Anuario del Centro de la Universidad Nacional de Educación a Distancia en Calatayud.
N.º 21, pp. 153-171, 2015

Apuntes sobre una de las más importante demostraciones de la historia de las matemáticas: EL ÚLTIMO TEOREMA DE FERMAT

Andrés MARTÍN SÁNCHEZ
Estudiante de Grado en la Facultad de Matemáticas de la UNED

Abstract

Se presentan en este artículo unos apuntes sobre una de las más importantes demostraciones en la Historia de las Matemáticas y las razones de su importancia, revisando a través del mismo, alguna de la terminología utilizada en las asignaturas de Lenguaje Matemático, Matemática Discreta e Historia de las Matemáticas del Grado de Matemáticas. Finalmente, se presenta a modo de cierre un cuadro de elaboración propia, en el que se ilustra la demostración del Último Teorema de Fermat mostrando la conexión entre varias ramas de las Matemáticas y su evolución histórica.

Palabras clave

Teorema, conjetura matemática, Pierre de Fermat, demostración matemática, Andrew Wiles, el Último Teorema de Fermat, Matemática Discreta, Historia de las Matemáticas, ramas de las matemáticas.

INTRODUCCIÓN

El tema elegido para este artículo se refiere a uno de los más importantes teoremas en Matemáticas, el proceso de su demostración y las razones de su importancia histórica[1].

En el excelente libro de Simon Singh [SIN], podemos encontrar la siguiente cita en forma de grafiti, que aparece en el Metro de Nueva York de la Octava Avenida:

"$x^n+y^n=z^n$: No tiene solución

He descubierto una demostración de esta proposición realmente maravillosa, pero no la puedo desarrollar, porque mi metro está a punto de llegar".

Esta cita del metro de Nueva York, cierta o no, parafrasea la más ilustre del matemático (y abogado) del siglo XVII Pierre de Fermat que escribiera al margen de una edición de la Aritmética de Diofanto y cuya prueba se debe a Andrew Wiles tres siglos después.

En el desarrollo de este artículo, pretendemos razonar las respuestas a los siguientes **interrogantes**:

- ¿Qué diferencia hay entre un teorema y una conjetura? ¿Realmente fue **Pierre de Fermat** tan insigne matemático, como para que una afirmación suya tan falta de pruebas como la expresada en el margen de ese libro, haya tenido en vilo a la comunidad matemática durante tres siglos?
- ¿Qué tiene que ver Andrew Wiles, matemático del siglo XXI, con la **civilización griega** de hace dos milenios? ¿Y con el **siglo XVII**?
- ¿Podemos considerar a Andrew Wiles un adelantado al movimiento de la **globalización** del siglo XXI?
- ¿Qué es una demostración en matemáticas? ¿En qué se basa la demostración del Último Teorema de Fermat?
- Finalmente, ¿está justificada la fama del Último Teorema de Fermat como uno de los más importantes de la Historia de las Matemáticas?

DESARROLLO

1. Sobre teoremas y conjeturas matemáticas: Pierre de Fermat

Un **teorema** en matemáticas es una afirmación sobre una verdad matemática, que precisa demostración. En caso de que no se conozca demostración, pero tampoco se haya probado lo contrario, la afirmación tiene categoría de **conjetura**.

---

1. Para la elaboración de un artículo de un tema de tanta profundidad matemática como es el que ocupa el presente trabajo, seguiremos el proceder que leemos en [ABA]:"El método científico que utilicé fue el de entender, copiar y pegar. No hay nada original mío. Utilicé el material que me iba pasando por las manos y fui poniéndolo en orden para entenderlo. Me puse una condición: no escribir nada (no copiar nada, sería más exacto) si no lo entendía. Lo propio, por tanto, es la manera de cortar y pegar que he seguido. Y si se quiere, la forma de ordenarlo. Nada más…Lo único original eran los comentarios que iba poniendo, cuando al cabo de unos cuantos apuntes, me parecía que ya tenía una opinión formada sobre aquello."

Quizá el teorema más conocido en Matemáticas sea el **teorema de Pitágoras**, que establece que en todo triángulo rectángulo, la suma de los cuadrados de los catetos es igual al cuadrado de la hipotenusa. Del teorema de Pitágoras, se conocen aproximadamente mil demostraciones, una de ellas elaborada por un presidente de los Estados Unidos.

Una conjetura ilustre, que ha ocupado la mente de la comunidad matemática durante varios siglos es la **conjetura de Goldbach**. Su enunciado es bien sencillo: "Todo número par mayor que dos puede escribirse como suma de dos números primos".

A pesar de su aparente simplicidad, este resultado aún no ha sido probado, siendo considerado incluso como el problema más difícil en la historia de las matemáticas.

En relación al teorema que es objeto de este trabajo (el Último Teorema de Fermat), dicho teorema fue enunciado por Fermat en la manera enigmática que se anunció en la introducción y que se detallará en la parte final de esta sección.

Empezamos esta referencia a Fermat con una cita atribuida a él que nos da idea de la fascinación que sentía este ilustre personaje por las matemáticas:

"He encontrado gran número de teoremas extraordinariamente bellos"

Veamos si esta fascinación se corresponde con la atribución que se le hace como el creador de la moderna Teoría de Números, o a la de un erudito generalista aficionado a la correspondencia con sus colegas de conjeturas sin pruebas.

En el libro de Eric Temple [Tem] encontramos los siguientes logros en la vida de Fermat además de los hitos en la teoría de Números que luego detallaremos:

- Elaboró la Geometría Analítica junto con Descartes, pero independientemente de él.
- Participó también con Pascal en la creación de la teoría matemática de la probabilidad.
- Sus conocimientos de las principales lenguas europeas y de la literatura de la Europa continental eran muy grandes y completos, y la filología griega y latina le son deudoras de diversas e importantes correcciones.
- Fermat reconstruye los Lugares planos de Apolonio y traduce la Aritmética de Diofanto.

En cuanto a la Teoría de Números, Fermat formuló sin demostrar lo que se conoce como el Pequeño Teorema de Fermat en que el matemático dio una vez más muestra de su inclinación al secretismo.

