EPISTEMOLOGÍA E HISTORIA DE LA CIENCIA

SELECCIÓN DE TRABAJOS DE LAS VIII JORNADAS

VOLUMEN 4 (1998), Nº 4

Horacio Faas
Luis Salvatico
Editores

ÁREA LOGICO-EPISTEMOLÓGICA DE LA ESCUELA DE FILOSOFÍA
CENTRO DE INVESTIGACIONES DE LA FACULTAD DE FILOSOFÍA Y HUMANIDADES
UNIVERSIDAD NACIONAL DE CÓRDOBA

Cómo demostrar en matemáticas

*Horacio Faas**

En su libro sobre la teoría de conjuntos y la hipótesis del continuo, Paul J. Cohen (COHEN 1966, p.2) se refiere a Brouwer en las siguientes palabras : "... la escuela de Brouwer (Intuicionismo) sólo admitiría conjuntos finitos como objetos legítimos de estudio, y aún un número entero solo no se consideraría definido a menos que se diese una regla absolutamente determinada para computarlo (Por ejemplo, el conjunto cuyo elemento es 5 si el último Teorema de Fermat es verdadero y 7 si es falso, no está bien definido de acuerdo con Brouwer)". No habría estado bien definido porque no se podía afirmar que el teorema de Fermat fuese verdadero ni que fuese falso. Lo de Brouwer tiene muchos años, aunque, como se sabe, es de nuestro siglo, pero lo de Cohen es de 1966. Veintinueve años más tarde, el enunciado de Brouwer ha cambiado de sentido.

Ese problema renuente se había constituido en un paradigma de lo que aparecía como no demostrado pero que podía eventualmente serlo. Matemáticos de los más eminentes aportaron a veces pequeñas contribuciones, se equivocaron otras, y en otros casos, como se dice de Hilbert, no se mostraron interesados porque quizás "lo más probable es que se fracase en el intento"(SINGH, 1997, p.227). Precisamente Hilbert, al decir de Chaitín[1], culminó dos mil años de tradición matemática que se remontan al tratamiento axiomático de la geometría por Euclides y pasan por el sueño de Leibniz de una lógica simbólica y por los monumentales *Principia Mathematica* de Russell y Whitehead. El programa de Hilbert pretendía formular un sistema axiomático formal que comprendiera toda la matemática. Tal sistema debía ser consistente y completo, es decir, completo en el sentido de que cualquier fórmula construida de acuerdo con las reglas sintácticas de formación de fórmulas, o su opuesta por la negación, debía ser demostrable en el sistema. De lográrselo, todo problema matemático tendría respuesta, afirmativa o negativa; todo enunciado matemático verdadero sería demostrable y todo falso, refutable. A esta situación para un sistema se le asignó el nombre de decidible, y su tratamiento constituyó el *problema de la decisión*. Habría sido el paraíso algorítmico, si uno asocia la noción de algoritmo a la de producible en un sistema formal, y ésta a la de computable mecánicamente. Si un sistema es consistente y completo (en el sentido apuntado), entonces es decidible, ya que dado un

* Universidad Nacional de Córdoba

[1] Cf. CHAITIN, 1992, p.1

enunciado A, sólo pueden pertenecer al sistema él o su negación, pero no ambos, por la condición de consistencia; pero ya que es completo, *debe* pertenecer al menos uno de ellos, y lo que pertenece al sistema formal ha sido generado a partir de los axiomas mediante una demostración, de modo que para cualquier enunciado A, es demostrable A, o es demostrable **no** A. En zonas elementales, como la de la lógica proposicional o la de la lógica cuantificacional uniforme, se da esa situación para una adecuada axiomatización. Hilbert soñó que algo parecido podría darse para toda la matemática.

Tal paraíso era pura fantasía, el duro golpe realístico del teorema de incompletitud de Gödel lo puso en jaque: si la aritmética era consistente, entonces era incompleta, y había enunciados verdaderos de la aritmética que no eran demostrables. Pocos años después, los trabajos de Turing y Church mostraron que desde la lógica elemental en adelante, los sistemas no eran decidibles.

Hay, entonces, enunciados matemáticos para los cuales no existe demostración formal, y que sin embargo son verdaderos, y una de las genialidades de Gödel consistió en haber construido uno de ellos y haber proporcionado la manera de encontrar nuevos. Pero esos enunciados, del tipo del que dice de sí mismo que es indemostrable, parecen pertenecer a un metalenguaje, y los matemáticos no se preocuparon mucho cuando Gödel los descubrió. Total, en el quehacer cotidiano de la matemática, no aparecían.

La famosa conferencia de Hilbert de 1900 había indicado veintitrés problemas no resueltos aún en toda la historia de la matemática, de los cuales uno era el Último Teorema de Fermat. Esos problemas eran genuinamente matemáticos, y el hallazgo de Gödel seguramente no los afectaría.

