TEORIA DE NUMEROS EN EL SIGLO XVIII

ENRIQUE LINES ESCARDO *

El legado de Fermat

A principios del siglo XVIII no existía una rama de la Matemática, que con métodos propios, se ocupara del estudio de las propiedades de los números enteros.

En el conjunto ordenado de los números enteros, las operaciones de suma y multiplicación establecen las reglas de juego de la más pura de las teorías matemáticas que sólo hasta fines del siglo no consiguió tener nombre propio, el de *Teoría de Números.*

No solo no existía una rama del Saber que se ocupara de las propiedades de los números "en sí", prescindiendo de toda otra servidumbre científica, sino que tampoco era presumible que los investigadores se sintieran atraídos a este campo de la Ciencia. El entusiasmo arrollador que con el nuevo Cálculo Infinitesimal había invadido a los círculos matemáticos, y los maravillosos éxitos logrados, no propiciaban una investigación cuyo mayor aliciente era el de un juego estético.

La tradición aritmética de los griegos asimilada por los círculos académicos franceses y potenciada por el genio de Fermat era, a principios del siglo XVIII, lo único con que se podía contar para el recorrido de un largo camino ascendente. Cuando Gauss en 1801, publica sus "Disquisitiones Arithmeticae" se había conseguido transformar esta materia en una ciencia sistemática y bella.

Ciertamente que quienes recogieron el legado de Fermat, se encontraron con una colección de proposiciones no demostradas o solo incompletamente, con afirmaciones no comprobables, con vías de razonamiento que se perdían. Se enunciaban inesperadas propiedades con la precisión de algo que ya ha sido demostrado, pero cuya prueba cuidadosamente se reservaba como reto a otros matemáticos.

El legado de Fermat, como escrito en cifra, para que sólo participaran de él los de un genio semejante, sirvió de acicate para que los grandes se sintieran atraídos, probándose a sí mismos, a la tarea de descubrir y superar lo escondido.

---

* Académico. Prof. Emérito de la Universidad Nacional de Educación a Distancia.

Tal vez sea lo más sorprendente de los papeles de Fermat, el que se haya ido confirmado la certeza de las proposiciones enunciadas (salvo una de menor importancia), demostrándose paso a paso a lo largo de los años, y ordinariamente encuadradas en importantes teorías matemáticas.

Muchas de estas proposiciones están recogidas en las cartas que escribió al P. Mersenne y también a su buen amigo Carcavi. Seguramente las proposiciones que él consideraba más importantes son las que se relacionan en una carta enviada a éste último en 1659, como resumen de los estudios realizados hasta aquella fecha. Ya en una carta a Pascal en 1654, había formulado algunas proposiciones, que luego repetiría en la famosa de Carcavi.

En una conferencia que dimos en este mismo lugar sobre Fermat, presentamos una lista de doce proposiciones, la mayoría enunciadas en la misiva a Carcavi, que constituye una parte notable del legado de Fermat. En ésta dedicaremos amplio espacio al comentario de los trabajos que grandes matemáticos realizaron en el siglo XVIII, para probar las proposiciones enunciadas, que transcribimos a continuación:

1.– "Si p es primo y a no múltiplo de p, se verifica

$$a^{p-1} \equiv 1 \pmod{p}$$ " *(Congruencia de Fermat)*

2.– "Todo número primo de la forma $4k+1$ se puede representar como suma de dos cuadrados, de manera única" *(Teorema de los dos cuadrados).*

3.– "Todo número entero y positivo es suma de cuatro cuadrados de números enteros, entre los que no se excluye el cero" *(Teorema de los cuatro cuadrados).*

4.– "Si d no es cuadrado, la ecuación

$$x^2 - dy^2 = 1 ,$$

tiene infinitas soluciones enteras" *(Ecuación de Fermat)*

5.– "La ecuación

$$x^3 + y^3 = z^3 ,$$

no tiene solución en números enteros positivos".

6.– "La única solución en números enteros de la ecuación

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

es $x = 3,\ y = 5$ "

7.– "Todo número de la forma

$$2^{2^k} + 1 \text{ , es primo"}$$

8.– "La ecuación

$$x^4 + y^4 = z^2 ,$$

y en particular, la ecuación

$$x^4 + y^4 = z^4 ,$$

no tiene solución en números enteros".

