El último teorema de Fermat-Wiles

*Fabio Abraham Contreras Oré**

Resumen

Este es un artículo de divulgación, que tiene el propósito de elaborar un resumen y comentarios del Libro: *Fermat. El teorema de Fermat. El problema más difícil del mundo*, aparecido en el 2012 del autor Luis Fernando Areán Álvarez. El teorema de Fermat-Wiles está formulado en el marco de la ciencia fundamental y no de la ciencia aplicada, pues, no está interesado en dar solución a un problema práctico, se trata de una propiedad de los números naturales que es de fácil comprensión, sin embargo su demostración duró más de 350 años. En ese andar, se ha tenido que elaborar mucha matemática. Areán Alvarez, recrea ésta historia, pero para su comprensión, el autor del presente artículo, ha añadido explicación de algunos términos utilizados en el referido libro.

Palabras clave

Teorema de Fermat-Wiles.

The Last Fermat-Wiles Theorem

Abstract

This is an article of disclosure, which aims to draw up *Fermat. Fermat's theorem. The most difficult problem in the world*. Appeared in 2012 by Luis Fernando Areán Álvarez.
Fermat-Wiles theorem is formulated within the framework of fundamental science, and it is not applied science because it is not interested in solving a practical problem, it is a property of the natural numbers that is easy to understand; however their demonstration lasted over 350 years. On that way, it has had to make many math's. Areán Alvarez recreates this story, but to understand, the author of this article, added explanation of some terms used in the referred book.

Keywords

Fermat – Wiles' theorem

Recibido: 06 septiembre 2015 | Aprobado: 02 de noviembre de 2015.

* Magister en Didáctica Universitaria. Investigador en la Dirección de Calidad Educativa de la Universidad Continental de Huancayo. Pasó un stage de especialización en Bordeaux-Francia. Fue Especialista en Educación del Instituto Nacional de Investigaciones y Desarrollo de la Educación (INIDE). Fue docente de la Facultad de Educación y de la Sección de Post Grado de la Universidad Nacional del Centro del Perú. Ex Director de la Dirección Regional de Educación. E-mail: conofabi@hotmail.com

¿quién fue Fermat?

Pierre de Fermat nació el 17 de agosto de 1601 en Beaumont de Lomagne – Francia y murió el 12 de enero de 1665, su padre era comerciante y él se graduó de abogado, sin embargo sería considerado más tarde "el príncipe de los aficionados de la matemática", para hacer referencia a su falta de formación profesional en la matemática. En sus tiempos libres se dedicó a resolver problemas de casi todas las áreas de las matemáticas conocidas en su época. Fermat fue el creador de la Geometría Analítica antes que Renato Descartes y también fue el iniciador de la Teoría de Probabilidades e iniciador del Cálculo Diferencial.

Su pasión por la lectura de los trabajos de Diofanto, fundamentalmente por *Aritmética de Diofanto de Alejandría* lo convirtió en un especialista de la *Teoría de los números*, rama cultivada ya por los griegos, que sin embargo fiel a la tradición helena no tiene aplicaciones prácticas y se cultiva simplemente por el placer de conocer las propiedades de los números.

Fermat era alguien a quién le gustaba retar a sus contemporáneos con preguntas y problemas o acertijos que él los resolvía, pero que frecuentemente no los escribía, o los escribía al margen de los libros que leía. No gustaba de publicar su producción. Todo lo que de él se conoce es lo que ha escrito en los márgenes de los libros o la correspondencia que mantenía con otros personajes con quienes compartía y discutía ideas.

Precisamente, en el margen una traducción realizada por Claude Gaspar de Bachet (1581-1638) de la *Aritmética de Diofanto de Alejandría* publicado en 1621; después de la muerte de Pierre de Fermat cuando su hijo Clemente Samuel publicó en 1670 una recopilación de los escritos de su padre con el nombre de *Arithmetica de Diofanto con observaciones de P. de Fermat,* en una de la 48 observaciones originales de Fermat se encontraría una que dice : *"Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquedratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas estdividere",* (Singh, 1999, p. 111) es decir: "Es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados, y en gene-

ral, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente. He encontrado una demostración realmente admirable, pero el margen del libro es muy pequeño para ponerla". Proposición que pasaría a la historia con el nombre del último teorema de Fermat.

