermanos franceses, Igor y Grichka Bogdanoff, habían conseguido publicar en revistas de física (dos de las cuales, *Classical and Quantum Gravity* y *Annals of Physics* tienen alto prestigio) cinco trabajos cuyo contenido era absurdo y se suponía que formaban parte de un engaño deliberado, como respuesta al famoso artículo que el físico Alan Sokal publicó en la revista de sociología *Social Text* con el título *"Transgressing the boundaries: towards a transformative hermeneutics of quantum gravity"*. Este artículo era una parodia llena de jerga sin sentido pero fue aceptado por la revista creyendo que iba completamente en serio. Sin embargo, en el caso Bogdanoff la realidad era diferente, pues estos hermanos, que son periodistas conocidos por dedicarse a realizar programas de divulgación científica para la televisión y acababan de conseguir los títulos de doctor por la Universidad de Borgoña (Grichka en matemáticas e Igor en física)[60] con el mismo material presente en los artículos, sostuvieron en todo momento que la investigación que habían realizado era genuina. El asunto desencadenó una auténtica tempestad en el mundo de la física teórica y las opiniones de los expertos comenzaron a aparecer, la gran mayoría confirmando que el contenido de los artículos era un completo sinsentido. Uno de los primeros físicos matemáticos en darse cuenta de ello fue John Baez, quien tiene una página web [3], donde se puede seguir la fascinante evolución del caso. Otra buena referencia es la Wikipedia [16].

Es significativa la última frase de la recensión, realizada por Robert Oeckl para *Mathematical Reviews*, del artículo que los Bogdanoff publicaron en la revista *Classical and Quantum Gravity*:[61]

> *To conclude, the present paper falls short of scientific standards and appears to have no meaningful content.*

No menos categóricos en sus opiniones han sido otros físicos destacados. Por ejemplo, J. Distler [34]:

> *The Bogdanov's papers consist of buzzwords from various fields of mathematical physics, string theory and quantum gravity, strung together into syntactically correct, but semantically meaningless prose.*

y también David Gross, premio Nobel de física en 2004 [91]:

> *It is easy to judge, even from the abstract alone, that these papers are nutty.*

Al generalizarse la convicción de que los artículos carecían de valor, la revista *Classical and Quantum Gravity* realizó una declaración sin precedentes en la que reconocía explícitamente que la aceptación del artículo de los Bogdanoff había sido un error. Después, el asunto comenzó a tomar aires de ópera bufa, porque surgieron algunos defensores de los Bogdanoff a través de las listas y foros de Internet, la

[60] La tesis de Grichka se titula *"Fluctuations quantiques de la signature de la métrique à l'échelle de Planck"* y la de Igor *"Ètat topologique de l'espace-temps a l'échelle 0"*.

[61] Para no alterar en lo más mínimo su contenido, citaré las opiniones sobre el trabajo de los Bogdanoff literalmente, en el idioma en que fueron formuladas.

mayoría de los cuales se descubrió eventualmente que eran los propios Bogdanoff actuando con nombres inventados [3, 12]. Pero lo interesante no es lo que ellos puedan hacer o decir, sino las implicaciones del caso para la ciencia. No solo los Bogdanoff consiguieron publicar sus trabajos carentes de significado en cinco revistas internacionales de física —algunas de ellas prestigiosas— y una de matemáticas sino que, además, obtuvieron el título de doctor con tesis doctorales de contenido similar, ante tribunales internacionales formados por investigadores reconocidos y después de haber sido objeto de numerosos informes (eso sí, ambas tesis fueron aprobadas con la mención "honorable", que es la mínima para pasar y significa que la tesis es considerada mediocre).

El contenido de los trabajos de los Bogdanoff es altamente especulativo y no tiene soporte experimental, de modo que su fundamento matemático hubiera debido jugar un papel fundamental cuando fueron evaluados antes de su publicación. Pero no parece que haya sido así a juzgar por las declaraciones de expertos como Baez o Distler, de las que se deduce que, matemáticamente, los artículos tampoco tienen sentido. Es inquietante que los filtros que deberían haber servido para detectar el absurdo fallaran repetidamente y más aún lo es que algunos de los implicados justifiquen a posteriori que haya ocurrido así. Las consecuencias son graves pues pueden contribuir a arrojar dudas sobre parte de la física teórica. Por ejemplo, P. Woit (quien en su libro [110], crítico con la *teoría de cuerdas*, dedica un capítulo entero a este asunto), declaró ([3]):

> *The Bogdanoff's work is significantly more incoherent than just about anything else being published. But the increasingly low standard of coherence in the whole field is what allowed them to think they were doing something sensible and to get it published.*