En efecto tal como leemos en [Bur], en la correspondencia con otro matemático de su época, Frénicle de Bessy, escribe en 1640 en relación a dicho teorema: "Te mandaría la demostración, si no temiera que esta demostración fuese demasiado larga".

Nos planteamos los siguientes interrogantes:

- ¿Realmente era larga esta demostración, o ese teorema era conjetura, por no tener demostración?
- ¿Era Fermat un aficionado tal como se sugiere en algunas partes del libro de [Tem] o realmente sus conjeturas y teoremas eran las propias de un gran matemático?

Para contestar estas preguntas, vamos a ver la evolución histórica de dicho teorema —el Pequeño Teorema de Fermat—. Parece ser que pasaron 100 años antes de que se publicara la primera demostración del Pequeño Teorema debida a Euler en 1736, aunque Leibniz había dejado la misma demostración en un manuscrito de 1683 que nunca se publicó. Así pues, al menos en este caso, la formulación de Fermat era consistente como lo prueba la demostración posterior.

A continuación, se enuncia dicho teorema y su correspondiente demostración.

Pequeño Teorema de Fermat:

Sea p un número primo y supongamos que $p \nmid a$.

Entonces $a^{p-1} \equiv 1 \pmod p$.

Demostración

Consideremos el conjunto {a, 2a, 3a, …, (p-1)a} de los primeros p-1 múltiplos positivos de a. En primer lugar, no hay dos de estos números que sean congruentes entre sí módulo p, pues si fuesen $ra \equiv sa$ con $1 \le r < s \le p-1$, como además $p \nmid a$, por la propiedad cancelativa de las congruencias sería $r \equiv s \pmod p$, lo cual es imposible, pues $|r-s| \le p-2$. Además, ninguno de los enteros del citado conjunto es congruente con cero módulo p, pues si fuese $ra \equiv 0 \pmod p$ para algún $r \in \{1, \ldots, p-1\}$, entonces $p \mid ra$, cuestión imposible pues p es primo y p no divide a ninguno de los enteros r y a. De esta manera, se deduce que cada uno de los enteros a, 2a, 3a, …, (p-1)a es congruente con uno y sólo uno de los enteros 1, 2, ..., p-1. Si ahora se multiplican todas estas congruencias miembro a miembro, se tiene que

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot a(p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$$

Es decir,

$$a^{p-1}(p-1)!\ (p-1)!\ (\mathrm{mod}\ p).$$

Para terminar, obsérvese que, como p no es divisor de (p-1)!, y nuevamente aplicando la propiedad cancelativa, se deduce que $a^{p-1} \equiv 1 \pmod p$, tal y como pretendíamos demostrar.

Veamos ahora un caso, sin embargo en que sus conjeturas fallaron. En [BUR] encontramos la historia de los primos de Fermat. Nada que ver con posibles relaciones consanguíneas, los **primos de Fermat** se refieren a los números de Fermat que son primos, siendo dichos números de Fermat los enteros de la forma, $F^n = 2^{2^n} + 1 \quad n \ge 0$. Fermat observó que todos los enteros $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65537$ eran primos y expresó su convicción de que F_n era primo para cada valor de n. De hecho, en su correspondencia con Mersenne, anunció confidencialmente: "He encontrado que los números de la forma $2^{2^n}+1$ son siempre números primos". Sin embargo, en correspondencias posteriores, Fermat lamentaba su inhabilidad para encontrar la demostración a esta conjetura. En este caso, sin embargo, al contrario que en el pequeño teorema de Fermat, su conjetura se resolvió negativamente en 1732 cuando Euler descubrió que F_5 era divisible por 641. Actualmente se desconoce si hay infinitos primos de Fermat o siquiera si hay alguno por encima de F_4. Actualmente la

conjetura más plausible es que los números de Fermat por encima de F_4 sean todos compuestos. No parece pues que en este caso Fermat haya acertado con su conjetura.

Llegamos ahora a la formulación de su famoso teorema, el Último **Teorema de Fermat** y su famosa anotación en la edición de Bachet de la Aritmética de Diofanto.

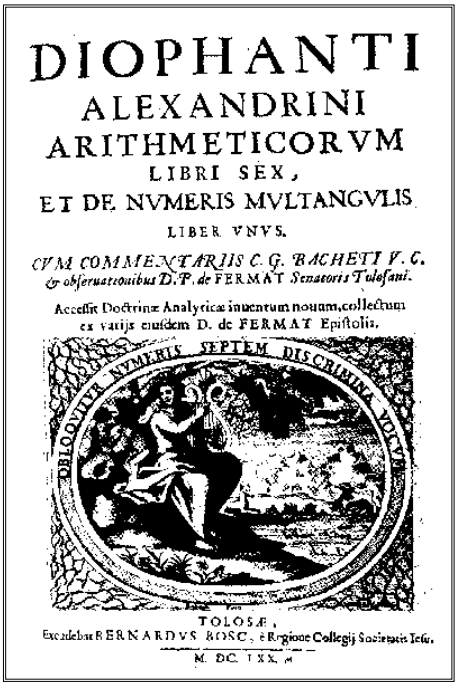

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT Senatoris Tolosani.
Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiuſdem D. de FERMAT Epiſtolis.
TOLOSÆ,
M. DC. LXX.

Figura 1. Edición de Bachet de la Aritmética de Diofanto

Dicho teorema ha ocupado a los matemáticos durante 300 años y su demostración finalmente la realizó Andrew Wiles hace poco más de una década. El enunciado de este teorema es bien sencillo, comprensible incluso para personas sin una profunda formación matemática:

$x^n+y^n=z^n$ con n>2 no tiene solución para x,y, z naturales.

La anotación que aparece en la edición de la obra de Diofanto lleva el sello de Fermat: "Por el contrario, es imposible dividir un cubo en dos cubos, una cuarta potencia en dos cuartas potencias y, en general, una potencia cualquiera de grado superior al segundo, en dos potencias del mismo grado. He descubierto una demostración verdaderamente admirable [de este teorema general] pero esta margen es muy pequeño para contenerla".

En el caso de n=2, la fórmula se verifica en el caso de las ternas pitagóricas, es decir las ternas de enteros que verifican el teorema de Pitágoras. Por ejemplo (3,4,5) es una terna pitagórica, que verifica el teorema de Pitágoras ($3^2+4^2=5^2$), considerando 3 y 4 las longitudes de los catetos y 5 la de la hipotenusa. Pero, ¿es cierto como afirma Fermat que esto no puede cumplirse para n>2?