9.– "Todo número primo de la forma $3k + 1$, se puede escribir como x^2+3y^2 ; y todo número primo de la forma $8k + 1$, o de la forma $8k + 3$, se puede escribir como $x^2 + 2y^2$, con x e y enteros".

10.– "Todo número es la suma de tres números triangulares, a lo más". (Los números triangulares son los de la forma $n(n-1)/2$).

11.– "Ningún número triangular es un cubo".

12.– "Si n es un número mayor que 2, es imposible hallar números enteros y positivos x, y, z, que verifiquen la ecuación

$$x^n + y^n = z^n \text{ ".} \quad \textit{(Ultimo teorema de Fermat)}$$

Esta lista que contiene la mayoría de las proposiciones de la carta de Fermat a Carcavi se ha completado con algunas otras importantes del mismo Fermat.

Se observa que las proposiciones 5^a y 8^a son casos particulares de la 12^a, que es el famoso "Ultimo teorema", proposición no demostrada hasta el presente con toda generalidad, aunque los progresos realizados en los últimos años son francamente esperanzadores.

Como nos hemos de referir con frecuencia a las proposiciones, entonces no demostradas,de esta lista, la denominaremos "relación" o "lista" de Fermat.

Panorámica de la Teoría de Números en el siglo XVIII

La historia de la Teoría de Números en el siglo XVIII está escrita por tres matemáticos egrégios. Euler (1707-1783), Lagrange (1736-1813) y Legendre (1752- 1833).

INTRODUCTIO
IN ANALYSIN
INFINITORUM.

AUCTORE

LEONHARDO EULERO,
Professore Regio BEROLINENSI, *& Academiæ Imperialis Scientiarum* PETROPOLITANÆ *Socio.*

TOMUS PRIMUS.

LAUSANNÆ,
Apud MARCUM-MICHAELEM BOUSQUET & Socios.

MDCCXLVIII.

Euler es el matemático universal, que con el nuevo Cálculo infinitesimal describe y explica el mundo físico, pero que a la vez está dotado de una intuición numérica no igualada. Lagrange es el fino analista que a través del modelo matemático estudia los procesos dinámicos y sigue con rigor lógico su evolución, pero que también sabe emplear este rigor para analizar las proposiciones aritméticas más difíciles, y demostrarlas. Finalmente, Legendre sigue la misma vía analítica que Lagrange, pero su interés ya está más próximo a la especulación pura, tanto funcional como en el campo aritmético. Su forma de exposición, ordenada y clara, tiene las notas de un estilo francés, siempre algo didáctico.

Aunque más adelante tratemos de la obra y otras circunstancias de estos grandes maestros, conviene dar noticia cronológica de sus vidas fijándolas en el ambiente cultural y científico propios. No olvidemos que el Tiempo es el notario de la Historia.

Leonhard Euler nace en 1707 en las proximidades de Basilea, la ciudad en la frontera de tres países y cruce de corrientes culturales, religiosas y comerciales. Después de estudiar Teología se dedica a las Matemáticas y a los 19 años consigue un premio de la Academia de Ciencias de París. En 1733, como Ayudante de Daniel Bernoulli, se traslada a San Petersburgo, y poco después le sucede como Profesor. En esta ciudad permanece hasta 1741, desarrollando una maravillosa actividad investigadora. Invitado por Federico II de Prusia, llega a Berlin en 1741, donde durante 25 años fue Director de la Clase de Matemáticas en la Academia. En 1766 llamado por Catalina la Grande, vuelve a San Petersburgo. Su delicada vista empeora, quedando al año siguiente completamente ciego, pero continuó con su gran actividad científica. El 7 de septiembre de 1783, después de haber tratado de los asuntos del día, y comentado la noticia del descubrimiento de Urano, con la tranquilidad de coronar una vida ejemplar, murió a los 76 años.