Antecedentes

Una interesante cuestión de la teoría de los números se encuentra relacionada con el Teorema de Pitágoras. Los griegos sabían que el triángulo de lados 3; 4 y 5 es un triángulo rectángulo. Fue Pitágoras quién demostró que en todo triángulo rectángulo los lados de dicho triángulo se relacionan mediante la siguiente ecuación: $a^2 + b^2 = c^2$ donde, a y b son las longitudes de los catetos y c es la longitud de la hipotenusa.

Se llaman *ternas pitagóricas* al conjunto de números enteros que cumplen con dicha relación, tal es el caso del triángulo de lados 3; 4 y 5.

Tratando de encontrar todas las ternas pitagóricas posibles, los griegos demostraron que cuando:

$$a = v^2 - u^2 \qquad b = 2uv \qquad c = v^2 + u^2$$

se pueden obtener ternas pitagóricas, habiendo encontrado las ternas pitagóricas primitivas (3;4;5) cuando u = 2 y v = 1; (5;12;13) cuando u = 3 y v = 2; (7; 24; 25) cuando u = 4 y v = 3; ...; (51;140;149) cuando u = 10 y v = 7; etc. Estas ternas se denominan primitivas, porque evidentemente cualquier múltiplo de estas ternas también cumplen con la condición $a^2 + b^2 = c^2$, produciéndose una infinidad de ternas a partir de la terna primitiva. Ejemplo: de (3,4,5) se tiene (6,8,10) ; (9,12,15) ; (12,16,20), etc.

En modo natural surge la pregunta: ¿Es posible encontrar ternas de números enteros que cumplan con $x^3 + y^3 = z^3$ ó $x^4 + y^4 = z^4$,... o aún un caso más general $x^n + y^n = z^n$ cuando $n > 2$?. Pues, si n =1, se tiene x + y = z, que tiene infinitas soluciones, se trata de la ley de clausura del conjunto de los naturales; además si n=2, entonces $x^2 + y^2 = z^2$ también tiene infinitas soluciones, se trata del teorema de Pitágoras restringida a los números enteros (ternas pitagóricas).

Según E. T. Bell, (1995 p. 31) y Aréan, L. (2012 p.12) Pierre de Fermat, leyendo la Aritmética de Diofanto de Alejandría habría encontrado una demostración admirable en 1637 en la que se concluye que no es posible encontrar soluciones a dicha ecuación con números enteros. Lamentablemente, tal demostración se perdió y nunca pudo ser encontrada, por lo que se convirtió en un reto para las generaciones de matemáticos de los siglos siguientes

La búsqueda de la demostración perdida

Leonhard Euler (1707-1783) uno de los más grandes matemáticos del siglo XVIII al encontrar por primera vez, el denominado último teorema de Fermat, tuvo la esperanza de poder resolverlo y se puso a leer con avidez lo ya desarrollado por Fermat con la firme decisión de hallar alguna huella que permitiera reconstruir tal demostración. Su dedicación tuvo como resultado el haber encontrado una demostración del propio Fermat para un caso aislado: $x^4 + y^4 = z^4$, no tiene soluciones enteras. En su demostración se había utilizado un método denominado de descenso infinito y creado por Fermat. Este es un método relacionado con las demostraciones por inducción completa pero al revés, y las demostraciones por el absurdo.

Fermat, supuso que existe una terna que cumple con la propiedad $x^4 + y^4 = z^4$, luego demuestra que si esta terna existe, existe otra solución más pequeña, y otra más pequeña, y así sucesivamente hasta el infinito, pero aquí entra una contradicción, la serie de números naturales no puede descender infinitamente, por tanto el supuesto inicial es falso y así se demuestra que no existen ternas tal que $x^4 + y^4 = z^4$