Es curioso que, incluso aquellos que, de alguna manera, se muestran comprensivos con el trabajo de los Bogdanoff, lo hacen sobre la base de que, aun siendo esencialmente incomprensible, podría quizá contener ideas físicas interesantes (aunque tan feliz coincidencia parece bastante improbable teniendo en cuenta que todos están de acuerdo en que la base matemática es muy débil). En esta línea está el comentario de R. Jackiw [91], que fue "rapporteur" de la tesis de Igor Bogdanoff:

> *It showed some originality and some familiarity with the jargon. That's all I ask. [...] It's like modern art. One person looks at a piece of art and says it is gibberish; another person looks and says it's wonderful [...] When physics talks about the universe before the Big Bang, it is completely speculative. I would be very careful before calling something nonsense, especially if I didn't understand it.*

Más crítico es el premio Nobel de física Frank Wilczek [91]:

> *The paper has a lot of the right buzz words. Referees rely on the good will of the authors. [...] The paper is essentially impossible to read, like "Finnegans Wake". [...] This says something profound about what happens to theoretical physics in the absence of the discipline of experiment.*

Es cierto que en este asunto la mayoría de los referees no hicieron bien su trabajo[62] pues, como se señala en [3] a la vista de los informes de algunos de ellos, estaban más preocupados por corregir erratas que por comprobar la lógica de los artículos. Probablemente haya influido el que los artículos sean esencialmente imposibles de leer[63] e incluso incomprensibles. Pero esto, que la mayoría interpreta como señal segura de que carecen de valor, parece que ha sido interpretado por algunos referees como *"no se entiende pero adelante, no vaya a ser que contenga ideas interesantes"*.

La forma y el estilo de los artículos de los Bogdanoff no son los usuales en matemáticas —las demostraciones matemáticas, aun no estando formalizadas son, debido a su gran objetividad, un antídoto eficaz contra situaciones como la descrita— y parece extremadamente improbable que trabajos de este tipo, que algunos han llamado "impresionistas", pudieran ser aceptados en una revista matemática de cierto prestigio.[64] Sin embargo, los autores (bajo su propio nombre o los de álter egos como Yang o Schwartz) se han defendido en muchas ocasiones de los ataques de los físicos alegando que su trabajo es matemático y que los críticos carecen, por lo tanto, de conocimientos para juzgar [109].[65] Se aprovechan así de que su trabajo es una mezcla de especulación física con jerga matemática y al ser atacados sobre el primer aspecto ponen énfasis en el segundo. Pero hay un amplio consenso sobre el escaso valor de sus matemáticas y sólo unos pocos piensan que este podría ser reivindicado por la interpretación física que hacen de las mismas. Aunque, como hemos visto, los círculos viciosos no son siempre malos, este no parece ser un buen ejemplo de ello…

En algunos campos de la física hay una fuerte tradición de trabajo especulativo, y es bueno que sea así porque muchas grandes ideas (la teoría de la relatividad, sin ir más lejos) surgieron de esta manera. Pero no toda especulación es razonable y parece que lo menos que cabe exigirle es que los fundamentos matemáticos sean sólidos, cosa que no ocurre en este caso. Además, algunas de las declaraciones anteriormente mencionadas sugieren que, de proliferar las investigaciones de este tipo, hay áreas de la física teórica que corren el riesgo de convertirse en cadenas especulativas.[66]

[62] Hay razones para que los referees no confíen demasiado en la buena voluntad de los autores. Una es que dicha buena voluntad podría estar ausente, como ocurrió en el caso de plagio masivo de artículos de física por autores de Universidades turcas descubierto en agosto de 2007 [1]. Otra razón es que, aunque sea real, la buena voluntad por sí sola no basta para hacer ciencia. Como dice el refrán, el infierno está empedrado de buenas intenciones…

[63] Las analogías artísticas y literarias de los comentarios anteriores van, ciertamente, más allá del ficcionalismo y apuntan a la dificultad de criticar el desarrollo de un relato fantástico con argumentos racionalistas. Ciertamente así sería en la metafísica de Tlön: *"Los metafísicos de Tlön no buscan la verdad ni siquiera la verosimilitud: buscan el asombro. Juzgan que la metafísica es una rama de la literatura fantástica"* [18]. Pero no parece deseable que la literatura fantástica entre a forme parte de la ciencia, pues sería de temer que el resultado no tuviera gran calidad ni científica ni literaria.