En la ciudad de Turín, en 1736, nace Joseph Louis Lagrange. Con 19 años es Profesor de la Real Escuela de Artillería de Turín, en la que permanece durante 10 años. En este periodo de tiempo investiga en la línea matemática característica del XVIII: la Matemática al servicio de la Mecánica y,en general, de la Física teórica. Por mediación de D'Alembert, en 1766, fue llamado por Federico II a Berlín, como sucesor de Euler, donde permaneció hasta 1787, y de esta época son sus trabajos sobre Toería de Números. Admirado como el matemático más eminente, ingresó en la Academia de Ciencias de París. Desde la fundación en 1795, miembro de la Comisión de Pesas y Medidas. Profesor de la Escuela Politécnica desde 1794 hasta 1799. Reconocido oficialmente a pesar de sus ideas monárquicas, en los tiempos cambiantes de la Revolución, y distinguido con altos cargos, muere en 1813, reposando en el Panteón.

Fue en París, en el año 1753, en donde nace Adrien Marie Legendre en el seno de una familia de cómoda posición. Su independencia económica le permite, desde joven, dedicarse a su afición, que es la Matemática. Desde 1775 a 1780 fue Profesor de la Escuela Militar de París.

A los 30 años ingresa en la Academia de Ciencias de París, primero como "Adjunto"

y desde 1785 como "Asociado". En 1782 había obtenido un premio de la Academia de Ciencias de Berlín, lo que fue principio de una relación con Lagrange,entonces en Berlín. Víctima de la Revolución pierde sus bienes e incluso su situación en la Academia. Durante el año 1794 preside la Comisión de Instrucción Pública. Desde 1788 a 1815 es examinador en la Escuela Politécnica. En 1813 reemplaza a Lagrange en el Bureau des Longitudes. Muere en 1833 este matemático parisino, testimonio fiel de la refinada cultura francesa que se extendía por Europa.

En la panorámica de la Teoría de Números en el XVIII, prescindiendo del orden cronológico, observamos en primer término la presencia dominante de los tres grandes genios: Euler, Lagrange y Legendre. Aunque se conocían y relacionaban, en sus investigaciones domina la nota personal, y se sienten más próximos al legado de Fermat que a los resultados conseguidos por sus coetáneos. Solamente es Euler, al que se le quedan estrechos todos los esquemas convencionales, quien empieza a recorrer nuevos caminos en la investigación de las propiedades de los números enteros, aunque nunca abandona los métodos puramente aritméticos.

Profundicemos algo más en este análisis, tratando de valorar los resultados con perspectiva de futuro, es decir, en cuanto fueron fundamento y señalaron métodos en una teoría que en el siglo siguiente fue llamada por Gauss "la reina de las Matemáticas".

La aplicación de las técnicas del nuevo Cálculo Infinitesimal a la resolución de problemas de la Teoría de Números, es un objetivo que se propuso Euler, convencido de las posibilidades ilimitadas de los nuevos métodos. Se trata, en efecto, de un propósito aparentemente contradictorio, por cuanto los métodos infinitesimales no parecen los adecuados para llegar a soluciones enteras ajenas al sentido de la aproximación. Seguramente la introducción de los métodos analíticos en la Teoría de Números, es el aspecto más original y característico de la obra de Euler en esta rama de la Matemática. Notable es también su obra original cuando usa los métodos aritmético-algébricos, de la que daremos noticia posteriormente, pero su contribución genial es el empleo de algoritmos indefinidos para resolver problemas de divisibilidad, representación de números como suma de cuadrados, etc. Euler es el precursor de una nueva Teoría de Números, que cuando Dirichlet, entre 1837 y 1839, publica su célebre memoria "Recherches sur diverses applications de l'Analyse infinitésimale a la théorie des nombres", muestra su real potencia y su necesidad para la resolución de los problemas más difíciles.

Hasta su estancia en Berlín no se interesa Lagrange por las cuestiones de Teoría de Números. Es entonces, al leer cuidadosamente los trabajos de Euler, su antecesor en la Academia de Ciencias, cuando despiertan su atención.