Leonhard Euler, utilizando el métodos de descenso infinito encontró una demostración para el caso $x^3 + y^3 = z^3$, sin embargo, esta última demostración incluye la aceptación de la existencia de los números denominados imaginarios, es decir $i = \sqrt{-1}$. Euler insinuó que no habría forma de resolver el teorema general. Sin embargo surgió una idea que abrigaría una esperanza. Pues, pues si no es posible resolver para el caso cuando n = 4, tampoco sería posible para el caso donde n fuera múltiplo de 4, es decir 8, 12, 16, ... 4m; pues en cualquier caso tales ecuaciones se reducen a una forma $x^4 + y^4 = z^4$, imposible de tener soluciones enteras. Lo mismo pasaría en el caso de n = 3, tampoco tendrían soluciones las potencias de 3, es decir, 6, 9, 12, 15,...3p. Consecuentemente, conforme al *teorema fundamental de la Aritmética,* que afirma que todo número entero se puede descomponer en el producto de números primos, entonces sería suficiente demostrar que la ecuación $x^n + y^n = z^n$ no tiene solución con números enteros cuando n es un número primo mayor que 2. Después de casi un siglo al fin se había dado un paso importante pero surge ahora otra dificultad: existen infinitos números primos.

La francesa Sophie Germain (1776-1831) en carta dirigida al Príncipe de las Matemáticas el alemán Karl Friedrich Gauss (1777-1855), bosqueja un cálculo que se concentraba en una caso más general los números primos *p* tal que *P = 2p + 1* también es un número primo. Tales como 5 porque 2x5+1 = 11 que también es primo, etc., pero no incluye en su lista al 13 porque 2x13 + 1 = 27, y 27 no es primo. Sophie Germaín utilizando un refinado argumento concluyó que cuando n es igual a estos primos la ecuación $x^n + y^n = z^n$ probablemente no tenga soluciones. El autor, afirma que con este método Sophie Germaín logró demostrar que el Teorema de Fermat-Wiles era cierto para todos los números primos regulares menores de 100. Además, que esta era la primera demostración no para casos particulares sino para una clase de números. Sin duda alguna un enorme progreso.

En 1825 se produce otro pequeño avance: Gustav Lejeune-Dirichlet (1805-1859) y Adrien-Marie Legendre (1752-1833), ambos en forma independiente demostraron que cuando n = 5 no tiene solución. Ellos utilizaron los resultados de S. Germain. Pocos años más tarde Gabriel Lamé (1795-1870) demostró que cuando n = 7 tampoco existe solución.

Estos avances súbitamente fueron alertados por un argumento de Ernest Kummer (1810-1893). Las demostraciones realizadas hasta la fecha, aún sin mencionarlas estaban basadas en el reconocimiento implícito de que la factorización es única. Así pues, los dominios de factorización única DFU, como en el caso de los números enteros, cuando se factoriza un número, sólo se puede hacer de una única manera como producto de números primos (salvo el orden); sin embargo desde Leonhard Euler para el caso n = 3 había habido necesidad de introducir los números complejos que están formados por una parte real y otra parte imaginaria, siendo todo número de la forma a + bi. Pero los números complejos no son dominios de factorización única, sino que admiten varias factorizaciones. Ejm. $15 = 3 \times 5$; pero también $15 = (2 + \sqrt{11}\, i)(2 - \sqrt{11}\, i) = (3 + \sqrt{6}\, i)(3 - \sqrt{6}\, i)$... es decir, no hay factorización única.

Tanto Gabriel Lamé como Augustin Louis Cauchy (1789-1857) que habían trabajado en la aceptación implícita de la factorización única quedaron desilusionados ante las observaciones de Ernest Kummer (1810-1893). Sin embargo, el propio Kummer desarrolló una poderosa

estrategia para demostrar que la conjetura de Fermat era cierta para una clase de exponentes, los exponentes primos regulares (los números primos que mediante un artificio podían ser aceptados como casos de factorización única, es decir un grupo de clase de ideales). Stewart (2014, p 158) ampliando lo que considera Areán, menciona que para el efecto hubo necesidad de crear el concepto de Ideal dentro de un anillo, como es el caso de los múltiplos de un número entero, pero un número ideal no es en realidad un número, se trata de símbolos que se comportan de forma muy parecida a los números. De ésta manera demostró que todo entero ciclotómico puede factorizarse unívocamente en números primos ideales. Así Kummer anunció que se podía demostrar que el último Teorema de Fermat, se podía demostrar para un número grande de exponentes, a los que llamó primos regulares. (en adelante para referirnos al último teorema de Fermat-Willes, qu es la denominación actual, sólo se escribirá TFW)

Pero por supuesto que quedaba en duda los exponentes que no pertenecieran a dicha clase (los exponentes primos irregulares o sea aquellos que aún con el artificio anterior no podían ser expresados como casos de factorización única), no pudiendo descartarse que en el segundo grupo de exponentes hubiera alguno para los que la conjetura fuera falsa. Los acontecimientos se estaban desarrollando lentamente.

