

UN PASEO POR EL ÚLTIMO TEOREMA DE FERMAT

Xavier Valls Aubert

Departament de Didàctica de les Matemàtiques i de les CCEE. UAB

Introducción

La primera vez que oí hablar del último teorema de Fermat, fue cuando cursaba quinto de bachillerato. Un día el profesor, no recuerdo exactamente por qué motivo, nos explicó su extraordinario origen, y lo difícil que era darle una respuesta conclusiva, a pesar de la relativa sencillez de su enunciado. Los más grandes matemáticos desde los tiempos de Fermat hasta la actualidad habían intentado resolver el problema en vano. Los nombres de Euler, Lagrange, Legendre, Gauss, Dirichlet, Kummer y muchos otros están ligados a su historia. Algunos de ellos habían obtenido soluciones en casos particulares, pero nadie había sido capaz de resolverlo de forma general. A pesar de las advertencias que nos hizo el profesor de que no intentáramos hallar una solución pues ya debíamos comprender que el problema era muy y muy difícil, al llegar a casa, eché mano de la calculadora y estuve varias horas intentando hallar un contraejemplo. Evidentemente no hallé ninguno, pero ha sido uno de los problemas que me hizo ver claro mi interés por las matemáticas.

Demos un breve paseo por su apasionante historia.

Un margen demasiado estrecho

Pierre Fermat era abogado y miembro del parlamento de Toulouse, y dedicaba su tiempo libre a las matemáticas. Su gran afición por ellas le ha convertido en una de las figuras clave de la historia de las matemáticas. Es uno de los creadores de la geometría analítica, y la teoría de las probabilidades, uno de los precursores del análisis infinitesimal y el fundador de la teoría de los números.

A finales de la década 1630-40, mientras estudia los trabajos de Diofanto sobre números, hace gran cantidad de notas en los márgenes del libro. Una de ellas, hace referencia a la proposición: "Dado un cuadrado dividirlo en dos cuadrados", y dice: "Por otro lado es imposible separar un cubo

en dos cubos, o un bicuadrado en dos bicuadrados o en general separar cualquier potencia que no sea un cuadrado en dos potencias del mismo exponente. He encontrado una prueba realmente maravillosa de este hecho, pero el margen no es lo suficientemente amplio para contenerla"¹.

El nombre de "Último teorema de Fermat" con el que se conoce este enunciado, no se debe a que fuera el último que enunció, sino, que de todas las proposiciones que Fermat propuso durante su vida y a las que no dio solución, ésta es la única a la que los matemáticos aún no habían sabido dar una respuesta completa.

Es curioso que, habiendo manifestado Fermat que tenía una demostración del teorema antes de 1640, no diera ninguna, pues murió veinticinco años después, en 1665. Este hecho y las dificultades que se han tenido que superar para dar una respuesta definitiva al teorema, hace dudar, a la mayoría de los matemáticos, de que la demostración tan *maravillosa* de Fermat fuera completamente correcta.

A principios de nuestro siglo, P. Wolfskehl ofreció un importante premio a quien obtuviera una prueba del teorema. El hecho de que pudiera haber una demostración elemental del problema, junto con la posibilidad de ganar el premio, desencadenaron una gran profusión de aficionados que creyendo haber resuelto el problema enviaban su solución a los matemáticos de prestigio para que las juzgaran. Explican que el eminente especialista en teoría de los números, E. Landau, ante la avalancha de soluciones, creó una trajeta que decía, "Apreciado Sr./a: Se acusa recibo de su intento

1. ¡Cuántas veces no se habrá deseado que el margen no fuera mayor!. De hecho A. Weil se pregunta que hubiera pasado si Fermat hubiera tenido conciencia de estar escribiendo para la eternidad.

de demostración del último teorema de Fermat y se le devuelve. El primer error se halla en la página __, línea __." y Landau la hacía rellenar a sus estudiantes. Después de la Primera Guerra Mundial, con la devaluación del marco alemán el premio carece de valor monetario y por tanto hay muy pocos amateurs que crean haber hallado una respuesta. De todas formas, algunos se empecinan en que lo han conseguido y consideran que existe una conspiración de los matemáticos para que no se les reconozcan sus méritos.