Entre los años 1766 y 1777 se ocupa de estos temas, pero lo sorprendente es que un fino analista como Lagrange, no se incline por los métodos funcionales eulerianos, sino por los aritmético-algébricos, en los que se enmarca la obra fermatiana. Ciertamente que el éxito acompaña a Lagrange, pues por una parte convierte en teoremas muchas de las conje-

turas de Fermat, y por otra en su memoria "Recherches d'Arithmétique" establece los fundamentos de una teoría de las formas cuadráticas binarias, que se presenta como la primera investigación sistemática de un capítulo de la Teoría de Números. Se trata, pues, de un paso de gran trascendencia y significado en el futuro desarrollo de esta rama de la Matemática. En cierto aspecto se puede considerar a Lagrange como continuador de la obra de Fermat, en el estilo racional del pensamiento francés.

Entre los múltiples intereses matemáticos del joven Legendre, en la época en que ganó el premio de la Academia de Berlín por un trabajo sobre Balística, también estaba la Teoría de Números a la manera clásica. Los problemas de representación de números por formas cuadráticas enteras, que años antes Lagrange había estudiado en su memoria fundamental, continuaron ocupando la atención de algunos admiradores, entre los que se encontraba Legendre quien también se interesó en esta línea de investigación. Sin embargo el nombre de Legendre está unido a una proposición muy significativa en la Teoría de Números, que es la llamada *Ley de reciprocidad cuadrática.* La historia de esta ley, presente en la intuición numérica de Euler, encontrada por Legendre, y demostrada la primera vez por Gauss, tiene una apasionante presencia a lo largo de los siglos. En 1798 publica Legendre su tratado "Theorie des nombres". El primero de esta rama de la Matemática con nombre propio.

De el prólogo de la "Theorie des nombres" de Legendre

En el prólogo de su tratado, Legendre describe la evolución de esta rama de la Matemática hasta el último cuarto del siglo XVIII. Citamos algunos párrafos del mismo, que se refieren a este siglo.

"Fermat, uno de ios geómetras cuyos trabajos contribuyeron en gran medida a acelerar el descubrimiento del nuevo Cálculo, cultivó con gran éxito la Ciencia de los números, y abrió rutas nuevas. Nos dejó un gran número de interesantes teoremas, pero casi siempre sin demostración. Esto correspondía al espíritu del tiempo, en el que los matemáticos proponían los problemas unos a otros. Se procuraba esconder el método a fín de reservar los nuevos triunfos, tanto para ellos mismos como para su nación. Por esto la mayoría de las demostraciones de Fermat se han perdido y, las pocas conservadas, nos hacen lamentar más la pérdida de las que nos faltan".

"Después de Fermat hasta Euler, los geómetras dedicados completamente a los descubrimientos o a las aplicaciones del nuevo Cálculo, no se ocuparon en absoluto de la Teoría de Números. Euler, el primero, se aplica a esta tarea; las numerosas memorias publicadas sobre esta materia en los Comentarios de Petersburgo (Commentarii Academiae Scientiarum Petropolitanae), y en otras obras, prueban con qué interés procuraba hacer que esta ciencia experimentara los mismos progresos que se manifestaban en otras partes de las Matemáticas. También parece cierto que Euler tenía un gusto especial por este tipo de investigaciones, y que se entregó con apasionamiento, cosa que les ocurre a la mayoría de los que

RECHERCHES

SUR

DIVERSES SORTES

D'INTÉGRALES DÉFINIES,

PAR M. LEGENDRE,

Lu à la Classe des Sciences Mathématiques et Physiques
de l'Institut de France, le 13 novembre 1809.

se ocupan de estas cuestiones. Sea como fuera, sus penetrantes investigaciones le conducen a la demostración de dos de los principales teoremas de Fermat". (Aquí enuncia Legendre, las proposiciones que hemos denominado "Congruencia de Fermat" y "Teorema de los dos cuadrados").

"Una multitud de otros descubrimientos importantes resaltan en las memorias de Euler. Se encuentra la teoría de los divisores de la cantidad $a^n + b^n$; el tratado de "Partitio numerorum" que está insertado en su "Introductio in Analysin infinitorum"; el uso de los factores inaginarios e irracionales en la resolución de las ecuaciones indeterminadas de segundo grado, suponiendo que se conoce una solución particular; la demostración de muchos teoremas sobre las potencias de los números, y en particular de las potencias negativas, enunciados por Fermat; de que la suma o diferencia de dos cubos no puede ser un cubo, y que la suma o diferencia de dos bicuadrados no puede ser un cuadrado". (Proposiciones 5^a y 8^a de la relación fermatiana).