La hipótesis del continuo era otro de los veintitrés, y aquí también Gödel aportó su contribución: demostró que dicha hipótesis era consistente con la teoría restringida de conjuntos (la teoría de conjuntos sin el axioma de elección). Podía, entonces, llegar a demostrarse. Para gran sorpresa de muchos, en 1963 Paul J. Cohen demostró que la negación de la hipótesis era también consistente con la teoría restringida de conjuntos. No se podía demostrar ni ella ni su negación. Para la teoría restringida de conjuntos, era un enunciado indecidible. Ya que el enunciado original de Gödel puede considerarse como perteneciente a la matemática informal, como luego señaló Lakatos, ahora había aparecido, por así decirlo, el primer enunciado indecidible realmente importante. ¿Sería el teorema de Fermat otro indecidible? Los matemáticos han estado intrigados u ocupados con él por más de trescientos años, pero hasta hace poco muchos de ellos le atribuían la inmortalidad; no confiaban en que fuera alguna vez demostrado o refutado. Era bastante curioso que un problema de planteo tan simple mostrase tan grandes complicaciones a la hora de intentar su demostración. De hecho, la demostración de Wiles de 1995 agrupa áreas de la matemática muy recientes y difíciles y que

parecían absolutamente dispares. Se comenta que no hay más de una docena de personas en el mundo capaces de entender y controlar el desarrollo completo.

El origen del teorema de Fermat se remonta a la matemática de la Grecia antigua, dos mil años antes de que Fermat lo planteara tal como lo conocemos hoy, y encadena a los pitagóricos con las más sofisticadas ideas de la matemática actual. Cuando el exponente es dos, se trata de las ternas pitagóricas, expresiones del ultrafamoso Teorema de Pitágoras, y las soluciones son infinitas. Parece que alrededor de 1637 Fermat planteó la cuestión para exponente mayor que dos, y allí propuso su tesis de que no había soluciones para ningún caso. Recién en 1670 apareció a la luz pública, con la edición de la traducción de Bachet de la *Aritmética de Diofanto (con observaciones de P. de Fermat)*. Como se sabe, Fermat había trabajado sobre ese libro y había ido haciendo anotaciones en los márgenes, muchas de las cuales eran nuevos teoremas cuya demostración omitía reiteradamente. Matemáticos posteriores fueron encontrando esas demostraciones, salvo la de uno de ellos -por eso la denominación de *Último*- y de la cual Fermat anotó que no la incluía porque no cabía en el margen. Pero esbozó una demostración para el caso en que el exponente es cuatro: si había soluciones, debían existir otras soluciones menores, y así sucesivamente, de modo tal que como la serie de los enteros positivos en su ordenamiento natural tiene un comienzo, se produce un absurdo que hace imposible dicha existencia. Esta estrategia se conoce como *método de descenso infinito* y fue utilizado un siglo más tarde por Euler para demostrar el teorema con exponente tres, aunque debió apelar al concepto de número imaginario, todavía un poco raro para la época. Pero no tuvo éxito para los infinitos casos restantes. Courant y Robbins, en su conocido *¿Qué es la matemática?*, cuya primera edición es de 1941, dicen que hasta entonces se habían logrado demostraciones para muchos exponentes, en particular para todos los menores que 619. Con el auxilio de computadoras, en los '80 se lo demostró para exponentes próximos a 25000, y más recientemente se había llegado ya a cerca de los 4.000.000. Pero claro, si los casos son infinitos, cualquier número finito es insignificante.

En esta demostración final, han jugado un papel importante las curvas elípticas (cuya expresión algebraica es $y^2=x^3+ax^2+bx+c$), objeto matemático de muy difícil tratamiento al cual se les ha acercado con aritméticas de dominio cíclico bautizadas *series-E*. En áreas matemáticas totalmente alejadas, se habían estudiado objetos que ofrecían alguna forma de simetría modular -del tipo de los espacios planos que se cubren totalmente con figuras (piénsese en los ejemplos de Penrose o las representaciones pictóricas de Escher), y que habían podido clasificarse según los tipos de elementos intervinientes y su cantidad, lo cual generaba lo llamadas *series-M*. En1955, Taniyama, quien había advertido equivalencias entre elementos de las series-E con otros de las series-M, propuso

que podría haber correspondencia entre cada uno de los de una con cada uno de los de la otra, es decir, a cada forma modular le correspondería una ecuación elíptica y viceversa. Esta propuesta pasó a llamarse posteriormente *Conjetura de Taniyama-Shimura*, con el agregado del nombre de quien también la asumió. Nuevamente aquí, pese a que se encontraban más y más correspondencias, la conjetura permaneció renuente a cualquier demostración. En 1984, Frey elaboró una ecuación elíptica que era una transformación de la ecuación de Fermat, y que pudo vincular a la conjetura de Taniyama con el teorema de Fermat, de tal modo que si la conjetura era verdadera, también lo era el teorema de Fermat.