Una generalización del teorema de Pitágoras

Antes de introducirnos en la propia historia del último teorema de Fermat, creo que es preciso aclarar la proposición a la que hace referencia la nota de Diofanto que Fermat comenta.

Todo el mundo recuerda haber estudiado en alguna ocasión el teorema de Pitágoras, que trata sobre triángulos rectángulos y cuyo enunciado es: "La suma de los cuadrados construidos sobre los catetos es igual al cuadrado construido sobre la hipotenusa", que reducido a la simplicidad de una ecuación se escribe

$$a^2 + b^2 = c^2$$

siendo a y b los catetos de triángulo rectángulo y c la hipotenusa.

También es posible que muchos recuerden que existe una solución muy sencilla de esta ecuación en números enteros, la dada por los números 3, 4 y 5, pues $3^2 + 4^2 = 5^2$ como es fácil comprobar. Pero, ésta no es la única solución en números enteros de dicha ecuación, si no, que como veremos en el próximo apartado, existen muchas más. Precisamente la proposición de Diofanto hace referencia a la búsqueda de todas las soluciones enteras posibles de dicha ecuación (descomponer un cuadrado en dos cuadrados), y de lo que se percató Fermat es que si cambiamos el exponente 2 por un 3, o por cualquier otro mayor, es decir, nos referimos a la ecuación

$$a^n + b^n = c^n, n > 2 \quad (1)$$

entonces no existe ninguna solución en números enteros no trivial, es decir, si no se admiten soluciones del tipo $7^5 + 0^5 = 7^5$, no existen números enteros a, b y c, distintos todos de cero, para los que la igualdad sea cierta.

Es curioso que siendo la formulación del teorema tan simple, sea tan difícil hallar un razonamiento que nos permita tener la certeza absoluta de que la relación (1) no es posible para cualquier n mayor que 2.

Ternas pitagóricas

Tal como hemos indicado anteriormente, Diofanto en su proposición, pretendía hallar una expresión general de todas las soluciones enteras de la ecuación $a^2 + b^2 = c^2$. Intentemos ver de qué manera.

La primera cuestión que creo interesante hacer notar es que si disponemos de una solución (por ejemplo, 3, 4 y 5), entonces podemos considerar una infinidad de soluciones múltiplos de ésta (por ejemplo, 6, 8 y 10; 9, 12 y 15;...), es decir, si a, b y c nos dan una solución, las ternas de la forma ak, bk y ck, también son solución (donde k es un número entero cualquiera). Por tanto, nos es lícito suponer que, en el caso de que a, b y c sean una solución, no tengan ningún divisor común, pues si tuvieran un divisor común d, podríamos hallar una solución más primitiva dividiendo los tres números por d. Una tal solución la llamaremos precisamente *primitiva*. A partir de ahora supondremos que toda solución es primitiva.

Si suponemos que tenemos una solución primitiva a, b y c, una segunda observación consiste en darse cuenta de que uno de los tres debe ser par, pues es imposible que los tres sean impares dado que la suma de dos números impares es un número par. Más aún, c, la hipotenusa, no puede ser par, pues su cuadrado sería múltiplo de 4, y por tanto a y b deberían ser impares, es decir, serían de la forma $2n+1$, y en consecuencia sus cuadrados tendrían una expresión de la forma $4n^2 + 4n + 1$, y la suma de los dos no podría ser múltiplo de 4. En consecuencia o a o b, es par. Sin pérdida de generalidad, podemos suponer que a es par.