[64] Entre los artículos de los Bogdanoff, sólo uno está en una revista de matemáticas: *Chinese Annals of Mathematics*. En [34] y [12] los Bogdanoff —o alguno de sus heterónimos— se olvidan (?) en alguna ocasión de la palabra *Chinese* y se refieren a su artículo en *Annals of Mathematics*. Una pequeña diferencia…

[65] Entre los críticos con el trabajo de los Bogdanov que ellos han descalificado por no conocer los grupos cuánticos suficientemente, figura Alain Connes, medallista Fields e iniciador de la *geometría no conmutativa*.

[66] A este respecto, son oportunas las palabras de Mac Lane en [97]: *"La conjetura ha sido desde hace tiempo aceptada y honrada en matemáticas [...] Pero el siguiente paso tiene que ser la*

Todo esto, unido a otras declaraciones que apuntan a que lo que ha ocurrido era inevitable e incluso normal, revela la existencia de un problema latente que va más allá del caso Bogdanoff. De todas formas, es posible sacar una consecuencia positiva de todo el asunto: finalmente, el concepto social de demostración al que se refería Manin ha funcionado y las "demostraciones" de los Bogdanoff no han sido aceptadas por la comunidad científica.

La especulación también tiene cabida en matemáticas[67] donde la formulación de conjeturas es una parte muy importante del proceso de descubrimiento, pero no hasta el punto de dar lugar a la aceptación de resultados sin demostración. No obstante, en tiempos recientes han surgido voces favorables a la aceptación como nuevos axiomas, basándose en una justificación pragmática, de hipótesis matemáticas que no han sido demostradas y, en concreto, de la *Hipótesis de Riemann* (HR). La propuesta de G.J. Chaitin en [21] es precisamente esta: puesto que existe una evidencia computacional considerable en favor de HR, lo suficientemente persuasiva para que un físico la considerase experimentalmente verificada,[68] y puesto que HR tiene consecuencias muy importantes para la teoría de los números primos, debe ser aceptada como un nuevo axioma.[69] Como justificación adicional para hacerlo aduce la posibilidad de que HR pudiera ser indecidible, en cuyo caso no tendría sentido esperar a que surja una demostración de este hecho pues, si es así, entonces HR debería ser "verdadera" ya que, en otro caso, sería posible encontrar un cero no trivial de la función ζ fuera de la recta crítica. Chaitin termina su nota con las palabras siguientes: *"la verdad puede ser alcanzada a través de aproximaciones sucesivas; la insistencia en el rigor instantáneo absoluto es estéril —esto es lo que he aprendido de la incompletitud"*.

Hay que tener en cuenta que la propuesta de Chaitin es muy diferente de las de los que buscan añadir axiomas a ZFC para decidir la hipótesis del continuo. En este último caso, ya sabemos que CH y $\neg$CH son independientes de ZFC y, aun así, nadie

---

demostración y no más especulación".

[67]Un matemático contemporáneo que ha empleado métodos altamente especulativos y poco rigurosos es René Thom (un medallista Fields), a quien su profunda intuición llevó a obtener resultados muy importantes en topología diferencial y en la teoría de singularidades, muchos de los cuales fueron después demostrados rigurosamente por otros matemáticos. En [59] se menciona una curiosa anécdota que ocurrió cuando, en su seminario del IHES, Thom enunció un teorema y Adrien Douady —quien también llegaría a ser un matemático de primera línea— le preguntó si lo había demostrado. Thom contestó: *"No, pero me jugaría la cabeza a que es cierto"*, lo que hizo que Douady murmurase: *"Con todas las cabezas de Thom que se han cortado ya [...]"*. La brillantez especulativa de Thom no parece un argumento convincente en favor de la aceptación en matemáticas de la especulación sin demostración (más allá de la necesaria y habitual en la formulación de conjeturas). Si se hiciese así, parece probable que habría muchas más especulaciones "tipo Bogdanoff" que "tipo Thom" y, además, incluso la "cabeza de Thom", puede no ser suficiente para convencer a un matemático. Como dice MacLane en [97], *"En términos teológicos, no somos salvados por la fe sola, sino por la fe y las obras"*.

[68]Aunque se han computado miles de millones de ceros no triviales de la función ζ y todos han resultado estar en la recta crítica, de acuerdo con lo predicho por HR, el valor de estos cálculos como evidencia en favor de HR es relativo, pues incluso ese número de ceros es pequeño en comparación con el infinito; más importante parece ser la evidencia proporcionada por la relación de HR con numerosos conceptos y resultados de la teoría de números y, en particular, con la teoría análoga en el contexto de variedades algebraicas sobre cuerpos finitos, que culminó con la demostración de Deligne de la *Hipótesis de Riemann para funciones zeta de variedades sobre cuerpos finitos* [17].