Kummer había probado que una demostración completa del TFW estaba más allá de las técnicas matemáticas conocidas hasta ese momento. Su argumento era una pieza brillante de lógica matemática y a su vez un duro golpe para la generación de matemáticos que tenían la esperanza de lograr una demostración que ya había anunciado Pierre de Fermat en 1637.

El problema de los fundamentos de la matemática

Un aspecto que no considera Aréan Alvarez, que sin embargo, en mi modesta opinión es muy importante, es aquella que vincula al TFW con los fundamentos de la matemática. (Singh, 1999 pp 219-231), pues, con la creación de la *Teoría de conjuntos* por Georg Cantor (1845-1918) se inicia un período de revisión de los fundamentos de la matemática debido fundamentalmente al hecho de que la aritmética y los sistemas numéricos fueron axiomatizados. La nueva axiomática rechaza el principio de evidencia que tanto habían reclamado los griegos respecto a la naturaleza de los axiomas. Ahora un axioma es simplemente una proposición no demostrada que se acepta para el inicio de una teoría, el axioma puede o no ser evidente, con la única condición de que el sistema sea *consistente, independiente y completo.*

La consistencia exige que dentro de la teoría no pueda demostrarse jamás una proposición p y su contrario ~p ambas como verdaderas. La independencia implica que los axiomas son tales que nunca un axioma pueda deducirse de los otros axiomas porque entonces ya no es un axioma sino un teorema, y finalmente que el sistema sea completo o que tenga todos los axiomas que la teoría necesita para su desarrollo.

Lamentablemente Kurt Gödel (1906-1978) en metamatemática estableció dos proposiciones de *indecidibilidad,* que puede resumirse brevemente en: Primer teorema de indecidibilidad: Si la teoría axiomática de los conjuntos es consistente, entonces hay dos teoremas que no pueden ser comprobados ni refutados. *Segundo teorema de indecidibilidad:* No hay ningún procedimiento constructivo que pueda demostrar que la teoría axiomática es consistente, *lo que condujo al denominado* teorema de incompletitud *de la Aritmética que manifiesta:* "Si la aritmética formal es no contradictoria (es consistente) existe una fórmula de la aritmética formal tal que ni F ni no-F son demostrables dentro de esta teoría". En otras palabras, si la

aritmética formal es consistente, entonces no es una teoría completa. La consistencia de una teoría implica la existencia de alguna proposición de esa teoría que no puede demostrarse que sea verdadera o que sea falsa. ¿Sería acaso, el TFW una proposición indemostrable? Si la respuesta es afirmativa se habría encontrado una prueba de que la aritmética es consistente o no contradictoria. Ahora, el problema es demostrar que es indemostrable.

La era de las computadoras y el TFW

Después de la Segunda Guerra Mundial con el desarrollo de las computadoras y después de haber descubierto un error en el trabajo de Cauchy y Lamé, Kummer mostró que lo que faltaba para probar el TFW era resolver los casos en los que *n* es igual a un número primo irregular (los únicos primos irregulares menores de 100 son 37; 59 y 67; sin embargo los primos irregulares son infinitos), por tanto, para lograr una demostración del TFW había que demostrar que lo era cuando los exponentes eran primos irregulares, pero los cálculos eran tediosos y muy complicados.

El propio Kummer y su colega Dimitri Mirimanoff (1889-) dedicaron varias semanas al cálculo de los tres primeros primos irregulares. Varias décadas después con la ayuda de la naciente tecnología de las computadoras estos cálculos se abreviarían y así en la década de los ochenta, Samuel S. Wagstaff (1945) de la Universidad de Illinois llegaría a comprobar que el último teorema de Fermat no tiene solución cuando *n* toma valores hasta veinticinco mil. Otros trabajos más recientes se han realizado con computadoras más veloces y de mayor capacidad y se ha logrado verificar que el último teorema de Fermat es verdadero para todos los valores cuando *n* llega hasta cuatro millones.