Antes de entrar de lleno en la parte final de este análisis, es preciso que el lector tenga presente la siguiente proposición, que es consecuencia inmediata del teorema fundamental de la aritmética: **Si el producto de dos números primos entre sí, es un cuadrado, entonces cada uno de los números debe ser un cuadrado.** El teorema fundamental de la aritmética asegura que para todo número existe una descomposición en producto de números primos y que esta descomposición es única². Ahora, basta pensar que las descomposiciones en factores primos de ambos no tienen factores en común, por ser primos entre sí, y por tanto, la descomposición del producto puede considerarse como la yuxtaposición de las dos, pero en ésta

² Aquí reside una de las principales dificultades de la demostración del último teorema de Fermat.

todos los exponentes deben ser pares, y en consecuencia en las de los dos números los exponentes también serán pares y los números cuadrados perfectos.

Supongamos pues que tenemos una terna pitagórica primitiva a , b y c , en la que a es par, podemos poner la relación $a^2+b^2=c^2$ de la forma $a^2=b^2-c^2=(b+c)(b-c)$, como a , $b+c$ y $b-c$ son todos pares podemos hallar enteros positivos tales que $a=2u$, $b+c=2v$ y $b-c=2w$, de donde obtenemos $(2u)^2=(2v)(2w)$ o bien $u^2=vw$. Además, v y w son primos entre sí pues si tenemos un divisor común a ellos dos entonces también dividiría a su suma $v+w=1/2(b+c)+1/2(b-c)=b$, y a su diferencia $v-w=1/2(b+c)-1/2(b-c)=c$, que por hipótesis hemos supuesto primos entre sí. Nos encontramos pues, que tenemos dos números primos entre sí v y w , cuyo producto es un cuadrado perfecto u^2 , estamos en las condiciones de la proposición anteriormente citada y por tanto v y w son cuadrados perfectos, es decir, deben existir enteros positivos p y q primos entre sí, tales que $v=p^2$ y $w=q^2$. En definitiva podemos escribir:

$$c=v+w=p^2+q^2 \text{ y } b=v-w=p^2-q^2, \quad (2)$$

lo que demuestra que p ha de ser mayor que q , y además p y q han de ser de paridades opuestas, pues tanto c como b son impares. Un pequeño cálculo fácil de completar da además:

$$a=2pq. \quad (3)$$

Ya hemos resuelto nuestro problema, pues tenemos que para obtener una terna pitagórica primitiva basta con seleccionar dos números p y q , tales que p sea mayor que q y ambos sean de distinta paridad, y a partir de ellos construir la terna a partir de las relaciones (*) y (**) que hemos obtenido, tal como se puede comprobar en la tabla 1.

p	q	$a=2pq$	$b=p^2-q^2$	$c=p^2+q^2$
2	1	3	4	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61

El último teorema para el exponente 4

Volvamos ahora al problema que nos ocupa. El mismo Fermat demostró la imposibilidad para el

caso en que el exponente sea 4, es decir, para la ecuación $a^4+b^4=c^4$. De hecho lo hace para el caso más general $a^4+b^4=c^2$, pues es evidente que si dos cuartas potencias no pueden dar un cuadrado mucho menos podrán dar otra cuarta potencia. El tipo de razonamiento que utiliza para la demostración de este hecho, es un proceso creado por el propio Fermat, al que se denomina descenso infinito y consiste en suponer que se dispone de una solución y construir a partir de ella una nueva solución en números estrictamente menores. Si esto es **siempre** posible nos lleva a una contradicción, pues dada una solución, solo existen un número finito de soluciones menores.

Veamos como se aplicaría el descenso infinito en nuestro caso. Si tenemos tres números a , b y c , tales que $a^4+b^4=c^2$, vamos a ver que es posible obtener otros tres números u , v y w inferiores a los anteriores y tales verifican la misma relación $u^4+v^4=w^2$. Ahora podemos aplicar a u , v y w , el mismo proceso y obtener otros tres números inferiores y que verifican la misma relación y así de forma indefinida. Como es imposible que existan infinitas soluciones menores que una finita dada, el error proviene de suponer que una tal solución existe.