[69]Chaitin también argumenta, por razones similares, en favor de la aceptación de que $P \neq NP$.

propone aceptar ¬CH como un nuevo axioma, sino más bien utilizar otros axiomas que presumiblemente deberían servir también para resolver otras cuestiones importantes. El problema de agregar axiomas a ZFC también ha sido considerado desde el punto de vista de que, a fin de cuentas, dichos axiomas se añadirían asimismo a todas las matemáticas (en la medida en que estas se basan en la teoría de conjuntos) y podrían eventualmente servir para decidir cuestiones que no son puramente conjuntistas. Por ejemplo, Gödel creía que serían necesarios nuevos y más fuertes axiomas conjuntistas para decidir no solo cuestiones como CH sino también problemas aritméticos de los que se pueden escribir en la forma más simple, la *puramente universal*, que él llamaba *problemas tipo Goldbach* [38]. Si alguno de los problemas aritméticos importantes que permanecen abiertos resultara ser indecidible en ZFC, este hecho proporcionaría un gran aliciente para la búsqueda de nuevos axiomas. Es cierto que ya se conocen enunciados aritméticos indecidibles, como el que construyó Gödel cuando demostró el primer teorema de incompletitud, pero aunque este enunciado tiene un interés metamatemático grande, su interés propiamente aritmético se puede decir que es nulo, y nunca habría surgido en el contexto de la teoría de números. Por eso se han hecho esfuerzos por construir enunciados matemáticamente interesantes, en el campo de la combinatoria finita, que sean independientes de la aritmética de Peano o, incluso, de ZFC. El primer ejemplo de este tipo fue construido por J. Paris y L. Harrington [93] y, posteriormente, H. Friedman ha continuado produciendo enunciados de combinatoria finita (relacionados con la teoría de Ramsey) cuya resolución requiere la existencia de cardinales grandes (véase, por ejemplo, [48]). Sin embargo, la demostración de estos enunciados es metamatemática, pues se basa en probar que son equivalentes a la 1-consistencia (una forma fuerte de consistencia) de una extensión de ZFC mediante cardinales grandes y, por eso, a pesar de la indudable importancia de los resultados de Friedman, que conectan dos ámbitos tan alejados en apariencia como son la combinatoria finita y los cardinales grandes, Feferman no los acepta como una justificación para postular la existencia de dichos cardinales [38].[70] Por otra parte, no hay ninguna evidencia que apoye la hipótesis de que alguno de los problemas aritméticos *formulados previamente* a estas construcciones vaya a resultar indecidible, y tampoco parece haberla en el caso de HR. El hecho de que la solución de un problema tarde en encontrarse no cuenta como evidencia de este tipo, pues basta pensar, por ejemplo, en lo que se tardó en encontrar

[70]La cuestión de si las matemáticas necesitan nuevos axiomas ha sido objeto de discusión, además de en [40], en la lista FOM (Foundations of Mathematics) [42], a partir de mayo de 2000. Por una parte, J. Steel defiende la necesidad de que las matemáticas adopten nuevos axiomas —en concreto, axiomas de cardinales grandes— puesto que estos son necesarios para la teoría de conjuntos. Por otra, H. Friedman y S.G. Simpson, proponentes de la llamada *matemática inversa* (“reverse mathematics”), sostienen que este argumento no es suficiente, pues la teoría de conjuntos está demasiado alejada de los problemas concretos y computacionales que forman el núcleo de las matemáticas. La matemática inversa [104], así llamada porque, partiendo de teoremas matemáticos concretos va “marcha atrás” buscando los axiomas necesarios para demostrarlos, pretende establecer conexiones más estrechas entre la teoría de conjuntos (y los sistemas formales) y las partes centrales de las matemáticas. Esta idea guía también los esfuerzos de Friedman para establecer conexiones entre los axiomas de cardinales grandes y la combinatoria finita.

la demostración del teorema de Fermat.[71] Además, lo que se busca al resolver HR es *comprender* algo muy básico, la relación entre la adición y la multiplicación.[72] Y ¿qué añadiría a nuestra comprensión el aceptar, sin más, a HR como verdadera?