Sin embargo, estos cálculos no pueden considerarse como una demostración, son simplemente evidencias, pero en matemática las evidencias no constituyen demostraciones. Una proposición adquiere la ciudadanía de teorema cuando se realiza su demostración, caso contrario queda como conjetura.

Se logra la demostración del TFW, más de 350 años después

Andrew Wiles, nacido el 11 de abril de 1953 en Cambridge- Inglaterra, lograría la hazaña de realizar la primera demostración completa del denominado último teorema de Fermat-Wiles.

Horizonte de la Ciencia 5 (9) Diciembre 2015 FE/UNCP. ISSN (Impreso): 2304-4330/ ISSN (En Línea): 2413-936X
Contreras, F. El último teorema de Fermat-Wiles. 211-218

Nuevamente Stewart (2014, p. 166) agrega un dato no considerado por Areán, en 1971 Wiles obtuvo un grado en matemáticas en Oxford y se trasladó a Cambridge para hacer su doctorado, parece que quiso ocuparse del último teorema de Fermat como tema de graduación, pero fue advertido Por Jhon Coates (1945-) que se trataba de un tema muy difícil para una tesis. Cuando Andrew Wiles se doctoró en 1978 su asesor Jhon Coates le aconsejó que debería estudiar un área de la matemática denominado *curvas elípticas* que son ecuaciones de la forma $y^2 = x^3 + ax^2 + bx + c$ donde a, b y c son números enteros y que están relacionadas con las ecuaciones que sirven para calcular el movimiento de los planetas (esta es la razón por la que se les denomina curvas elípticas). Demostrar que una ecuación de una curva elíptica tiene un solo conjunto de soluciones en números enteros es una tarea inmensamente difícil. Sin embargo mediante propiedades de la teoría de grupos de Evariste Galois (1811-1832) y fundamentalmente con la denominada *aritmética del reloj* es posible encontrar soluciones. Para ello cada ecuación de una curva elíptica proporciona una *serie E*. La serie E lleva la esencia de la ecuación elíptica y se constituye en una especie de ADN de las ecuaciones elípticas.

En 1954 dos jóvenes matemáticos japoneses Goro Shimura (1928-) y Yutaka Taniyama (1927-1958) comenzaron a estudiar ecuaciones que ya habían sido abandonadas en Occidente : *formas modulares*, los teóricos de los números consideraban cinco operaciones fundamentales: adición, sustracción, multiplicación, división y formas modulares (La operación formas modulares, se refiere a la simetría de las figuras geométricas). Las formas modulares que habitan en el espacio hiperbólico tienen varios diseños y tamaños, pero cada uno de ellos está construido con los mismos componentes básicos. Las formas modulares proporcionan una *serie M* que a su vez se constituyen en una especie de ADN de las formas modulares.

Taniyama y Shimura creían firmemente que había una relación entre las ecuaciones elípticas y las formas modulares, sin embargo por más que afinaron sus argumentos lógicos nunca pudieron demostrar tal relación. Taniyama-Shimura, estaban convencidos que a toda ecuación elíptica le corresponde una forma modular. Esta proposición se conoció como la conjetura de Taniyama-Shimura, que fue la base de muchos avances en la Matemática pese a su condición de conjetura. Sin embargo, se encontraron nuevas evidencias de tal relación. Si la conjetura de Taniyama-Shimura era verdadera, ello permitiría a los matemáticos abordar, a través del mundo modular, problemas elípticos que habían permanecido sin resolver durante siglos. Entre ellos el último teorema de Fermat.

En 1984 Gerhard Frey (1944-) con un razonamiento por el absurdo logró establecer el puente que estaba faltando para la demostración del último teorema de Fermat. Pensó en una solución hipotética del último teorema de Fermat. Existen los números enteros A, B y C que satisfacen la ecuación de Fermat $x^n + y^n = z^n$ Frey convirtió la ecuación original de Fermat con la solución hipotética en la ecuación elíptica $y^2 = x^3 + (A^N - B^N)\,x^2 - A^N B^N$. Luego, si la conjetura de Taniyama-Shimura es verdadera entonces toda ecuación elíptica es modular. Si toda ecuación elíptica es modular entonces no puede existir la ecuación elíptica de Frey. Si la ecuación elíptica de Frey no existe entonces no puede haber soluciones a la ecuación de Fermat. Por tanto el último teorema de Fermat es verdadero.