Supongamos pues que tenemos una terna a , b y c , tales que $a^4+b^4=c^2$, que es primitiva (no tiene divisores comunes). En particular a^2 , b^2 y c , son una terna pitagórica, de la que podemos suponer que a es par, existen por tanto p y q tales que $a^2=2pq$ y $b^2=p^2-q^2$. Esta última relación nos da otra terna pitagórica de hipotenusa p , b impar y q par, por lo que podemos encontrar números m y n con $p=m^2+n^2$ y $q=2mn$ de donde

$$a^2=4mn(m^2+n^2) \text{ con } m \text{ y } n \text{ primos entre sí}$$

y haciendo uso ahora de la proposición que hemos utilizado al hallar la ternas pitagóricas tenemos que tanto m , como n , como m^2+n^2 deben ser cuadrados perfectos, es decir, existen u , v y w tales que $m=u^2$, $n=v^2$ y $m^2+n^2=w^2$ y en definitiva $u^4+v^4=w^2$.

con lo que hemos obtenido una ecuación igual a la de partida, pero en la que los números u , v y w son más pequeños que los a , b y c originales (ya que $u^2=m < 4mn(m^2+n^2)=a^2$). Hemos obtenido pues los tres números que nos permiten aplicar el razonamiento del descenso infinito.

Suponer que existen a , b y c , tales que $a^4+b^4=c^2$, nos ha llevado a una contradicción, lo que nos

obliga a decidir que tal relación no es posible en números enteros positivos. Por tanto el teorema es cierto para $n=4$.

La demostración de Euler para el caso $n=3$.

El primero en dar solución al caso $n=3$, es decir, a la ecuación $a^3+b^3=c^3$, es Euler. En 1770 la publica, pero ya en 1754 había comunicado en una carta a Goldbach tener una prueba. Su demostración utiliza como en el caso de las cuartas potencias el método del descenso infinito, y propiedades de los enteros de la forma u^3+3v^3 , que en aquel entonces no estaban del todo esclarecidas, por lo que se considera que su prueba no era concluyente.

Veamos qual era la argumentación de Euler. Supongamos que tenemos tres enteros, a , b y c tales que verifican la relación $a^3+b^3=c^3$, podemos suponer que son primos entre si. Por tanto uno de ellos es par. Si suponemos que c es par podemos hallar p y q enteros primos entre si y de distinta paridad de forma que $a=p+q$ y $b=p-q$ de donde $a+b=2p$. Entonces $c^3=a^3+b^3=(a+b)(a^2-ab+b^2)=2p((p+q)^2-(p+q)(p-q)+(p-q)^2)=2p(p^2+3q^2)$.

De igual forma si suponemos que a o b es par, pongamos a , podemos hallar p y q enteros primos entre si y de distinta paridad de forma que $c=q+p$ y $b=q-p$ de donde $c-b=2p$ y $a^3=c^3-b^3=(c-b)(c^2+cb+b^2)=2p((q+p)^2+(q+p)(q-p)+(q-p)^2)=2p(p^2+3q^2)$.

Es decir, en ambos casos llegamos a que la misma expresión $2p(p^2+3q^2)$ ha de ser un cubo.

Ahora por analogía con las ternas pitagóricas sería conveniente que $2p$ y p^2+3q^2 fueran primos entre si y por tanto cada uno de ellos habría de ser un cubo. Esto no es cierto únicamente si p es múltiplo de 3. Nos encontramos pues ante dos posibilidades o bien p no es múltiplo de 3 y $2p$ y p^2+3q^2 son primos entre si o bien p es múltiplo 3. Abordaremos inicialmente el primer caso y después veremos como reducir el segundo al primero.