A pesar de todo, hay que reconocer que aceptar HR sería muy diferente a aceptar las especulaciones tipo Bogdanoff, pues aquí el significado de lo que estaríamos aceptando estaría perfectamente claro (además de tener apoyo heurístico y experimental). Aun así, la comunidad matemática en general es completamente reacia a hacerlo. No sólo no hay evidencia convincente de que HR sea indemostrable sino que hay que admitir la posibilidad —aunque tendría consecuencias desagradables— de que pudiera resultar falsa (así lo creía Littlewood antes de su muerte). Esto no impide estudiar las consecuencias de HR y, de hecho, se han demostrado muchos resultados interesantes que dependen de su verificación —siendo este un argumento importante en favor de la misma— pero, teniendo en cuenta la tradición matemática, no parece muy necesario cambiar artificialmente su estatus. Es posible que de esta forma se desanimaran los esfuerzos para obtener una demostración y el no buscarla supondría —en el mejor de los casos, es decir, suponiendo que HR no sea falsa— una doble renuncia, en la medida de que la demostración juega no sólo el papel de verificación sino también el de explicación. Al renunciar a la verificación estaríamos renunciando al rigor inherente a las demostraciones matemáticas, y al renunciar a la explicación renunciaríamos a la posibilidad de obtener una mejor comprensión de algunos conceptos aritméticos básicos y todo ello, aparentemente, a cambio de nada.

Epílogo

A lo largo de las secciones anteriores hemos visto que hay razones para pensar que nuestra comprensión de los conjuntos no es tan perfecta como sugiere su sencillez estructural, y que la posibilidad de reducir las matemáticas a la teoría de conjuntos es también bastante discutible y, en todo caso, dista mucho de ser realizable en la práctica. La primera cuestión tiene como consecuencia que la teoría de conjuntos se haya desarrollado como una disciplina matemática con sus propios problemas —algunos muy difíciles— y esto afecta también a la segunda, pues el interés de los conjuntos no se circunscribe ya a los problemas fundacionales. Ambas cuestiones plantean problemas filosóficos interesantes que, salvo en algunos casos extremos, no parecen tener apenas influencia en el desarrollo de la práctica matemática. A pesar de todo, los conjuntos proporcionan un lenguaje que es, a la vez, muy económico y muy potente y esto los hace idóneos para modelar satisfactoriamente gran cantidad de fenómenos en matemáticas y también en informática (aunque ello no suponga que

[71] Y en la potencia de los métodos que hubo que desarrollar para ello, que van mucho más allá de lo que se podría pensar a partir del enunciado del teorema.

[72] En palabras de B. Conrey, citado en [100]: *"La Hipótesis de Riemann es la conexión más básica que existe entre la adición y la multiplicación, así que yo pienso en ella en los términos más sencillos como algo realmente básico que no comprendemos sobre la relación entre adición y multiplicación".* También A. Connes, citado asimismo en [100]: *"... es probablemente el problema más básico en matemáticas, en el sentido de que entrelaza la adición y la multiplicación. Es un profundo agujero en nuestra comprensión".*

esta tenga que ser la única —y, en ocasiones, ni siquiera la mejor— forma de hacerlo). Por todo ello se puede decir que, con independencia de los problemas fundacionales, la teoría de conjuntos sigue siendo una parte muy importante de las matemáticas.

Referencias

[1] 2007 Plagiarism Ring Affair, en `http://www.eurekajournalwatch.org/index.php/2007_Plagiarism_Ring_Affair`.

[2] P. Aczel, *Non-Well-Founded Sets*, CSLI Lecture Notes, Vol. 14, CLSI Publications, Stanford, 1988.

[3] J. Baez, `http://math.ucr.edu/home/baez/bogdanoff/`.

[4] J. Bagaria, Natural axioms of set theory and the continuum problem, en `http://www.crm.cat/Publications/04/pr591.pdf`.

[5] M. Balaguer, *Platonism and anti-Platonism in mathematics*, Oxford Univ. Press, 1998.

[6] M. Barr, Terminal coalgebras in well-founded set theory, *Theoretical Computer Science* **114** (1993), 299–315.

[7] J. Barwise y L. Moss, Hypersets, *Math. Intelligencer* **13** (1991), no. 4, 31–41.

[8] J. Barwise y L. Moss, *Vicious Circles. On the Mathematics of Non-Wellfounded Phenomena*, CSLI Lecture Notes 60, CLSI Publications, Stanford, 1996.

[9] P. Benacerraf, What numbers could not be, en [10], 272–295.

[10] P. Benacerraf y H. Putnam (Eds.), *Philosophy of Mathematics*, 2nd ed., Cambridge Univ. Press, 1983.

[11] J. Berstein y S. Gelbart (Eds.), *Introduction to the Langlands program*, Birkhäuser, 2003.

[12] F. Besnard, `http://perso.orange.fr/fabien.besnard/bogdanoff.htm`.

