SOBRE LA CONJETURA DE FERMAT

01.La historia:

Pierre de Fermat, que nació en el año 1601 en Beaumont-de-Lomagne, Francia, y murió en París en 1665, fué de profesión jurista y aficionado a la Matemática, disciplina en la que dejó resultados notables tanto en teoría de curvas, como en el cálculo de probabilidades o en la teoría de números.

Tenía la costumbre de anotar en los márgenes de los textos que leía posibles demostraciones de los resultados que aparecian expuestos u otros resultados que él mismo podía deducir. Así, dejó en uno de los márgenes de la *Aritmética, de Diofanto,* una conjetura muy simple de explicitar pero tan difícil de demostrar que ha traido al mundo científico de cabeza durante más de 300 años.

Lo curioso es que en el mismo márgen de dicho texto, Fermat escribió que poseía una demostración "maravillosa" que, sin embargo, no cabía en el estrecho márgen del libro de Diofanto. Este hecho ha representado históricamente un enigma, pues las generaciones posteriores, a la vista de la dificutad de dar con una demostración, "maravillosa" o no, se plantearon que, o bien el doctor Pierre de Fermat se quedó olimpicamente con el personal, o bien, estaba en un craso error al considerar que disponía de algún tipo de demostración.

La *Última Conjetura de Fermat*, o bien, como generalmente ha sido denominada, *El último Teorema de Fermat*, afirma sencillamente que la expresión $x^n + y^n = z^n,\ x,y,z \in Z, n \in N$ no tiene solución para n > 2. O sea, que si x^n e y^n son potencias perfectas de números enteros, nunca podrá ser $x^n + y^n$ potencia perfecta de números enteros cuando es n > 2.

Pierre de Fermat. Museo de Ciencias y Letras de Toulouse

Todos los intentos realizados en los tres siglos siguientes a la muerte de Fermat, tanto de encontrar una demostración de la veracidad de la conjetura, como de encontrar un caso que la contradijera, han resultado fallidos. Nunca se pudo, en ese intervalo de tiempo, avanzar más en lo que respecta a la conjetura, aunque es cierto que las investigaciones desarrolladas por diferentes matemáticos en los siglos XVIII, XIX y XX, han servido para desarrollar de forma extraordinaria la teoría de números.

Tanto es así que, desde 1908, existía un premio de 100.000 marcos que habría de entregarse a la persona o personas que lograran una demostración de la conjetura que se pudiera contrastar antes del dia 13 de septiembre del año 2007. El premio, administrado por la universidad de Gotinga, se ofrecía por la demostración, no por encontrar un ejemplo que rechace la conjetura. En el año 1997 se hizo entrega al profesor Andrew John Wiles de dicho premio.

02. Las infinitas soluciones del caso pitagórico:

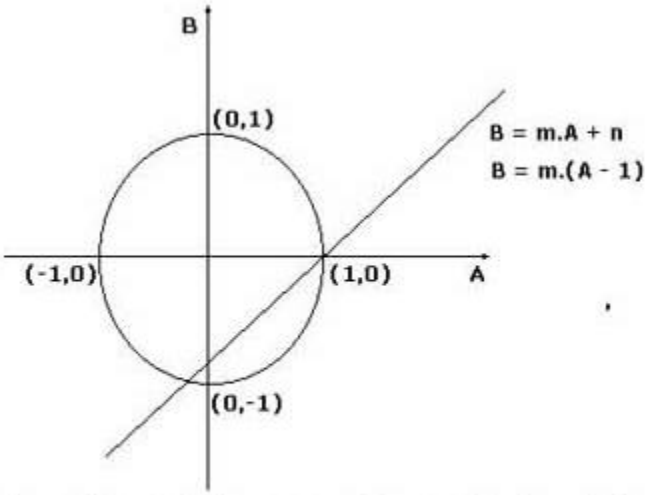
El caso pitagórico corresponde a la situación en la que n = 2. Este, evidentemente, no es el caso al que se refiere la conjetura de Fermat. Lo que vamos a ver a continuación es como, a partir de una solución particular de la ecuación pitagórica $x^2+y^2=z^2$ podemos generar todas las infinitas soluciones de la misma.

Si dividimos por z^2 toda la ecuación, se tendría:

$$x^2+y^2=z^2 \rightarrow \left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1 \rightarrow A^2+B^2=1,\ A,B\in Q$$

Que es, evidentemente, la ecuación de una circunferencia de radio unidad.