Suponemos que 3 no divide a p y que por tanto $2p$ y p^2+3q^2 són cubos. En este punto es donde la demostración de Euler tiene su punto flojo pues, supone que la única forma de que p^2+3q^2 sea un cubo es de que existan t y s tales que $p^2+3q^2=(t^2+3s^2)^3$, cuestión que no justifica de forma clara. Una vez establecida, la demostración es fácil.

A partir de la identidad:

$$(t^2+3s^2)(u^2+3v^2)=t^2u^2+9s^2v^2+3(t^2v^2+s^2u^2)+6tsuv-6tsuv=(tu+3sv)^2+3(tv+su)^2,$$

podemos escribir:

$$(t^2+3s^2)^3=(t^2+3s^2)[(t^2-3s^2)^2+3(2ts)^2]=[t(t^2+3s^2)-3s(2ts)]^2+3[t(2ts)+s(t^2-3s^2)]^2=(t^3-9ts^2)^2+3(3t^2s-3s^3)^2$$

de donde $p=t^3-9ts^2$ y $q=3t^2s-3s^3$. Si factorizamos estas expresiones obtenemos

$$p=t(t-3s)(t+3s) \text{ y } q=3s(t-s)(t+s)$$

y por tanto t y s han de ser primos entre si pues cualquier factor común lo sería también de p y q y además han de ser de distinta paridad sino p y q serían ambos pares. Considerando que $2p=2t(t-3s)(t+3s)$ ha de ser un cubo, y que $t-3s$ y $t+3s$ son impares, cualquier factor común entre $2t$ y $t\pm 3s$ ha de serlo de t y $t\pm 3s$ y en definitiva de t y $\pm 3s$. Igualmente cualquier factor común de $t-3s$ y $t+3s$ ha de serlo de t y $3s$. En todos los casos llegamos a que t ha de ser múltiplo de 3, pero entonces p también lo sería en contra de la hipótesis. Es decir $2t$, $t-3s$ y $t+3s$ són primos entre si y cada uno debe ser un cubo, y por tanto existen x , y y z tales que $2t=x^3$, $t-3s=y^3$ y $t+3s=z^3$, de donde $x^3=y^3+z^3$, con lo que en el caso que p no sea divisible por 3, hemos conseguido el descenso pues no es difícil ver que los valores de x , y y z son menores que los de a , b y c .

Ataquemos ahora el caso en que p es divisible por 3. Tenemos que $p=3r$ y 3 no divide a q . Entonces $2p(p^2+3q^2)=3^2r(3p^2+q^2)$. Es fácil ver que 3^2r y $3p^2+q^2$ son primos entre si y en consecuencia son cubos. Volviendo a aplicar a $3p^2+q^2$ el punto débil del razonamiento de Euler, deben existir números enteros t y s que verifican

$$q=t(t-3s)(t+3s) \text{ y } r=3s(t-s)(t+s)$$

Como $3^2r=3^3s(t-s)(t+s)$ es un cubo, $2s(t-s)(t+s)$ ha de serlo y también en este caso estos factores son primos entre sí, por tanto igual que en el caso anterior existen x , y y z tales que $2t=x^3$, $t-s=y^3$ y $t+s=z^3$, y obtenemos $x^3=y^3+z^3$ donde aplicar el descenso. Con lo cual concluimos la demostración del último teorema de Fermat dada por Euler para el caso $n=3$. La primera prueba conclusiva la da Gauss utilizando propiedades de $\mathbb{Q}(\sqrt{-3})$.

Como anécdota podemos añadir que Euler formuló una conjetura más general: ninguna

potencia enésima puede ser suma de menos de n potencias enésimas, es decir la ecuación

$$a_1^n + a_2^n + \dots + a_r^n = a^n$$

no tiene soluciones en números enteros si $r < n$. Esta ecuación para el caso de dos sumandos se reduce al último teorema de Fermat. Esta conjetura se ha mostrado no ser cierta, pues existen contraejemplos como:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5 \text{ y } 95800^4 + 217519^4 + 414560^4 = 422481^4,$$

el primero hallado por Lander y Parkin en 1966 y el segundo por Elkies y Frye en 1987.