La dudas que se pudieran plantear aquí (si no supiéramos nada del posterior desarrollo del teorema como lo conocemos ahora), de lo expuesto en relación con el gusto por las conjeturas de Fermat es:

- ¿Realmente Fermat tenía una prueba de este teorema?
- Si no la tuviera, ¿hemos de considerar la conjetura lo suficientemente válida como para dedicar el esfuerzo de la comunidad matemática a su demostración, como finalmente se logró demostrar en sentido positivo para su pequeño teorema?
- Por el contrario ¿tendrá esta conjetura una demostración en sentido negativo, contradiciendo las intuiciones de Fermat sobre el teorema?
- Lo que es peor ¿y si no se lograra demostrar esta conjetura en sentido positivo o negativo nunca porque simplemente no es demostrable?

En este punto, buscamos la ayuda de los que escriben y conocen del tema y encontramos la siguiente respuesta en el libro de Eric Temple sobre los grandes matemáticos de la historia [TEM]:

"Es difícil o quizá imposible saber por qué algunos teoremas en Aritmética se consideran importantes, mientras otros igualmente difíciles de probar son considerados triviales. Un criterio, aunque no necesariamente concluyente, es que el teorema pueda usarse en otros campos de la Matemática. Otro criterio es el de que sugiera investigaciones en Aritmética o en Matemática en general, y un tercer criterio es que en algún aspecto sea universal. El teorema de Fermat justamente satisface todas esas algo arbitrarias exigencias: es de uso indispensable en muchas partes de la Matemática, incluyendo la teoría de grupos que, a su vez, es la raíz de la teoría de ecuaciones algebraicas; ha sugerido muchas investigaciones, entre las cuales puede mencionarse como un ejemplo importante todo el estudio de las raíces primitivas; finalmente, es universal, en el sentido, de que juzga una propiedad de todos los números naturales, esas propiedades generales son extremadamente difíciles de encontrar y se conocen muy pocos casos"

Así pues, en relación al primer interrogante de la introducción acerca de la credibilidad de Pierre de Fermat en relación al Teorema que lleva su nombre, concluimos que tenía algo entre manos cuando escribió esa nota al margen del manuscrito de Diofanto y que los esfuerzos de la comunidad matemática en demostrar su conjetura se fundamentan en una base sólida.

2. Sobre la historia de las matemáticas y la aritmética de Diofanto

A Diofanto de Alejandría [s.III dC] se le ha considerado como el padre del Álgebra, aunque tal como encontramos en [BOY] esta afirmación es necesario matizarla, en el sentido de que el objeto de análisis de su obra fundamental (la Aritmética) forma parte hoy generalmente de los cursos de Teoría de Números más bien que del álgebra elemental.

En cualquier caso, a Diofanto se le debe el apellido de un tipo especial de ecuaciones algebraicas, las llamadas ecuaciones diofánticas, que son aquéllas con una o varias indeterminadas con coeficientes enteros, de las que sólo se desean soluciones enteras, en particular las naturales.

La ecuación de Fermat, ($x^n+y^n=z^n$, n>2), es un caso particular de ecuación diofántica sin solución. Consideremos n=2 y veamos como se demuestra en [BUR] la existencia y forma de las soluciones de esta otra ecuación diofántica.

Teorema:

Consideremos la ecuación pitagórica $x^2+y^2=z^2$. Las soluciones naturales (x,y,z) de dicha ecuación tales que mcd (x,y,z)= 1 son:

$$\begin{cases} x=2\lambda\mu \\ y=\lambda^2-\mu^2 \\ z=\lambda^2+\mu^2 \end{cases} \quad \text{o} \quad \begin{cases} x=\lambda^2-\mu^2 \\ y=2\lambda\mu \\ z=\lambda^2+\mu^2 \end{cases}$$

donde λ y μ son dos naturales de distinta paridad tales que $\lambda > \mu$ y mcd $(\lambda, \mu)=1$.

Demostración

Sea (x,y,z)una solución de la ecuación $x^2+y^2=z^2$ tal que mcd (x,y,z)=1. Se deduce inmediatamente que mcd (x,y)=1, pues si d es divisor natural de x e y, entonces d^2 es divisor de x^2 e y^2, luego también lo es de $x^2+y^2=z^2$, así es que d también divide a z, por lo que d=1.Como es mcd (x,y)=1, x o y son impares, así es que suponemos que lo es y (si el impar fuese x obtendríamos, intercambiando los papeles de x e y, la otra solución). Si x también fuese impar serían $x= 2m-1$, $y=2n-1$ para ciertos m,n. Entonces:

$$z^2=x^2+y^2=(2m-1)^2+(2n-1)^2=4(m^2+n^2-m-n)+2$$

lo cual es absurdo porque cualquier cuadrado es congruente con 0 o 1 módulo 4.

Por tanto, x es par y también lo es x^2, luego $z^2=x^2+y^2$ es impar y z es impar. Así,

$$x^2=z^2-y^2=(z+y)(z-y)$$

donde $z+y$ y $z-y$ son pares. Existen, por tanto, u,v,w tales que $z+y=2u$, $z-y=2v$, $x=2w$ y entonces

$$4w^2=x^2=(z+y)(z-y)=2u.2v=4w, \text{ luego } w^2=uv.$$

Vamos a comprobar ahora que u y v son coprimos. Si fuese mcd (u,v)≠1, existiría algún número primo p divisor de u y v, con lo que p también dividiría a $u+v=1/2(2u+2v)=1/2(z+y+z-y)=z$ y $u-v=1/2(2u-2v)=1/2(z+y-z+y)=y$ y por tanto p sería divisor de $z^2-y^2=x^2$, lo que, por ser p primo, conduce a que p es divisor de x, pero esto no puede ser si mcd (x,y)=1. Así pues, u y v son coprimos y su producto es un cuadrado (w^2), luego ambos son cuadrados y existen por tanto λ y μ tales que $u=\lambda^2$, $v=\mu^2$, de manera que