Partamos de la solución particular más simple. Por ejemplo de A = 1, B = 0. También serán soluciones A= -1, B = 0, y A = 0, B = 1, o, también, A= 0, B = -1. Estas soluciones, las más simples por ser enteras, estarían situadas en los puntos de corte de la circunferencia de radio unidad con los ejes cartesianos del plano AB:



Al variar la pendiente m de la recta, se obtienen todas las soluciones de la ecuación pitagórica.

Todos los puntos de esa circunferencia verifican, evidentemente, la ecuación de la misma, es decir, están sobre la circunferencia, por lo que la intersección de una recta cualquiera con la circunferencia nos dará un punto solución de la ecuación anterior..

Consideremos, por ejemplo, la recta que pasa por (1,0) y veamos su interección con la circunferencia:

$$\begin{cases} A^2+B^2=1 \\ \\ B=m.(A-1) \end{cases} \Rightarrow A^2+m^2.(A-1)^2=1 \Rightarrow \left(1+m^2\right).A^2-2m^2.A+m^2-1=0$$

ecuación de segundo grado en A, con soluciones dadas por

$$A=\frac{m^2\pm 1}{m^2+1}=\begin{cases}\dfrac{m^2+1}{m^2+1}=1 \\ \dfrac{m^2-1}{m^2+1}\end{cases}$$

para A = 1, B = m.(A - 1) = 0 o sea, (A, B) = (1, 0) trivialmente.

Veamos la otra solución:

$$A=\frac{m^2-1}{m^2+1},\quad B=m.(A-1)=m.\left(\frac{m^2-1}{m^2+1}-1\right)=.\frac{-2m}{m^2+1}$$

Por tanto:

$$(A,B)=\left(\frac{m^2-1}{m^2+1},\frac{-2m}{m^2+1}\right)$$

Esto quiere decir que si sustituimos m por el cociente de dos enteros, que para que resulte positiva la segunda componente, ha de ser negativo:

$$m=-\frac{p}{q},\ p,q\ \ primos\ entre\ si$$

resulta:

$$A = \frac{p^2 - q^2}{p^2 + q^2}, \quad B = \frac{2pq}{p^2 + q^2}$$

y, deshaciendo el cambio inicial A = x/z, B = y/z, se tiene, finalmente que el conjunto de todas las infinitas soluciones de la ecuación pitagórica puede expresarse por las formas modulares que la parametrizan con parámetros p y q (números enteros primos entre sí):

$$x = p^2 - q^2, \quad y = 2pq, \quad z = p^2 + q^2$$

Así, en definitiva, si se toman dos números enteros, primos entre sí cualesquiera que sean, puede encontrarse inmediatamente la correspondiente solución de la ecuación diofántica pitagórica:

para p = -3, q = 7, se tiene que es x = -40, y = 42, z = 58.

para p = 10, q = 3, se tiene que es x = 91 , y = 60 z = 109.

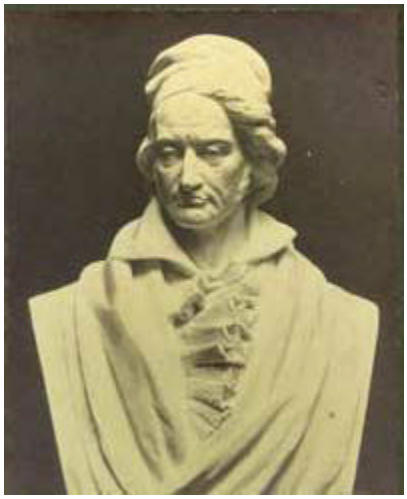
para p = 6, q = 5, se tiene que es x = 11, y = 60, z = 61.

Se tiene, en definitiva, que el caso pitagórico N = 2, de la ecuación diofántica $x^N + y^N = z^N$ tiene infinitas soluciones. Sin embargo, los casos no pitagóricos N > 2 no admitían ni un solo ejemplo de existencia de solución entera, ni tampoco se le pudo encontrar una prueba de imposibilidad de soluciones durante más de 350 años. Durante estos años hubieron muchos intentos de demostración de la conjetura de Fermat.

03. Los intentos clásicos de demostración de la conjetura:

Durante más de 350 años fueron muchos los intentos de demostración de la conjetura de Fermat, interviniendo en el estudio del problema tanto matemáticos de la talla de Euler, Dirichlet, Legendre, Gauss o Kummer, como otros menos conocidos. Todos ellos, en un esfuerzo épico en la historia de la Matemática, intentaron la prueba del enunciado para ciertas condiciones parciales, para ciertos exponentes N de la ecuación diofántica. Para algunos de estos exponentes se logró el propósito, pero la demostración general de esta proposición permanecería faltalmente inalcanzable a los esfuerzos de la comunidad matemática.