[13] A. Blass y Yu. Gurevich, Why Sets?, *Bulletin of the European Association for Theoretical Computer Science* **84** (2004), 139–156.

[14] A. Blass, Yu. Gurevich y S. Shelah, Choiceless polynomial time, *Ann. Pure Appl. Logic* **100** (1999), 141–187.

[15] A. Blass, Yu. Gurevich y J. Van den Bussche, Abstract state machines and computationally complete query languages, *Information and Computation* **174** (2002), 20–36.

[16] Bogdanov Affair – Wikipedia, `http://en.wikipedia.org/wiki/Bogdanov_Affair`.

[17] E. Bombieri, Problems of the Millennium: the Riemann Hypothesis, en `http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf`

[18] J.L. Borges, Tlön, Uqbar, Orbis Tertius, en *Ficciones*, Alianza Editorial, 1971.

[19] J.R. BROWN, *Philosophy of mathematics: an introduction to the world of proof and pictures*, Routledge, 1999.

[20] The CALCULEMUS project, en `http://www.calculemus.net`.

[21] G.J. CHAITIN, Thoughts on the Riemann Hypothesis, *Math. Intelligencer* **26** (2004), no. 1, 4–7.

[22] P.J. COHEN, *Set theory and the continuum hypothesis*, Benjamin, 1966.

[23] D. CORFIELD, *Towards a philosophy of real mathematics*, Cambridge Univ. Press, 2003.

[24] H.G. DALES, The mathematician as a formalist, en [25], 181–200.

[25] H.G. DALES Y G. OLIVERI (EDS.), *Truth in Mathematics*, Clarendon Press, 1998.

[26] D. VAN DANTZIG, Is $10^{10^{10}}$ a finite number?, *Dialectica* **9** (1955–56), 272–277.

[27] P.J. DAVIS Y R. HERSH, *The Mathematical Experience*, Birkhäuser, 1981.

[28] P. DEHORNOY, Au-delà du forcing: la notion de vérité essentielle en théorie des ensembles, en `http://www.math.unicaen.fr/~dehornoy/surveys.html`.

[29] P. DEHORNOY, Progres récents sur l'hypothèse du continu (d'après Woodin), Seminaire Bourbaki, exposé 915, mars 2003, en `http://www.math.unicaen.fr/~dehornoy/surveys.html`.

[30] O. DEISER, *Orte, Listen, Aggregate*, Habilitationsschrift, Freie Universität Berlin, 2006.

[31] K. DEVLIN, *The Joy of Sets*, Springer-Verlag, 1993.

[32] K. DEVLIN, `http://www.maa.org/devlin/devlin_6_01.html`.

[33] E.W. DIJKSTRA, Real mathematicians don't prove, en `http://www.cs.utexas.edu/users/EWD/ewd10xx/EWD1012.pdf`.

[34] J. DISTLER, `http://golem.ph.utexas.edu/~distler/blog/archives/000375.html`.

[35] H.D. EBBINGHAUS, Is there a logic for polynomial time?, *Logic Journal of the IGPL* **7** (1999), 359–374.

[36] P.C. EKLOF Y A.H. MEKLER, *Almost free modules. Set theoretic methods*, revised edition, North-Holland, 2002.

[37] Experimental Mathematics Website, `http://www.experimentalmath.info`.

[38] S. FEFERMAN, Does mathematics need new axioms?, *Amer. Math. Monthly* **106** (1999), 99–111.

[39] S. FEFERMAN, Predicativity, en *The Oxford Handbook of the Philosophy of Mathematics and Logic* (S. Shapiro, Ed.), Oxford Univ. Press, 2005.

[40] S. FEFERMAN, H.M. FRIEDMAN, P. MADDY Y J. STEEL, Does mathematics need new axioms? (Proceedings of a symposium), *Bulletin of Symbolic Logic* **6** (2000), 401–446.

[41] J. FERREIRÓS, *Labyrinth of Thought: A history of set theory and its role in modern mathematics*, Birkhäuser, 1999.

[42] FOM archives, en `http://www.cs.nyu.edu/pipermail/fom/`.

[43] M. Foreman, Generic Large Cardinals: New Axioms for Mathematics?, *Documenta Math.*, Proceedings of the International Congress of Mathematics, Vol. II, (Berlin, 1998), pp. 11–21.

[44] M. Forti y F. Honsell, Set theory with free construction principles, *Ann. Scuola Normale Superiore di Pisa* **10** (1983), 493–522.

[45] A. Fraenkel, Y. Bar-Hillel y A. Levy, *Foundations of set theory*, 2nd ed., North-Holland, 1973.