"En fin, se encuentran en sus mismos escritos, un gran número de cuestiones indeterminadas resueltas por artificios analíticos muy ingeniosos".

"Durante mucho tiempo fue Euler casi el único geómetra que se ocupó de la Teoría de Números. Posteriormente Lagrange participó también en la misma carrera, y sus primeros pasos estuvieron señalados por el mismo éxito que los que había cosechado en las investigaciones de un género más sublime".

"Un método general para resolver las ecuaciones indeterminadas de segundo grado, y lo que es más difícil, un método para resolverlas en números enteros, fue el primer paso de este ilustre sabio. Posteriormente aplicó las fracciones continuas a esta rama del Análisis, y fue el primero en demostrar que es periódico el desarrollo, en fracción contínua, de la raíz de una ecuación de segundo grado con coeficientes racionales. También demostró que el problema de Fermat relativo a la ecuación $x^2 - dy^2 = 1$, es siempre resoluble, lo que nunca había sido demostrado rigurosamente, aunque muchos geómetras propusieron métodos para la resolución de la ecuación".

"El mismo sabio, en investigaciones posteriores que están consignadas en las Memorias de Berlín (Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlín), ha sido el primero en demostrar que todo número entero es la suma de cuatro cuadrados".

Otros notables resultados de Euler, Lagrange y Legendre

Según hemos visto, en la panorámica de la Teoría de Números en el XVIII, se destacaban como las más importantes aportaciones de los citados matemáticos a esta teoría, las siguientes: la introducción de los métodos analíticos por Euler; la elaboración de la teoría de las formas cuadráticas binarias por Lagrange y la ley de reciprocidad cuadrática

por Legendre. De cada una de ellas haremos un análisis detallado más adelante.

Naturalmente que esta calificación de la importancia de los resultados es discutible y en parte no coincide con la opinión de los matemáticos de fines del siglo XVIII. En el prólogo citado de su tratado, Legendre califica como principales teoremas de Fermat las proposiciones 1^a y 2^a de su relación, y de los métodos analíticos sólo dice que son muy ingeniosos.

En todo caso, aparte de las tres aportaciones fundamentales señaladas, otros muchos resultados son reseñables en este periodo. La mayoría se deben a Euler, cuya producción es inmensa, lo que dificulta establecer un orden cronológico en la realización de sus trabajos. Con frecuencia la fecha de publicación no se corresponde con la de la redacción. Ejemplo de ello es la proposición recíproca del teorema de Euclides, en su IX libro, sobre los números *perfectos*, es decir, de aquéllos que son iguales a la suma de sus divisores propios:

"Si un número primo par es perfecto, tiene la forma

$$2^{p-1}\,(2^p-1)\,,$$

en donde p y 2^p-1 son primos".

La proposición recíproca se publicó después de la muerte de Euler, y sin duda el estudio de estos números fue un tema que le entretuvo en su juventud.

También se ocupó Euler de los pares de *números amigos*, es decir, pares de números en los que cada uno de ellos es igual a la suma de los divisores propios del otro. De estos pares de números dio una lista de 62 (con dos equivocaciones). Anteriormente sólo se conocían 3 pares de números amigos.

Algunos resultados de Euler relativos a la Aritmética de los números son realmente sorprendentes, tal es el caso de los que llamó *números idóneos*, que son los de la lista siguiente:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13,$$
$$15, 16, 18, 21, \ldots, 1320, 1365, 1848.$$

en total 65 números idóneos.

"Si d es un número idóneo y ab = d, y un número n admite una sola representación de la forma $n = ax^2 + by^2$, con ax y by primos entre sí, entonces n es de una de las formas p, 2p, o 2^k, donde p es un número primo".

En particular, todo número impar representable en dicha forma, es primo. Por ejem-

plo, es primo $18518809 = 197^2+1848.100^2$, pues $1848 = 1.1848$ y 197.1 y 1848.100 son primos entre sí.

Hasta hoy no se ha demostrado si los únicos números idóneos son los dados por Euler, que sólo demostró su carácter en los casos 1,2 y 3. Posteriormente Gauss demostró los casos restantes en el contexto de las formas cuadráticas binarias enteras.