$$z=u+v=\lambda^2+\mu^2, \quad y=u-v=\lambda^2-\mu^2.$$

Para obtener la expresión de x, como $w^2=uv=\lambda^2\mu^2$ y w, λ y μ son números naturales, se tiene que $w=\lambda\mu$, así es que

$$x=2w=2\lambda\mu.$$

Como $y=\lambda^2-\mu^2$ es natural resulta $\lambda > \mu$, así es que sólo resta comprobar que

mcd(λ,μ)=*1* son de distinta paridad. La primera se deduce de 1=mcd(u,v)= =mcd(λ^2,μ^2)=*[mcd(λ, μ)]*^{2} y para la segunda, si λ y μ fuesen de igual paridad también lo serían λ^2 *y* μ^2, así es que *z*= λ^2 + μ^2 *e y*= λ^2 - μ^2 serían ambos pares, por lo que $x^2 = z^2 - y^2$ y por tanto, x, serían pares igualmente. Pero esto es imposible por ser mcd (x,y,z)=1. La comprobación de que la terna (x,y,z) obtenida es la solución de la ecuación es inmediata

Contestando a la segunda pregunta de los preliminares hemos establecido la relación de Andrew Wiles con la civilización griega de hace dos milenios a través de la figura de Diofanto de Alejandría, al cual se debe el apellido de las llamadas ecuaciones diofánticas, que son aquellas ecuaciones en varias incógnitas de las que sólo se desean las soluciones enteras, y es que la ecuación del teorema de Fermat demostrada por Wiles es un caso particular de ecuación diofántica.

3. Sobre las ramas en matemáticas y la conjetura Taniyama-Shimura

Según la Sociedad Estadounidense de Matemáticas hay 5000 ramas distintas de Matemáticas en las que se distinguen cuatro objetos de estudios básicos: la cantidad, la estructura, el espacio y el cambio, que se corresponden con la aritmética, el álgebra, la geometría y el análisis.

Traemos aesta sección, la descripción de la **conjetura de Taniyama-Shimura** en relación a las curvas elípticas y modulares. En apariencia, estos conceptos no tienen nada que ver con la demostración de un teorema clásico de la Teoría de Números como es el del teorema de Fermat, pero como luego se verá, esta hipótesis es básica en la demostración del teorema. Pasaremos a describir las curvas elípticas, a continuación las formas modulares y seguidamente la ligazón entre ambas a través de la hipótesis de Taniyama-Shimura. Se finalizará este apartado con la trágica parte de la historia de la conjetura.

3.1. Las curvas elípticas

El término de **curva elíptica** se aplica a cualquier ecuación de la forma

$$y^2=x^3+ax^2+bx+c$$

donde a, b y c son números enteros.

El desafío de las curvas elípticas, al igual que en el último teorema de Fermat, es descubrir si tienen soluciones con números enteros, y en tal caso, cuántas.

Las curvas elípticas tienen la particularidad de que con sólo cambiar los valores de a, b y c en la ecuación de la curva elíptica general, se genera una variedad infinita de ecuaciones susceptibles de solución.

En [Sin] encontramos como las curvas elípticas fueron estudiadas en un principio por los antiguos matemáticos griegos, como Diofanto, que dedicó buena parte de su Aritmética a investigar sus propiedades. El estudio de estas propiedades ha sido objeto de matemáticos como Fermat y el propio Wiles.

Encontrar la cantidad exacta de soluciones para las ecuaciones que Wiles estudiaba era una labor tan difícil que el único modo de progresar pasaba por simplificar el problema. Una manera de hacerlo es buscar soluciones comprendidas en

un espacio finito de números mediante la llamada **aritmética de los relojes**. Esta aritmética consiste en considerar un espacio de números limitado tal como el que tenemos en un reloj. La suma de 1 y 12 que en la aritmética tradicional da 13, en un reloj convencional da 1 nuevamente. No sólo la suma, sino también la multiplicación es posible en esta aritmética de manera que trabajando con esta aritmética es relativamente fácil hallar todas las soluciones posibles de una ecuación elíptica para la aritmética de un reloj determinado.

Por ejemplo, si se trabaja en el reloj de cinco números, es sencillo elaborar la relación completa de soluciones de la ecuación

$$x^3-x^2=y^2+y$$

Las soluciones son:

$$x=0,\ y=0$$
$$x=0,\ y=4$$
$$x=1,\ y=0$$
$$x=1,\ y=4$$

Aunque alguna de estas soluciones no sería válida en la aritmética normal, todas son aceptables en la aritmética del reloj de cinco números.

Por ejemplo, la cuarta solución, x=1, y=4, funciona de este modo

$$x^3-x^2=y^2+y$$
$$1^3-1^2=4^2+4$$
$$0=20$$

Pero el 20 equivale al 0 en esta aritmética, pues el resto que queda al dividir 20 entre 5 es 0.

Como no es posible hallar la totalidad de soluciones para una curva elíptica si se trabaja en un espacio infinito, los matemáticos se plantearon el cálculo de la cantidad de soluciones en cada aritmética de relojes posible. Para el ejemplo anterior de curva elíptica, el número de soluciones en el reloj de cinco números es cuatro y se representa como $E_5=4$. Se puede hallar el número de soluciones en otras aritméticas y los resultados se resumen en forma de lista, dando el número total de soluciones en cada reloj, llamando a esta lista la "serie L" de la curva elíptica. Por claridad, en [SIN] se utiliza el termino "serie E" y se avanza en la descripción de dichas series escribiendo que la **serie E** contiene una gran cantidad de información acerca de la curva elíptica de la que procede. Es lo que se llama el ADN de las ecuaciones elípticas.

3.2. Las formas modulares

Las formas **modulares** son objetos definidos en el espacio complejo (cada punto queda determinado por cuatro coordenadas) con un número ilimitado de simetrías. En la Wikipedia leemos que:

Definición. Una forma modular es una función analítica $f:H \to C$ del semiplano superior $H = \{x+ iy : y>0\}$ en los complejos C, tal que f satisfaga ciertas condiciones de simetría (entre ellas $f(x) = f(x+N)$ para todo x y algún entero N fijo) y una condición de crecimiento (holomorficidad en el punto en el infinito).

Por lo tanto la teoría de las formas modulares pertenece al análisis complejo.