El último teorema para exponente p primo impar

Ahora basta ver el teorema para exponentes primos impares. Veamos por qué. Si existe algún número para el cual el teorema no es cierto, es decir, si existe algún n para el que podemos hallar números enteros a , b y c , tales que $a^n + b^n = c^n$, entonces esta relación también es cierta para cualquier divisor p de n , pues si $n = pq$, podemos escribir $(a^q)^p + (b^q)^p = (c^q)^p$, y por tanto la relación es cierta para p . Ahora tenemos que o bien n es divisible por 4, o bien lo es por un primo impar, como ya hemos visto que el mismo Fermat demostró la imposibilidad para $n=4$, en todo caso el divisor de n debe ser un primo impar. Por tanto, para demostrar el teorema no hay pérdida de generalidad si se supone que el exponente es un número primo impar.

No es hasta 1825, en que Legendre y Dirichlet dan una demostración de forma independiente para el caso $n=5$ y en 1839, Lamé la da para $n=7$. Estas demostraciones son muy artificiosas y los argumentos que en ellas se utilizan de una enorme complejidad, siendo para cada caso diferentes. De hecho, en la carta a Goldbach, antes citada, Euler ya pone de manifiesto que su demostración para el caso $n=3$ difiere en gran manera de la dada por Fermat para las cuartas potencias y que por tanto una solución global parece ha de ser de una gran dificultad.

A mediados de la década 1840-1850, de forma independiente Lamé y Kummer, se dan cuenta de que la causa de que al crecer n aumente la dificultad se halla en que uno de los factores en la descomposición de $a^n + b^n$ tiene grado creciente. Entonces consideran la posibilidad de descomponer la expresión de forma completa en factores lineales, introduciendo un número

complejo tal que $z^n=1$, es decir, z es una raíz enésima de la unidad, y obteniendo la siguiente factorización:

$$a^n + b^n = (a+b)(a+zb)(a+z^2b)\dots(a+z^{n-1}b) = c^n$$

De hecho Lamé creía estar a un paso de hallar una prueba general del teorema. Ésta se basaba en el hecho de que para los enteros ciclotómicos, los números que se obtienen al introducir z , verificaran el teorema de unicidad de la descomposición en números primos de forma análoga al que verifican los números enteros. Precisamente Kummer se percató de que esto no era cierto. Vio que en algunos dominios de enteros ciclotómicos los conceptos de número irreducible y de número primo, que en los enteros habituales coinciden, no son equivalentes.

De hecho la definición que usualmente damos de número primo, que sólo sea divisible por él mismo y por la unidad, corresponde a la de elemento irreducible, que en este caso decimos, que cualquier posible factorización del elemento en producto de dos uno de ellos ha de ser una unidad. Mientras que la propiedad que a nosotros nos interesa de un número primo, es decir, que si divide a un producto ha de dividir a uno de los factores, ésta corresponde a la propia definición de número primo. Se demuestra fácilmente que un número primo siempre es irreducible, pero hay ejemplos de que el recíproco no es cierto.

Fueron todas estas cuestiones las que obligaron a Kummer a introducir los conceptos de número ideal y primo regular, dando una demostración del teorema para los primos regulares. De hecho solo hay tres primos no regulares (37, 59 y 67) menores que 100, y por tanto Kummer da respuesta al problema para todos los números menores que 100, pues posteriormente trató éstos de forma separada. Además, Kummer conjeturó que solo habría un número finito de primos irregulares (lo que habría reducido el problema a tratar solo éstos), pero posteriormente se percató de la falsedad de este hecho. Posteriormente se ha demostrado que existe una infinidad de primos irregulares, pero en cambio, queda aún como problema abierto si el conjunto de primos regulares es infinito.