Pasemos ahora a citar algunas de las proposiciones más interesantes obtenidas por los matemáticos del siglo XVIII, muchas de ellas relacionadas con la lista de Fermat.

En 1732, Euler hace notar que la proposición 7ª de Fermat:

"Todo número de la forma $2^{2^k}+1$ es primo"

no es cierta. Para $k = 5$, es

$$2^{2^5}+1 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417.$$

En 1736, da Euler la primera demostración de la proposición 1ª de la relación de Fermat, llamada posteriormente "congruencia de Fermat". Una importante generalización de esta congruencia debida al mismo Euler, apareció en 1760, y dice:

"Si m es un entero y a primo con m, se tiene

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

en donde $\varphi(m)$ es el indicador del número m".

Las nociones eulerianas de *indicador, raíz primitiva* e *índice modular,* son básicas en la teoría aritmética de números.

En el periodo 1754-55 aparece la demostración por Euler de la proposición 2ª de la lista de Fermat:

"Todo número primo de la forma $4k+1$ es la suma de dos cuadrados".

También en este periodo, dio Euler la proposición:

"Todo divisor de la suma de dos números primos entre sí es una suma de dos cuadrados".

Ya en el periodo 1732-33, había estudiado Euler la ecuación $x^2-dy^2=1$, que aparece en la proposición 4ª de la relación de Fermat,y la llamó equivocadamente ecuación de Pell.El interés de Euler por esta ecuación fue paso previo para resolver en números enteros

la ecuación más general $ax^2 + bx + c = y^2$.

Fue en 1759 cuando Euler dio una solución de la ecuación, desarrollando $\sqrt{d}$ en fracción continua. En 1766, Lagrange completó este resultado, probando que $\sqrt{d}$ tiene un desarrollo periódico en fracción continua, y a partir de él se obtienen las infinitas soluciones enteras de la ecuación. Estas soluciones son los pares $x = p_n$, $y = q_n$, que forman las reducidas $\frac{p_n}{q_n}$ del desarrollo en fracción continua de $\sqrt{d}$, que es periódico de periodo p, para los valores de $n = kp - 1$, con $k = 1,2, \ldots$.

Esta ecuación tiene un especial significado en la historia de la Teoría de Números. De la India antigua proceden algunas soluciones en casos particulares, y parece que en Grecia se tenían conocimientos extensos sobre sus soluciones enteras. En el reto de Fermat a los matemáticos ingleses, Wallis (1616 - 1703) dio soluciones para valores de d que originaban cálculos muy complicados.

En 1760 Euler demostró la no existencia de soluciones enteras positivas de las ecuaciones $x^3 + y^3 = z^3$, y $x^4 + y^4 = z^2$, que son las proposiciones 4^a y 8^a de la relación de Fermat.

En el periodo 1760-61, prueba Euler la primera parte de la proposición 9^a de la relación de Fermat:

"Todo número primo de la forma $3k + 1$ se puede expresar univocamente en la $x^2 + 3y^2$ ".

Proposiciones análogas de representación de determinados números primos fueron dadas por Euler y Lagrange en el ámbito de la teoría de las formas cuadráticas binarias.

Un teorema básico en la teoría de las ecuaciones de congruencia fue dado por Lagrange en 1768:

"Sea p un número primo: y $f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$ un polinomio de grado m con coeficientes enteros, entonces es m el número máximo de raíces de la ecuación $f(x) \equiv 0$ (mód. p)".

De la misma época es la demostración definitiva de Lagrange del teorema de los cuatro cuadrados, que es la proposición 3^a de la relación de Fermat. Esta proposición se considerará detalladamente al final.

Y aunque se sale del siglo XVIII finalizamos esta noticia con el trabajo de Legendre, de 1828, en el que demuestra el último teorema de Fermat en el caso $n = 5$.

Como se ve, la mayoría de los trabajos reseñados son de Euler. Aparte del texto que

dedica Legendre en el prólogo de su tratado a elogiar la obra de Euler en este campo de la Matemática, son también expresivas sus palabras al principio de un trabajo sobre Análisis Indeterminado: "Se sabe en que medida existen pocos objetos sobre los que este gran geómetra no haya extendido una nueva claridad, y que la Teoría de los Números, en particular, es una de las que ha cultivado con mayor placer".