El desafío que representó el problema de la conjetura de Fermat originó un desarrollo extraordinaro de la investigación en la teoría de los números, descubriéndose relaciones, propiedades y aplicaciones en el campo numérico que de no ser por ese estudio hubieran pasado muchos años antes de evidenciarse. En este sentido, se considera a Fermat el padre de la teoría de números.


Carlos F. Gauss (1777-1855)


Adrian M. Legendre (1752-1833)


Agustin L. Cauchy (1789-1857)


Gabriel Lamé (1795-1870)


Peter G. L. Dirichlet (1805-1859)


Erns Eduard Kummer (1803-1893)

04. Curvas elípticas. Curvas elípticas modulares:

Las curvas elípticas sobre un cuerpo K son en general expresiones del tipo siguiente:

$$y^2 = x^3 + a.x^2 + b.x + c, \quad a,b,c \in K$$

si el cuerpo K = Q, entonces estamos en el caso racional.

Una curva se dice modular si puede ser parametrizada por funciones modulares, esto es, por funciones de variable compleja, o sea, si se puede reducir a una combinación de funciones con el mismo módulo, o, dicho de otra manera, si se le puede hacer corresponder una forma modular.

Una curva elíptica modular es una curva elíptica que se puede parametrizar por una forma modular, o por una combinacion de formas modulares.

05. La conjetura de Taniyama-Shimura:

Esta conjetura, hecha por Yutaka Taniyama (Kisai, 1927 - Tokio, 1958) y por Goro Shimura (1930 -) puede enunciarse de esta manera:

- "Todas las curvas elípticas son modulares"

o bien:

- "A cada forma modular le corresponde una curva elíptica, y viciversa, a cada curva elíptica le corresponde una forma modular"

Yutaka Taniyama murió en 1958, a los 31 años, sin que hubiera podido siquiera vislumbrar lo que al cabo de 35 años supondría su conjetura sobre la modularidad de las curvas elípticas en el estudio del enunciado de Fermat.

Yutaka Taniyama

06. El trabajo de Gerhard Frey y de Kenneth A. Ribet:

El último acto de la historia de la Conjetura de Fermat comenzó en el año 1984, cuando al matemático alemán, de la universidad de Essen (Institut für Experimentalle Mathematik) se le ocurrió escribir la siguiente expresión

$$y^2 = x.(x + A^n).(x - B^n)$$

donde tanto A^n como B^n son potencias n-simas perfectas de números enteros con la condición de que tambien $A^n + B^n$ sea potencia perfecta (n>2). La ecuación anterior es, realizando operaciones de simplificación:

$$y^2 = x^3 + (A^n - B^n).x^2 - A^n.B^n.x$$

o bien:

$$y^2 = x\left[x^2 + (A^n - B^n).x - A^n.B^n\right]$$

donde el discriminante del polinomio de segundo grado es:

$$\Delta^2 = \left(A^n - B^n\right)^2 - 4.(-A^n.B^n) = A^{2n} + B^{2n} + 2.A^n.B^n = \left(A^n + B^n\right)^2$$

y de aquí que el discriminante habría de ser potencia perfecta de números enteros:

$$\Delta = A^n + B^n$$

Ahora bien, Kennet A. Ribet, de la Universidad de Berkeley, demostró en junio del año 1986 que la expresión

$$y^2 = x^3 + (A^n - B^n).x^2 - A^n.B^n.x$$

donde el discriminante fuera una potencia perfecta no puede ser modular.

07. Andrew Wiles:

A la vista del trabajo de Gerhard Frey y de Kenneth A. Ribet, habría de deducirse que, o bien la conjetura de Taniyama-Shimura no es cierta, existiendo curvas elípticas que no son modulares, o bien, si fuera verdad que todas las curvas elípticas son modulares habría que concluir que la expresión construida por Frey:

$$y^2 = x^3 + (A^n - B^n).x^2 - A^n.B^n.x$$

simplemente, no existe. Es decir, no podría existir una curva elíptica con la expresión anterior en la que el discriminante fuera un cuadrado perfecto, o, dicho de otro modo, no podría existir una expresión en la que aparecieran dos números, A^n y B^n, potencias perfectas, de modo que también fuera $A^n + B^n$ potencia perfecta, esto es, quedaría demostrada la Conjetura de Fermat.