Tal como podemos leer en [SIN], por desgracia, dibujar e incluso imaginar, una forma modular es imposible y a continuación trata de explicar por qué. Leemos así que en el caso de un cuadrado estamos en presencia de un objeto de dos dimensiones, con un espacio definido por los ejes x e y. Una forma modular también está definida por dos ejes, pero los dos son complejos, por lo que este espacio es tetradimensional (x_r, x_i, y_r,y_i).

Este espacio de cuatro dimensiones es llamado **espacio hiperbólico** y es difícil de entender para los humanos que viven en un mundo de tres dimensiones, pero el espacio hiperbólico de cuatro dimensiones es un concepto matemáticamente válido, y es esta dimensión lo que proporciona a las formas modulares un nivel tan elevado de simetría.

Y aquí, en [SIN], se trae la representación de Escher en su obra Circle Limit IV del mundo en el espacio hiperbólico bidimensional tal como se reproduce en la siguiente figura.

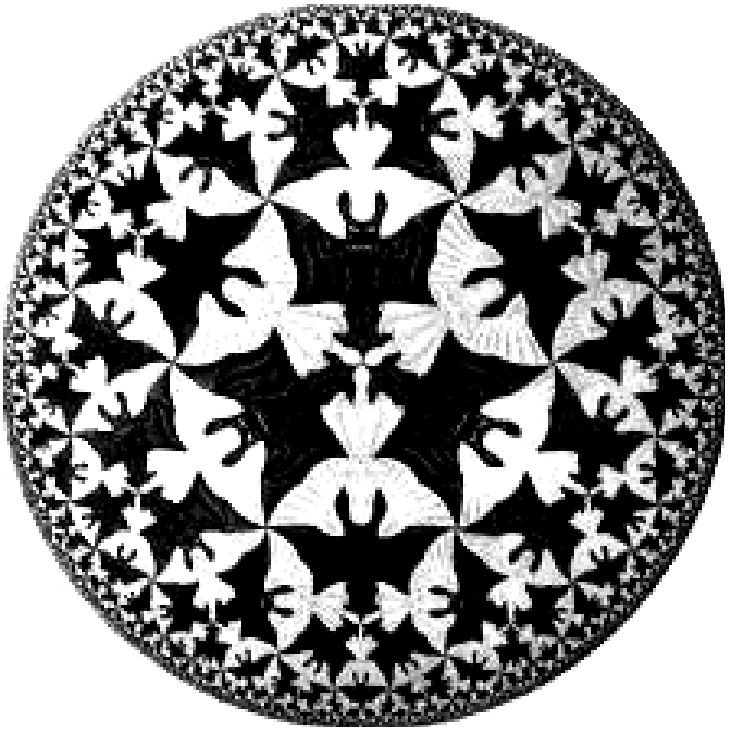


Figura 2. "Cicle Limit IV" de Escher

En el plano hiperbólico real, los murciélagos y los ángeles serían todos del mismo tamaño, y la repetición sería indicativa del alto grado de simetría. Aunque parte de la simetría se puede apreciar en la página bidimensional, existe una distorsión creciente hacia el borde de la pintura. Parece que sí nos hemos aproximado a una representación siquiera intuitiva y elegante del mundo hiperbólico en contra de lo que el mismo autor lamentaba tan sólo unas líneas antes. A nosotros nos basta para hacernos una idea geométrica de lo que es el mundo hiperbólico.

A posteriori, se describe en [SIN] lo que él llama el ADN de las formas modulares por analogía a lo que había considerado como ADN de las formas elípticas (las series E). Este ADN no es otro que las **series M**. Las series M se definen a partir de lo que en [SIN] se llaman ingredientes que componen una forma modular y cuya cantidad es lo que diferencia cada forma modular. Así cada forma modular particular puede contener una medida del ingrediente uno (M_1=1), tres medidas del ingrediente dos (M_2=3), dos medidas del ingrediente tres (M_3=2), etc..

Parece claro, donde el autor [SIN] nos quiere llevar con esta notación, y que no es otra cosa que la evidencia de una analogía entre las formas modulares y las curvas elípticas, al menos formalmente.

3.3. La conjetura de Taniyama-Shimura

La conjetura de Taniyama- Shimura tal como está formulada en la Wikipedia afirma lo siguiente:

Conjetura Taniyama-Shimura:

Para todo parámetro t real o complejo, existen formas modulares f y g tales que $x=f(t)$, $y = g(t)$ son una solución de la ecuación

$$y^2=x^3+ax^2+bx+c$$

Es decir, la conjetura de Taniyama-Shimura relaciona una forma modular con una ecuación elíptica a través de sus respectivas series M y E. El ADN matemático que construye cada una de esas dos entidades es exactamente el mismo.

3.4 Un tinte trágico

La conjetura Taniyama-Shimura fue inicialmente propuesta por Yutaka Taniyama en 1955 y desarrollada posteriormente por Taniyama junto a Goro Shimura y por André Weil. La historia de elaboración de esta conjetura tiene una nota trágica en el sucidio de uno de sus autores, Taniyama. En el MacTutor encontramos esta nota de Taniyama explicando su suicidio:

"Until yesterday I have had no definite intention of killing myself. But more than a few must have noticed I have been tired both physically and mentally. As to the cause of my suicide, I don't quite understand it myself, but it is not the result of a particular incident, nor of a specific matter. Merely may I say, I am in the frame of mind that I lost confidence in my future. There may be some to whom my suicide will be troubling or a blow to a certain degree. I sincerely hope that this incident will cast no dark shadow over the future of that person. At any rate I cannot deny that this is a kind of betrayal, but please excuse it as my last act in my own way, as I have been doing all my life".

Que traducido al castellano quedaría como:

"Hasta ayer no tenía intención definitiva de suicidarme. Pero bastantes habrán notado que he estado cansado tanto física como mentalmente. En cuanto a la causa de mi suicidio, no la entiendo ni yo mismo, pero no es el resultado de ningún incidente particular ni una cuestión específica. Simplemente puedo decir, que estoy en

un estado mental en que he perdido confianza en mi futuro. Habrá alguien para quien mi suicidio puede ser un duro golpe en un cierto grado. Espero sinceramente que este incidente no arroje sombras oscuras sobre el futuro de esta persona. En cierta manera no puedo negar que este incidente es un modo de tración, pero por favor perdónese este mi último acto a mi manera, tal como he venido haciendo toda mi vida.