[46] C. Freiling, Axioms of symmetry: Throwing darts at the real line, *J. Symbolic Logic* **51** (1986), 190–200.

[47] E. Frenkel, Recent advances in the Langlands program, *Bull. Amer. Math. Soc.* **41** (2004), 151–184.

[48] H. Friedman, Finite functions and the necessary use of large cardinals, *Ann. of Math.* **148** (1998), 803–893.

[49] K. Gödel, *The Consistency of the Continuum-Hypothesis*, Princeton University Press, 1940.

[50] K. Gödel, On Formally Undecidable Propositions of Principia Mathematica and Related Systems, en *From Frege to Gödel* (J. van Heijenoort, Ed.), Harvard University Press, 1967.

[51] K. Gödel, What is Cantor's Continuum Problem?, en [10], 470–485.

[52] J.A. Goguen, A categorical manifesto, *Math. Struct. Comp. Sci.* **1** (1991), 49–67.

[53] T. Gowers, What is the difference between naive and abstract set theory?, en `http://www.dpmms.cam.ac.uk/~wtg10/settheory.html`.

[54] Yu. Gurevich, Platonism, Constructivism, and Computer Proofs vs. Proofs by Hand, *Bulletin of the European Association for Theoretical Computer Science* **57** (1995), 145–166.

[55] K. Hrbacek y T. Jech, *Introduction to set theory*, 3rd ed., Marcel Dekker, 1999.

[56] N. Immerman, *Descriptive Complexity*, Springer-Verlag, 1998.

[57] C. Ivorra Castillo, *Lógica y teoría de conjuntos*, en `http://www.uv.es/~ivorra/Libros/Logica.pdf`.

[58] C. Ivorra Castillo, *Pruebas de consistencia*, en `http://www.uv.es/~ivorra/Libros/CONJUNTOS.pdf`.

[59] A. Jackson, The IHES at forty, *Notices of the American Math. Soc.* **46** (1999), 329–337.

[60] B. Jacobs y J. Rutten, A tutorial on (Co)Algebras and (Co)Induction, *Bulletin of the European Association for Theoretical Computer Science* **62** (1997), 222–259.

[61] R. Jensen, The fine structure of the constructible hierarchy, *Ann. Math. Logic* **4** (1972), 229–308.

[62] V.F.R. Jones, A credo of sorts, en [25], 203–214.

[63] S. Kahrs, A formalist's perspective of mathematics, en `http://www.cs.ukc.ac.uk/people/staff/smk/manifesto.ps`.

[64] A. Kanamori, *The higher infinite: large cardinals in set theory from their beginnings*, 2nd ed., Springer-Verlag, 2003.

[65] S.A. Kripke, Outline of a theory of truth, *Journal of Philosophy* **72** (1975), 53–81.

[66] K. Kunen, *Set theory. An introduction to independence proofs*, North-Holland, 1980.

[67] I. Lakatos, *Pruebas y refutaciones*, Alianza Editorial, 1978.

[68] C.W.H. Lam, The search for a finite projective plane of order 10, *American Mathematical Monthly* **98** (1991), 305–318.

[69] F.W. Lawvere, Variable quantities and variable structures in topoi, en *Algebra, Topology, and Category Theory* (A. Heller, M. Tierney, Eds.), Academic Press, 1976, pp. 101–131.

[70] F.W. Lawvere y R. Rosebrugh, *Sets for mathematics*, Cambridge University Press, 2003.

[71] P. Maddy, Believing the Axioms. I, II. *J. Symbolic Logic* **53** (1988), 481–511; 736–764.

[72] P. Maddy, *Realism in mathematics*, Oxford Univ. Press, 1993.

[73] P. Maddy, *Naturalism in mathematics*, Oxford Univ. Press, 1997.

[74] P. Maddy, How to be a naturalist about mathematics, en [25], 161–180.

[75] E.G. Manes y M.A. Arbib, *Algebraic approaches to program semantics*, Springer-Verlag, 1986.

[76] Yu. I. Manin, *A Course in Mathematical Logic*, Springer-Verlag, 1977.

[77] Yu. I. Manin, Contribución a la discusión en *The theory and practice of proof, 1*, Proc. of the 7th International Congress on Mathematical Education, Montreal, 1992.

[78] Yu. I. Manin, Georg Cantor and his heritage, `arXiv:math/0209244` (2002).

[79] Yu. I. Manin, The notion of dimension in geometry and algebra, *Bull. Amer. Math. Soc.* **43** (2006), 139–161.

[80] Yu. I. Manin, Mathematical knowledge: internal, social and cultural aspects, `arXiv:math/0703427v1` (2007).