Andrew Wiles utilizando un razonamiento por inducción matemática finalmente logró demostrar que la conjetura de Taniyama-Shimura era verdadera. Primero demostró que era verdadero para N = 1, luego suponiendo que es verdadera para un N había que demostrar que también era verdadero para N + 1, es decir para el sucesor de N. Esta tarea no fue nada fácil. Los cálculos eran enormes y tediosos. Hubo necesidad de recurrir al uso de la técnica combinada de Kolyvagin-Flach y a la teoría de Iwasawa. Ambas, por si solas eran insuficientes.

El 24 de junio de 1993 al terminar una serie de tres conferencias sobre "Formas modulares, curvas elípticas y teoría de Galois" se anunció al mundo la demostración de la conjetura Taniyama-Shimura y como corolario de este teorema el último teorema de Fermat-Wiles, sin embargo el Comité que debería verificar, encontró un error, faltaba justificar uno de los pasos. La corrección de este pequeño detalle llevaría algo más de un año. Andrew Wiles tuvo que recurrir a la ayuda de uno de sus brillantes alumnos Richard Lawrence Taylor (1962), finalmente entre setiembre y octubre de 1994 se corrigió lo que faltaba y se entregó al Comité evaluador el informe completo en 130 páginas de Matemáticas que se tuvo que crear para lograr semejante hazaña. En 1995, el Comité encargado de la revisión aceptó la demostración de TFW.

Por esta epopeya intelectual en 1998 recibió la Medalla Fields de Matemática, asimismo, el asteroide 9999 se ha denominado Asteroide Wiles, en su honor. El presente artículo de divulgación es un homenaje a los veinte años de la demostración del TFW y a la generación de matemáticos que nos han enseñado el valor de no rendirse.

Conclusiones

1. La proposición lanzada por Pierre de Fermat se hizo en 1637 y lo convirtió en Teorema en 1995 Andrew Wiles. Por esa razón en la actualidad se conoce con el nombre de Teorema de Fermat-Wiles.
2. Para la demostración del TFW hubo que crear nueva matemática, matemática que no existía en los tiempos de Fermat. Tal vez Fermat generalizó muy pronto su proposición y cuando se dio cuenta de que había un error en la demostración que afirma haber logrado, nunca volvió a mencionarla. O tal vez si lo demostró, en cuyo caso debe haber sido por un camino totalmente diferente al de Andrew Wiles. La demostración del ahora teorema de Taniyama-Shimura, ha permitido enormes avances en la teoría de números.
3. En la demostración del último teorema de Fermat-Wiles se constata la unidad del pensamiento matemático, puede considerarse como una demostración aritmético-geométrico-algebraico.
4. El teorema de Fermat fue propuesto en 1637, la demostración final se realizó en 1994; por la persistencia de generaciones de matemáticos.
5. El problema es viejo, pero las matemáticas para resolverlo son modernas. Con las matemáticas tradicionales, todo indica que no es posible resolverlas. Esto hace indispensable renovar la enseñanza de la matemática en las universidades, revitalizándolas con el espíritu de la matemática después de 1910 (nacimiento oficial del algebra moderna)
6. Matemáticas y matemáticos sin fronteras lograron la hazaña de su demostración

Referencias bibliográficas

Areán L.F. (2012) *Fermat. El teorema de Fermat. El problema más difícil del mundo.* España: EDITEC.

Bell. E.T. (1995) *Historia de las matemáticas.* México: Fondo de Cultura Económica.

Dunham, W. (1995) *El universo de las matemáticas.* Madrid, España: Ediciones Pirámide S.A.

García Venturini, A. E. (2003) *Los matemáticos que hicieron historia.* Buenos Aires, Argentina: Ediciones Cooperativas.

Singh, S. (1999) *El último teorema de Fermat.* Argentina: Grupo editorial Norma.

Singh, S. (2003) *El enigma de Fermata.* España: El planeta.

Stewart I. (2014) *Los grandes problemas matemáticos.* Barcelona. España: Editorial Crítica. 147-169.