Todo el problema se reduciría, por consiguiente, a probar la conjetura de Taniyama-Shimura para que quedase probado el enunciado de Fermat, o, por el contrario, a probar la falsedad de tal conjetura, que probaría también la falsedad de la Conjetura de Fermat.

El trabajo del matemático inglés, profesor luego en Princenton, Andrew John Wiles (1953-) consistió, en definitiva, en estudiar a fondo la Conjetura de Taniyama-Shimura y tratar de dar con una demostración de la misma, o bien, con una demostración de su falsedad.

Entre los años 1986 y 1993, desarrollando un aparato matemático de gran complejidad, A. Wiles se dedicó al estudio de la Conjetura de Taniyama-Shimura, hasta comunicar a la comunidad científica, en 1993, que habia logrado la prueba. Un análisis detallado del trabajo presentado por Wiles descubrió un fallo sustancial en la argumentación, que le hizo revisarlo con la ayda de su discípulo Richard Taylor, revisión que le costó un año de trabajo. Finalmente, en 1994, la prueba de Andrew Wiles del Teorema de Fermat, fué aceptada.


Andrew Wiles y Richard Taylor

08. Documentación:

Bibliografía:

Aczel, A. D., "Fermat's last theorem", Dell, N.Y., 1997.
Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. Math. 141 (1995), 443-551.
Andrew Wiles and Richard Taylor, Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (1995), 553-572.
Carmichael, R. D., "The Theory of numbers and Diophantine Analysis", Dover, N.Y., 1959.
Klein, Félix, "Elementary Mathematics from an Advanced Stand point,Arithmetics, Algebra, Analysis", Dover, N.Y., 1947.
Rademacher, H. y Toeplitz, O., "Números y Figuras", Alianza Editorial, Madrid,1970.
Singh, Simon, "El enigma de Fermat", Planeta, 1998.
Tate, John, "Rational points in eliptical curves", New York, Springer Verlag, 1992

Artículos de prensa a raiz de la demostración de Wiles:

"At Last, Shout of `Eureka!' in Age-Old Math Mystery," by Gina Kolata, New York Times, June 24, 1993.
"a^n + b^n = c^n, Le theoreme de Fermat enfin resolu?" Jean-Francois Augereau, Le Monde, June 25, 1993.
"350 Years Later, Math Conundrum Bites the Dust," by Gina Kolata, International Herald Tribune, June 25, 1993.
"x^n + y^n = z^n: Princeton professor appears to have proved Fermat's Last Theorem," by Kim A. McDonald, Chronicle of Higher Education, July 7, 1993.
"Math Whiz who Battled 350-Year-Old Problem," by Gina Kolata, New York Times, June 29, 1993.
"Fermat's Last Theorem Finally Yields," by Barry Cipra, Science, July 2, 1993.
"Curvy Path Leads to Fermat's Last Theorem," by Ivars Peterson, Science News, July 3, 1993.
"Fini to Fermat's Last Theorem," by Michael D. Lemonick, Time, July 5, 1993.
"Wiles Proves Taniyama's Conjecture; Fermat's Last Theorem Follows," by Kenneth A. Ribet, Notices of the AMS, July/August 1993.
"No Margin Would Contain It: A proof of Fermat's last theorem comes to Andrew Wiles," by Peter G. Brown, The Sciences, September/October 1993.

"Update on Proof of Fermat's Last Theorem: Gap appears in proof but experts laud Wiles's accomplishment," by Allyn Jackson, Notices of the AMS, March 1994.
"Fermat's Last Theorem and modern arithmetic," by B. Hayes and K. Ribet, American Scientist, March--April, 1994.
"Princeton Mathematician Looks Back on Fermat Proof," by Barry Cipra, Science, May 26, 1995.

Páginas Web en la red:

- Ecuaciones diofánticas elementales.
http://193.146.240.173/codigo/semana/10_4_99/diofanto.htm

- Pierre de Fermat, el padre de la Teoría de Números
http://centros5.pntic.mec.es/cpr.de.aranjuez/foro/circo/FERMAT.htm<

- Los 23 problemas de Hilbert y su transfondo histórico
http://www.math.temple.edu/~gmendoza/boletin_amv/conten/vol5/v5n2p117.pdf<

- Los problemas futuros de la Matemática- Conferencia
http://www.geocities.com/Athens/4346/hilb.html<

- Nota sobre el Ultimo Teorema de Fermat y su Demostración por Andrew Wiles
http://www.ciencia.cl/CienciaAlDia/volumen2/numero1/articulos/articulo1.html<

- Fermat's Last Theorem
http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html>

Carlos S. Chinea
casanchi@teleline.es