Otra cita que fija a este gigante de la Matemática en la Historia, es la de André Weil "Se debe tener presente que Euler partió absolutamente de cero, excepto de las proposiciones de apariencia misteriosa que enunciaba Fermat ...".

Euler y los métodos analíticos en la Teoría de Números

Realmente los métodos del Análisis Matemático tienen vigencia en la Teoría de Números desde los trabajos de Dirichlet, pero el germen de este encuentro entre ambas ramas de la Matemática está en las investigaciones de Euler.

Analizaremos algunos de los resultados de este célebre matemático, tratando de descubrir las inesperadas relaciones entre los procesos analíticos, en los que interviene esencialmente el paso al límite, y los aritmético-algébricos que corresponden a la Matemática discreta de los números enteros.

En todo caso se puede adelantar que el puente entre unos y otros está en los desarrollos en serie y productos infinitos, que Euler manejaba con una destreza y virtuosismo sorprendentes.

En una serie de potencias de coeficientes enteros o racionales, se establece, sin duda, una relación entre la ley de formación de los coeficientes, que tiene sentido finito, y el valor de la suma de la serie (dentro de su dominio de convergencia) que define una función, ordinariamente trascendente.

Euler fue el primero que estableció una relación entre series del tipo $\sum \frac{1}{n^s}$, con s real, y problemas de la Teoría de Números. Es ejemplar la demostración de la existencia de infinitos números primos, basada en la divergencia de la serie armónica $\sum \frac{1}{n}$.

Se parte de la igualdad

$$\prod_{p>1} \left(1-\frac{1}{p}\right)^{-1} = \prod_{p>1} \left(1+\frac{1}{p}+\frac{1}{p^2}+\dots\right) = \sum \frac{1}{n},$$

en la que los productos están extendidos a todos los números primos.

Si fuera finito el conjunto de los números primos, el producto del primer miembro

tendría un número finito de factores, por lo que su valor sería finito. Pero, por el contrario, la serie del segundo miembro es divergente. Esta contradicción muestra que el conjunto de los números primos es infinito.

La transformación básica por la que se pasa de un producto infinito, referido al conjunto de los primos, a una serie referida al conjunto de todos los números naturales, se puede generalizar, y se tiene

$$\prod_{p>1}\left(1-\frac{1}{p^s}\right)^{-1}=\sum_{n\geqslant 1}\frac{1}{n^s}$$

Para $s>1$, la serie del segundo miembro converge, y tiene sentido la igualdad anterior. La suma de la serie define la función ζ (s), que para valores reales de s fue estudiada posteriormente por Dirichlet (1805-1859), y después por Riemann (1826-1866) como función de variable compleja.

La función *zeta de Riemann* es una de las más importantes de la teoría de los números primos. La *conjetura de Riemann* de que los ceros de la función ζ (s) tienen su parte real igual a $\frac{1}{2}$, salvo los ceros conocidos que son los enteros negativos, es una de las más famosas cuestiones abiertas. Hilbert, en su famoso discurso inaugural del Congreso Internacional de Matemáticas de París en 1900, la propuso como uno de los 23 problemas fundamentales que debería ocupar la atención de los matemáticos durante nuestro siglo, que entonces empezaba.

Volviendo al estudio de los métodos de Euler, citaremos un desarrollo, aparantemente alejado de la Teoría de Números, pero que en realidad tiene una profunda vinculación a los procesos analíticos de esta teoría.

Se trata del desarrollo de la función

$$f(x)=\frac{x}{e^x-1}=\sum_{n\geqslant 0}\frac{B_n}{n!}x^n.$$

Los coeficientes $B_0, B_1, \ldots$ designan los llamados *números de Bernoulli*, que verifican la relación recurrente

$$B_n=-\sum_{k=0}^{n-1}B_k\,\frac{1}{k!}\,\frac{n!}{(n-k+1)!}.$$

Estos números aparecen en otras muchas ramas de la Matemática, por ejemplo en Topología Algebraica.