Lo que Wiles logró es la demostración de la conjetura de Taniyama-Shimura, por inducción matemática, apoyándose en una forma de ordenar inspirada en Galois con adaptación del método de Kolyvagin y Flach. Se había recorrido un largo camino, con reiterada aplicación de lo que en lógica se llama el método de demostración condicional.

Otra famosa conjetura, la de que cuatro colores por lo menos son suficientes para colorear un mapa de cualquier complejidad, fue solucionada por fin en 1976 mediante el uso de computadoras, ya que se había logrado reducir el problema a 1482 casos particulares. El tiempo de computadora necesario fue de 1200 horas. Sin duda, hoy se haría en mucho menos tiempo.

La demostración de la clasificación de grupos simples finitos consta de 500 artículos escritos por más de cien matemáticos. Se dice que un solo matemático, Daniel Gorenstein, entendía la demostración entera, de 15000 páginas. Gorenstein murió en 1992.

De todos modos, tanto en este teorema de las 15000 páginas, como en la demostración de Wiles del de Fermat, se mantiene la tradición del control paso a paso de la demostración. En el de los cuatro colores, en cambio, ese control no se hizo para la gran mayoría de los casos, ni se hará nunca.

¿Ha cambiado la noción de demostración en matemáticas? No podría darse una respuesta categórica. Con respecto a la teoría, continúa habiendo consenso en no aceptar una conjetura hasta que haya una demostración aceptable. Pero aquí radica actualmente el problema. La aceptabilidad de una demostración depende en este momento, cada vez más, de que seamos capaces de confiar en el trabajo de las computadoras

También la práctica cotidiana de los matemáticos ha cambiado en esta parte del siglo. Antes se recurría a lápiz y papel para establecer conjeturas y confirmarlas, o para refutarlas. Por ejemplo, cuando Fermat propuso que todos los números obtenidos elevando 2 a la n-ésima potencia de 2 y agregándole 1, eran primos, había obtenido confirmaciones para $n = 1, 2, 3, 4$, pero Euler calculó el resultado para $n = 6$ y encontró que la conjetura era falsa, y allí terminó el asunto. Esa suerte de "matemática experimental" se deja ahora en manos de las computadoras.

Lo que ocurre actualmente es que los matemáticos acuden cada vez más a esta manera de trabajar, al recurso a la observación de resultados que proveen las computadoras, y de tal forma se acercan al estilo de científicos empíricos como los físicos. Al destacar esta situación, Chaitín[2] no deja de sorprenderse de que esta actitud se haya tomado por razones ajenas a los hallazgos teóricos. Parece que se hubieran ignorado los resultados logrados por Gödel, Turing, Church sobre limitaciones de los sistemas formales, y los más recientes del propio Chaitin, y se hubiera seguido encajonado en el ideal hilbertiano. Digo encajonado para no desmerecer a Hilbert, o a su entusiasta seguidor von Neumann, quienes advirtieron la importancia del Teorema de Gödel de 1931. Me refiero a la forma de trabajo de la gran mayoría de los matemáticos. Chaitin se considera un continuador de Turing por haber descubierto un número cuya incomputabilidad es mucho mayor que la de los incomputables de Turing: el número **Omega**, que define así:

$$0 < \text{Omega} = \mathbf{Sum}_{\text{p se detiene}} 2^{-|p|} < 1$$

y que es igual a la *probabilidad de detención*. Esta noción corresponde a la probabilidad de que uno genere al azar -por ejemplo mediante el resultado de tirar reiteradamente una moneda- un programa de computación (como una cadena de bits) que se detenga (**Sum** es sumatoria, y los términos de la sumatoria son las probabilidades de que cada uno de los programas que se detiene se haya obtenido de la manera aleatoria indicada, de modo que cada programa que se detiene aporta a la suma la inversa de $2^{|p|}$, siendo $|p|$ la longitud de ese programa en bits). Según muestra Chaitin, no hay algoritmo posible que compute ese número, ya que se trata de un número real *normal* en el sentido de Borel, y cuya normalidad se da para cualquier base, no tan sólo para base diez como ocurre con algún número normal conocido. Mediante una adecuada ecuación diofantina, esta situación azarosa puede llevarse a la teoría de números (aunque hace falta aceptar variables en los exponentes).