Un mes después Suzuki, su prometida, también se suicidó dejando una nota que incluía estas frases: " Nos prometimos uno al otro, que no importaba donde fuéremos, nunca nos separaríamos. Ahora que él se ha ido, debo ir también para unirme con él".

Encontramos así en esta fascinante historia de la demostración del teorema de Fermat un suicidio a la japonesa que añade aún más interés si cabe a esta trama.

Aún no sabemos cómo (esto se describirá a continuación), pero si hemos adelantado en este apartado que la fundamentación de la demostración de Andrew Wiles de la conjetura de Fermat de la teoría clásica de números se basa en un enfoque novedoso que relaciona el mundo de la curvas elípticas y las curvas modulares. El enfoque es tan novedoso que sólo ha podido venir de manos de la cultura japonesa.

Relacionando el enfoque oriental dado por la hipótesis de Taniyama-Shimura y el enfoque clásico producto de la historia occidental de las matemáticas de los últimos siglos podemos responder al interrogante de la introducción en sentido positivo y afirmamos que Andrew Wiles sí puede considerarse en cierto modo un estandarte de la globalización en la demostración de su teorema.

4. Sobre las demostraciones en matemáticas: el argumento de Frey

En este apartado nos centraremos en los trabajos que fueron utilizados por Andrew Wiles para la demostración del teorema, pero no detallaremos los numerosos intentos fallidos de grandes matemáticos como Lamé, Legendre, Kummer, entre otros para la demostración del mismo.

Por su parte, sin embargo, en el siglo XIX Euler, demostró la conjetura para **n= 3** y **n=4**, Dirichlet para **n=5** y Lame para **n=7**. Sophie German clasificó en dos casos la resolución del problema llegando a demostrar la conjetura para uno de los casos y todos los **n primos menores que 100** [ACZ]

Los argumentos definitivos que dieron paso a la demostración del teorema de Fermat por parte de Andrew Wiles provienen de la novedosa aportación de Frey de que el teorema de Fermat no es un caso aislado de la Teoría de Números en las matemáticas, sino que estaba relacionado directamente con propiedades fundamentales del espacio.

En [SIN] y [ACZ] encontramos como se fraguaron estos acontecimientos:

4.1. Faltings

En 1983 Faltings demostró la **conjetura de Mordell**. Dicha conjetura establece una conexión entre el número de agujeros en una superficie y el hecho de que una ecuación asociada a las superficie tenga un número finito o infinito de soluciones. Si la superficie de soluciones presentaba dos o más agujeros, entonces la ecuación tenía sólo un número finito de soluciones enteras. Las repercusiones en el último teorema de Fermat fueron inmediatas toda vez que que la ecuación de Fermat para

n mayor que 3 tenía género 2 o más (tenía 2 o más agujeros) por lo que si existían soluciones de enteros para esta ecuación tenían que ser finitas.

Un número finito podía ser cualquier valor entero entre 0, que fue lo que Fermat aseguró, hasta un millón o un billón.

Poco después se demostró que el número de soluciones para la ecuación de Fermat, en caso de existir, disminuía a medida que n aumentaba. Es decir, se probó que el último teorema de Fermat era verdadero "casi siempre". Si existían soluciones para la ecuación (caso en el cual el teorema sería falso) entonces eran pocas y muy distantes entre sí.

Así pues, el estado del último teorema de Fermat en 1983 era el siguiente: se había demostrado que era verdadero para n menor que un millón y para todo n mayor, en caso de existir soluciones, debían ser pocas y cada vez menos numerosas a medida que n aumentase.

Vamos a exponer ahora el argumento que da el vuelco en la historia de demostración del teorema, que no es otro que el argumento de Frey, demostrado más tarde por Ken Ribet.

4.2 Argumento de Frey

El argumento de Frey consistió en suponer que la conjetura de Fermat era falsa, es decir, que existe al menos una solución entera a la ecuación de Fermat

$$x^n+y^n=z^n \text{ con } n>2$$

Reordenando la ecuación Frey llegaba a una expresión de la forma

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

que es en realidad una ecuación elíptica

$$y^2=x^3+ax^2+bx+c$$

haciendo las identificaciones

$$a=A^n-B^n,\ b=0,\ c=-A^nB^n.$$

En otras palabras el argumento de Frey es como sigue:

- Si (y solo si) el último teorema de Fermat es falso, entonces existe la solución elíptica de Frey.
- La ecuación elíptica de Frey es tan extraña que de ninguna manera puede ser modular.
- La conjetura de Taniyama-Shimura asegura que cada ecuación elíptica debe ser modular.
- ¡En consecuencia, la conjetura de Taniyama-Shimura debe ser falsa!

Lo más interesante de este argumento es que puede formularse al revés:

- Si la conjetura de Taniyama-Shimura se puede demostrar cierta, entonces cada ecuación elíptica tiene que ser modular.
- Si cada ecuación elíptica es modular, entonces está prohibida la existencia de la ecuación elíptica de Frey.
- Si la ecuación elíptica de Frey no existe, entonces no puede haber solución a la ecuación de Fermat.
- ¡Entonces el último teorema de Fermat es cierto!

Frey había definido claramente la tarea que había por delante. Los matemáticos demostrarían automáticamente el último teorema de Fermat si eran capaces de probar primero la conjetura de Taniyama-Shimura.

4.3 Ken Ribet

El argumento de Frey era impecable salvo por dos importantes detalles: descansaban sobre dos conjeturas no resueltas, la de Taniyama- Shimura y lo que a partir de entonces se llamó conjetura de Frey, es decir la naturaleza extraña de la curva de Frey. Ken Ribet logró demostrar la conjetura de Frey en 1986. Sólo hacía falta que alguién demostrase la aparentemente imposible conjetura de Shimura y Taniyama. Entonces el último teorema de Fermat pasaría a ser verdadero automáticamente.

En este apartado, se contesta a la penúltima pregunta de la introducción acerca de los antecedentes de la demostración del teorema. Y es que previamente a la contribución de Wiles se había logrado reducir la incertidumbre de la conjetura de Fermat a un número finito de soluciones a través de los trabajos de Frey y se había logrado acotar la demostración del teorema únicamente a la demostración de la conjetura de Taniyama- Shimura gracias a las aportaciones de Frey y Ribet de que ambos problemas eran equivalentes.