Por fin una solución!. Por fin?... Emoción hasta el último instante

Es preciso hacer notar que la historia de la resolución del último teorema de Fermat también ha sido apasionante. Amigos y colegas sabedores de mi gran afición en este problema me han suministrado gran cantidad de recortes de prensa

con la noticia de que alguien reclamaba la gloria de su solución, nunca después confirmada. De todas formas parece que por fin podemos anunciar que realmente se ha encontrado la preciada solución, aunque también en este caso hemos tenido que sufrir.

El profesor de origen inglés Andrew Wiles de la Universitat de Princeton, en el transcurso de unas conferencias en Cambridge, a finales de junio de 1993, anunció que había dado solución al problema. Parecía que de esta forma se cerraba un interrogante que se había mantenido abierto durante más de tres siglos y medio, y que había generado gran cantidad de literatura matemática. Pues bien, el 4 de diciembre de 1993, el profesor Wiles confesaba que su demostración era incompleta y que por tanto el problema continuaba abierto, aunque también manifestó su confianza en poder dar solución a las lagunas aparecidas en un plazo de tiempo razonable. Realmente así ha sido pues, a mediados de diciembre pasado, la prensa informaba de que en la Universidad de Princeton el profesor Andrew Wiles y su equipo celebraban la resolución definitiva del problema.

La demostración del profesor Wiles está basada en los temas más avanzados y de mayor abstracción en el campo de la teoría de los números, como son: las formas modulares, las curvas elípticas y las representaciones de Galois, por lo que existen muy pocos matemáticos que puedan comprender en profundidad su argumentación. Además, ésta tiene una extensión considerable, unas 200 páginas. Por todo esto es posible que la comunidad matemática tendrá aún que esperar un cierto tiempo antes de que se sepa con seguridad si todos sus argumentos son correctos.

De hecho, hasta la aparición de la demostración del profesor Wiles, podríamos decir que el último teorema de Fermat se había prácticamente demostrado, dado que se sabía era cierto para todo número dentro de los límites computacionales. Pues Inkeri, en 1953, había demostrado que en caso de que se hallara un n para el que se verificara la igualdad, los valores de a , b y c , serían tan grandes que el universo no sería lo suficientemente grande para poder escribir los números que darían el contraejemplo al teorema, y además en 1987 Tanner y Wagstaff habían verificado el teorema para todo $n < 150000$, y en junio de 1993 se había demostrado para todo $n < 4000000$. Pero para que el teorema pudiera ser considerado como tal, precisamente faltaba una prueba que nos diera la certeza de

que no podía existir ningún número n , fuera cual fuera su magnitud, para el que la ecuación (1) se verificara, y no hubiéramos de depender pura y exclusivamente de suposiciones, por más plausibles que éstas fueran. También, en este contexto se debe valorar la importancia de la solución dada por Andrew Wiles.

Bibliografía

BAKER, A. 1986. Breve introducción a la teoría de números. Madrid. Alianza Editorial.

BEILER, A. H. 1966. Recreations in the theory of numbers. New York. Dover.

BELL, E. T. 1949. Historia de las matemáticas. México. Fondo de cultura económica.

BOYER, C. B. 1986. Historia de la matemática. Madrid. Alianza Editorial.

DUDLEY, U. 1978. Elementary Number Theory. San Francisco. W. H. Freeman and Company.

EDWARDS, H. M. 1977. Fermat's Last Theorem. New York. Springer-Verlag.

GRAHAM, R.L.; KNUTH, D.E.; PATASHNIK, O. 1989. Concrete Mathematics. New York. Addison-Wesley.

REY PASTOR, J.; BABINI, J. 1985. Historia de la matemática. Barcelona. Gedisa.

SERRES, M. 1991. Historia de las ciencias. Madrid. Cátedra.

WEIL, A. 1987. Number Theory: An approach through history from Hammurapi to Legendre. Boston. Birkhäuser.