[81] A.R.D. Mathias, A term of length 4,523,659,424,929, *Synthese* **133** (2002), 75–86.

[82] J.P. Mayberry, *The foundations of mathematics in the theory of sets*, Cambridge University Press, Cambridge, 2000.

[83] W. McCune, Solution of the Robbins Problem, *J. Automated Reasoning* **19**(3) (1997), 263–276.

[84] J.D. Monk, *Mathematical Logic*, Springer-Verlag, 1976.

[85] Y.N. Moschovakis, *Notes on Set Theory*, Springer-Verlag, New York, 1994.

[86] L. Moss, Parametric Corecursion, *Theoretical Computer Science* **260** (2001), 139–163.

[87] D. Mumford, The dawning of the age of stochasticity, en *Mathematics: Frontiers and Perspectives* (V. Arnold, M. Atiyah, P. Lax y B. Mazur, Eds.), American Mathematical Society, 2000.

[88] E. Nelson, *Predicative arithmetic*, Mathematical Notes 32, Princeton University Press, 1986.

[89] E. Nelson, Confessions of an apostate mathematician, en `http://www.math.princeton.edu/~nelson/papers.html`.

[90] M. Ojeda Aciego, Lógica, matemática, deducción automática, *La Gaceta de la RSME* **8** (2005), 93–119.

[91] D. Overbye (artículo en *New York Times*), en `http://query.nytimes.com/gst/fullpage.html?res=9401E4DB1431F93AA35752C1A9649C8B63&sec=&spon=&pagewanted=all`.

[92] R.J. Parikh, Existence and feasibility in arithmetic, *J. Symbolic Logic* **36** (1971), 494–508.

[93] J. Paris y L. Harrington, A mathematical incompleteness in Peano arithmetic, en *Handbook for mathematical logic* (J. Barwise, Ed.), Studies in Logic and the Foundations of Mathematics, North-Holland (1977), pp. 1133–1142.

[94] H. Putnam, Mathematics without foundations, *Journal of Philosophy* **64** (1967), 5–22.

[95] W.V. Quine, The ways of paradox, en *The ways of paradox and other essays*, 2nd ed., Harvard University Press, 1976.

[96] Y. Rav, Why do we prove theorems?, *Philosophia Mathematica* **7** (1999), 5–41.

[97] Responses to "Theoretical mathematics: Toward a cultural sysnthesis of mathematics and theoretical physics", por A. Jaffe y F. Quinn, *Bull. Amer. Math. Soc.* **30** (1994), 178–207.

[98] J. Roitman, *Introduction to modern set theory*, Wiley, 1990.

[99] B. Russell y A.N. Whitehead, *Principia Mathematica (hasta *56)*, Paraninfo, 1981.

[100] K. Sabbagh, *Dr. Riemann's Zeros*, Atlantic Books, 2003.

[101] S. Shelah, Infinite abelian groups, Whitehead problem and some constructions, *Israel J. Math.* **18** (1974), 243–256.

[102] S. Shelah, The future of set theory, en *Set Theory and the Reals*, 1–12, Israel Math. Conf. Proc. 6, Bar-Ilan Univ., Ramat Gan, 1993, e-print en `arXiv:math.LO/0211397`.

[103] S. Shelah, The generalized continuum hypothesis revisited, SH460, en `http://shelah.logic.at/`.

[104] S.G. Simpson, *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1999.

[105] R. Solovay, A model of set theory in which every set of reals is Lebesgue measurable, *Ann. of Math.* **92** (1970), 1–56.

[106] R. Taylor, Galois representations, *Ann. Fac. Sci. Toulouse* **13** (2004), 73–119.

[107] T. TYMOCZKO, *New directions in the philosophy of mathematics*, Birkhäuser, 1986.

[108] H. WANG, The concept of set, en [10], 530–570.

[109] P. WOIT, `http://www.math.columbia.edu/~woit/blog/archives/000034.html`.

[110] P. WOIT, *Not Even Wrong: The Failure of String Theory And the Search for Unity in Physical Law*, Basic Books, 2006.

[111] W.H. WOODIN, The Continuum Hypothesis. Parts I and II, *Notices of the Amer. Math. Soc.* **48** (2001), 567–576; 681–690.

[112] The Z Notation, en `http://vl.zuser.org/`.

JOSÉ LUIS GÓMEZ PARDO, DEPARTAMENTO DE ÁLXEBRA, UNIVERSIDADE DE SANTIAGO DE COMPOSTELA, 15782 SANTIAGO DE COMPOSTELA
Correo electrónico: `pardo@usc.es`