5. Sobre la demostración del teorema de Fermat y Andrew Wiles

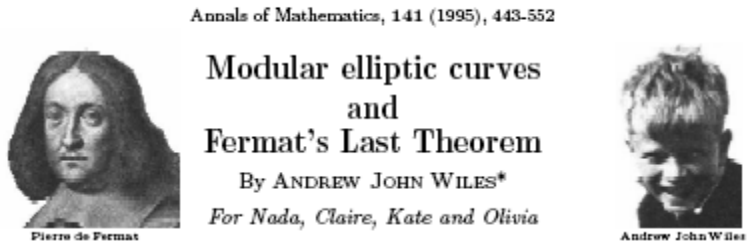
Hemos visto en el anterior apartado como Frey logra ingeniosamente esbozar la transformación de la ecuación de Fermat en la de una curva elíptica, lo que implica la ligazón de las hipótesis de Taniyama-Shimura con la ecuación de Fermat. Anteriormente se había explicado cómo la conjetura de Taniyama-Shimura establece que cada curva elíptica puede asociarse unívocamente con un objeto matemático denominado, la llamada forma modular. El razonamiento de Frey consistía en considerar que si el último teorema de Fermat fuese falso, entonces existiría una curva elíptica tal que no puede asociarse con ninguna forma modular, y por lo tanto la conjetura de Taniyama-Shimura sería falsa. Ken Ribet logra demostrar en 1986 que el esbozo de Frey es válido, de manera que aquel que lograra demostrar la conjetura de Taniyama-Shimura demostraría el último teorema de Fermat.

Andrew Wiles fue quien logró demostrar la conjetura de Taniyama-Shimura y de esta forma lograr su sueño infantil de demostrar el Teorema de Fermat. Para ello utilizó la inducción matemática a partir de una primera correspondencia de un elemento de la sucesión elíptica con otro de la sucesión modular.

De esta manera tal como se describe en [Sin], "por medio de la conjetura de Taniyama-Shimura, Wiles había unificado los mundos elíptico y modular, y al hacerlo había provisto a las matemáticas de un atajo para muchas otras demostraciones; problemas en un dominio podrían ser resueltos por analogía recurriendo a problemas en el dominio paralelo. Problemas clásicos sin resolver de las curvas elípticas, algunos de los cuales se remontan a los antiguos griegos, podrían ser reexaminados usando las herramientas y técnicas modulares disponibles".

Para profundizar en las complejidades de la demostración matemática en la

siguiente figura se ilustra la primera página de las más de 100 páginas de la demostración que se publicó en los Anales de Matemáticas de 1995 y cuyo escrutinio fue objeto de minucioso análisis por un selecto comité experto de insignes matemáticos antes para la validación definitiva de la demostración del teorema.



Annals of Mathematics, 141 (1995), 443-552

Pierre de Fermat

Modular elliptic curves and Fermat's Last Theorem

By Andrew John Wiles*

For Nada, Claire, Kate and Olivia

Andrew John Wiles

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere: cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

- Pierre de Fermat ~ 1637

Abstract. When Andrew John Wiles was 10 years old, he read Eric Temple Bell's *The Last Problem* and was so impressed by it that he decided that he would be the first person to prove Fermat's Last Theorem. This theorem states that there are no nonzero integers a, b, c, n with $n > 2$ such that $a^n + b^n = c^n$. This object of this paper is to prove that all semistable elliptic curves over the set of rational numbers are modular. Fermat's Last Theorem follows as a corollary by virtue of work by Frey, Serre and Ribet.

Introduction

An elliptic curve over $\mathbf{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over $\mathbf{Q}$ with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over $\mathbf{Q}$ is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

*The work on this paper was supported by an NSF grant.

Figura 3. Demostración del teorema de Fermat (Annal of Mathematics)

Responderemos finalmente a la última pregunta de los preliminares acerca de la fama del Último Teorema de Fermat. La respuesta es sí, y así lo justificamos.

Teorema:

Se considera justa la fama del Último Teorema de Fermat y su proceso de demostración como uno de los más importantes de la historia de las matemáticas.

Demostración

Para justificar esta fama nos apoyamos en esta nota que encontramos en [ACZ] sobre el teorema que resume este trabajo (nota que comentamos entre paréntesis con apoyo de la figura): "Lo que resulta interesante del último teorema de Fermat, es que abarca la historia de las matemáticas desde los albores de la civilización hasta nuestro tiempo (flecha verde en figura 4). La solución definitiva del teorema también abarca toda la amplitud de las matemáticas, incluyendo campos que no pertenecen a la teoría de números (cuadro rojo en misma figura): álgebra (cuadro rosa), análisis (cuadro azul), geometría (cuadro azul otra vez) y topología (cuadro rosa otra vez), es decir, prácticamente todas las matemáticas". Además, el teorema une dos concepciones de las matemáticas como son la occidental y oriental y en su demostración encontramos todas las técnicas de resolución de problemas de matemáticas, ya que, la conjetura de Taniyama-Shimura es en realidad una analogía (ver figura), la argumentación de Frey ligando el teorema de Fermat y la conjetura de Taniyama-Shimura se basa en la reducción al absurdo y el procedimiento deductivo (ver figura 4) y la demostración de la conjetura de Taniyama-Shimura por Wiles que permite a su vez la demostración del teorema, se basa en la otra estrategia de resolución de problemas que es el procedimiento inductivo. Parafraseando a Fermat, la demostración de este teorema es realmente maravillosa. Por todo lo cual, se justifica la fama y demostración-desarrollo del Último Teorema de Fermat como uno de los más importantes en la Historia de las Matemáticas.

CONCLUSIONES

A partir de una introducción con interrogantes para la descripción de la demostración del ú**ltimo teorema** Fermat ($x^n+y^n=z^n$ no tiene solución para n>2) por Andrew Wiles:

- Se ha esbozado la figura del autor del teorema, **Pierre de Fermat**, demostrando su otro teorema. Éste y otros **teoremas (y conjeturas**) que se detallan dan muestra de la importancia de este matemático del siglo XVII.
- Se han introducido las ecuaciones diofánticas a través de la figura de **Diofanto de Alejandría**, de las que el último teorema es un caso particular. Se ha demostrado la ecuación diofántica equivalente al teorema de Fermat para n =2, ligando un teorema demostrado en el siglo XX con una figura **histórica de las Matemática**s de dos milenios antes.