Chaitin dice que así como existe el azar en física, a pesar de la oposición inicial de eminentes físicos como Einstein, su propio trabajo muestra que también se da ese fenómeno en matemáticas, aún en zonas tan iniciales como teoría elemental de números. Turing había demostrado que hay números incomputables, pues el *problema de la detención* es insoluble; lo que Chaitin propone con su teoría algorítmica de la información es que hay algo así como grados de compatibilidad: su número Omega es mucho menos computable que otros ya que es un número absolutamente incompresible. No hay manera de expresarlo como no sea con las cifras (bits en la presentación binaria) que uno usaría para mostrarlo. Es un número absolutamente azaroso que puede, sin embargo, incluirse en teoría de números mediante la ecuación diofantina con variables en exponentes que antes citamos.

---

[2] Ibídem, p. 16.

En otra línea, la propuesta de Barwise y Etchemendy revisa la posición más aceptada sobre la demostración en lo referente al uso de diagramas. Citan a Tennant como expositor actual de esa posición: ". ..[El diagrama] es sólo una técnica heurística para poner en marcha ciertas formas de inferencia. . . es dispensable como instrumento de demostración, en verdad. . . no tiene un lugar propio como tal en la demostración. Pues la demostración es un objeto sintáctico que consiste solamente de oraciones dispuestas en una secuencia finita e inspeccionable"(BARWISE, 1996, p.3). Y siguen, en la página siguiente: "Es a este dogma que queremos desafiar". Pero ese dogma es la noción clásica de demostración desde Euclides, y sobre todo desde Frege y Hilbert.

El desafío puede producirse por la utilización efectiva de diagramas en una demostración, como pretende Barwise (tarea que efectivamente se cumple en su programa *Hyperproof*[3], o por el no cumplimiento de alguna de las características exigidas por Tennant. En el caso de los cuatro colores, se cuestiona lo de inspeccionable; si bien lo es en principio, no lo es en la práctica, y no se han inspeccionado todos los casos para aceptar la demostración. Lo de Wiles sigue siendo clásico.

No ha sido todo esto lo que ha cambiado el estilo de los matemáticos, sino algo mucho más pedestre: la existencia de las computadoras.

¿Podría la situación descrita abonar los argumentos en pro del holismo en el sentido de Resnik[4] ? Al final del capítulo 7 de Resnik1997, se sostiene que los separatistas deben de afirmar algo más que una simple cuestión de conveniencia metodológica, ya que de otra manera no se distinguirían de los holistas, y que, además, no hay hasta el momento una fundamentación absolutamente incontrovertida de la división entre ciencias formales y empíricas.

Resnik afirma además que las matemáticas buscan también, como las demás ciencias, evidencias empíricas en las que apoyarse, y que las antiguas disciplinas matemáticas son más fácilmente aceptadas que algunas de las nuevas porque han sido corroboradas por siglos de utilización exitosa. Sin embargo, con respecto a la aceptación de una demostración particular, dice:

> "Lo que es especial en matemáticas es que hasta que no sea posible demostrar (o refutar) una conjetura, los matemáticos la consideran como un problema abierto, aún cuando, para las pautas de las ciencias naturales, la evidencia no deductiva que decide el resultado en uno u otro sentido sea superabundante. Si, por ejemplo, décadas de funcionamiento de computadoras hubieran producido nuevos pares de primos gemelos, es improbable los matemáticos consideraran como establecida a la conjetura de los primos gemelos. Por el contrario, los científicos naturales tomarían experimentos similares como decisivos".[5]

---

[3] Cf. BARWISE y ETCHEMENDY, 1994.

[4] Cf. RESNIK, 1997, passim, pero particularmente Cap. 8.

[5] Ibídem, p. 118.

En conclusión, aunque el programa de Hilbert es irrealizable, la noción clásica de demostración que él ha enfatizado se sigue manteniendo y, aunque sea como ideal, la firmeza de una secuencia finita controlable en cada uno de sus pasos no ha cedido.

Referencias

BARWISE 1994: Barwise, Jon, y John Etchemendy, *Hyperproof*, CSLI, Stanford, EE.UU., 1994.

BARWISE 1996. Barwise, Jon, y John Etchemendy, *Visual Information and Valid Reasoning*, en Allwein y Barwise, ed., *Logical Reasoning with Diagrams*, Oxford University Press, New York, 1996

CHAITIN 1992: Chaitin, G. J., *Randomness in Arithmetic and the Decline & Fall of Reductionism in Pure Mathematics*, transcripción de una conferencia del 22-10-92 en la Universidad de New Mexico, EE.UU.

COHEN 1966. Cohen, Paul J., *Set Theory and the Continuum Hypothesis*, W.A. Benjamin Inc, New York, 1966.

RESNIK 1997: Resnik, Michael D: *Mathematics as a Science of Patterns*, Clarendon Press, Oxford, 1997.

SINGH 1997: Singh, Simon, *Fermat's Last Theorem*, Fourth Estate, Londres, 1997.