- Seguidamente, se ha **formulado la conjetura de Taniyama-Shimura** relacionando las formas modulares de las funciones complejas con el estudio de las curvas elípticas, estableciendo puentes entre dos **ramas** hasta entonces desconexas de las matemáticas
- A continuación, se ha expuesto el ingenioso **argumento de Frey** que relaciona el teorema de Fermat con las curvas elípticas y la conjetura de Taniyama-Shimura, de modo que si alguien es capaz de demostrar esta conjetura, también estaría resuelto el último teorema de Fermat. Ken Ribet demostró la conjetura de Frey base del argumento.
- Acto seguido, se ha presentado la **prueba de Andrew Wiles** del último teorema, es decir la demostración de la conjetura de **Taniyama-Shimura.**
- En el último apartado, se justifica la fama del Último Teorema de Fermat, en base a la revisión histórica que se hace en el artículo de la Teoría de Números, a las estrategias de resolución de problemas presentes en la demostración, y la importancia del teorema dentro de la Historia de las Matemáticas.

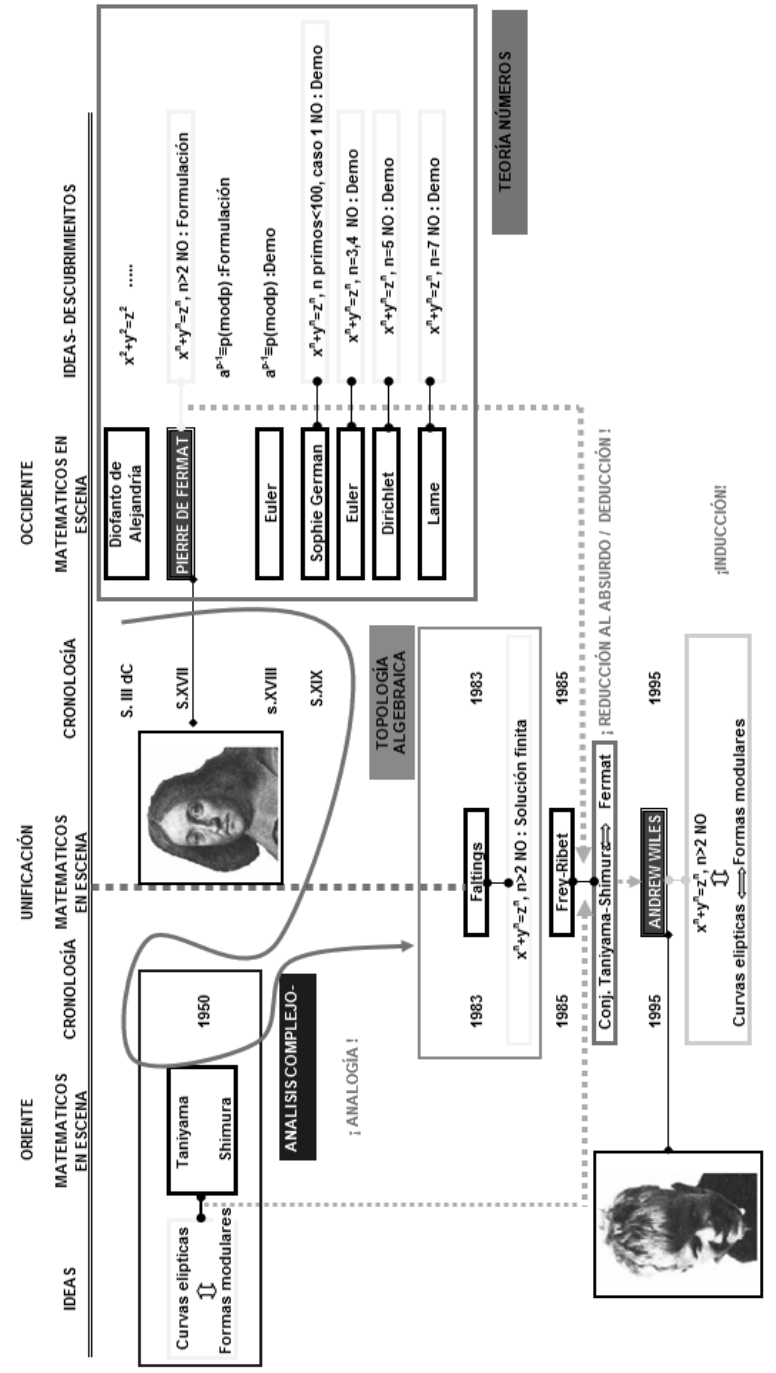


Figura 4. El último teorema de Fermat. Conexión histórica y con otras ramas de las matemáticas (elaboración propia)

BIBLIOGRAFÍA

a) General

[ABA] ABADÍA, LEOPOLDO. *La crisis ninja y otros misterios de la economía actual*. Espasa, Barcelona, 2003.

[ACZ] ACZEL, AMIR D. *El último teorema de Fermat. El secreto de un antiguo problema matemático*. Fondo de cultura económica, México, 2003.

[BOY] BOYER, C.B. *Historia de la matemática*. Alianza Editorial, Madrid, 1986.

[BUR] BURTON, DAVID M. *Elementary Number Theory*. McGraw-Hill, New York, 1998.

[SIN] SINGH, SIMON. *Fermats Letzter Satz*. Die abenteuerliche Geschichte eines mathematischen Rätsels. DTV, München, 2007.

[TEM] TEMPLE BELL, ERIC. Grandes Matemáticos. Editorial Losada, 2010

[VER] VERA, FRANCISCO. *20 matemáticos célebres*. www.librosmaravillosos.com

[WIL] WILES, ANDREW JOHN. *Modular elliptic curves and Fermat's Last Theorem*. Annals of Mathematics, 141 (1995), 443-552

b) Paginas web

en.wikipedia.org/wiki/

www-history.mcs.st-and.ac.uk/