Una de las más celebradas fórmulas de Euler, publicada en 1736, en sus "Institutiones Calculi Differentialis" es

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{2^{2k-1}\pi^{2k}\,|B_{2k}|}{(2k)!},$$

también relacionada con la función ζ (s), antes mencionada.

Muy representativo de las ideas de Euler, en la aplicación de los métodos analíticos a la resolución de problemas de la Teoría de Números, es su trabajo sobre el "Teorema de los cuatro cuadrados" (proposición 3^a de la relación de Fermat).

De este tema se ocupó muchos años, y no consiguió una demostración completa del mismo, que estaba reservada para Lagrange que en 1770 publicó "Démonstration d'un théoréme d'arithmétique". Sin embargo, posteriormente Euler simplificó esta demostración.

En su intento por demostrar el teorema, Euler consideró la función f definida como suma de una serie de potencias:

$$f(x) = 1 + x + x^4 + x^9 + x^{25} + \ldots,$$

que evidentemente converge si $|x| < 1$ y formó la nueva serie

$$[f(x)]^4 = \sum_{n \geq 0} r(n)\, x^n,$$

obtenida como producto de series. Precisamente al aplicar esta regla se observa que el coeficiente r (n) de x^n es el número de descomposiciones de n como suma de cuatro cuadrados: r (0) = 0. r (1) = 1, r (2) = 2, r (3) = 3, r (4) =), r(5) = 7, ...

Para demostrar el teorema, basta probar que es $r(n) > 0$, para todo n, es decir, que ninguno de los coeficientes de la serie es nulo. Pasaron muchos años hasta que Jacobi demostrara esta propiedad, en el contexto de la teoría de las funciones elípticas.

Con estos métodos, situaba Euler una proposición de Teoría de Números, en el marco de la Teoría de Funciones.

Para valorar la trascendencia de estas ideas conviene considerar las cosas desde un punto de vista más general. Sea f: N → N una *función aritmética,* es decir, una función en la que el dominio es el conjunto N de los números naturales y el recorrido pertenece a este mismo conjunto.

Euler define la *función generatriz* de f, como la serie de potencias

$$F(x) = \sum_{n=0}^{\infty} f(n)x^n$$

suponiendo que no es nulo su radio de convergencia.

De la relación entre f y F, es decir, de la relación entre los coeficientes de la serie de potencias y la función suma de la serie, se trata de obtener propiedades numéricas de f a partir de las funcionales de F. En realidad Euler solo trató casos particulares de funciones aritméticas referentes a particiones de números. En general, una *partición de un número natural n en k sumandos,* es una expresión $n = n_1 + n_2 + \ldots + n_k$, en la que los sumandos son números naturales, incluído el cero. Si se designa por p(n) el número de estas particiones, queda definida la función aritmética p.

Para la función generatriz de p, Euler da la siguiente fórmula factorial

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} (1 - x^m)^{-1}, \text{ con } p(0) = 1.$$

Análogamente, designando por q(n) el número de las particiones de n en sumandos impares, y por r(n) el número de particiones de n en sumandos distintos, obtiene Euler para sus funciones generatrices las siguientes fórmulas factoriales

$$\sum_{n=0}^{\infty} q(n)x^n = \prod_{m=0}^{\infty} (1 - x^{2m+1})^{-1}, \text{ con } q(0) = 1,$$

$$\sum_{n=0}^{\infty} r(n)x^n = \prod^{\infty} (1 + x^m), \qquad \text{con } r(0) = 1.$$

Por medio de las funciones generatrices demostró la importante propiedad

$$q(n) = r(n).$$

Un resultado, también notable, que muestra una vez más la intuición numérica de Euler y su destreza en el manejo de las series, es la fórmula

$$\prod_{n=1}^{\infty} (1 - x^m) = \sum_{k=\infty}^{+\infty} (-1)^k x^{3k^2 + k},$$

que seguramente obtuvo calculando muchos términos. Años más tarde dio una demostración de la misma. Ciertamente que el lugar de esta fórmula es la teoría de las funciones elípticas.

Prescindiendo de otros resultados de tipo analítico con indudable proyección en la Teoría de Números, citamos finalmente la siguiente fórmula, oscura en su interpretación y de difícil prueba:

$$\frac{1-2^{m-1}+3^{m-1}-4^{m-1}+\ldots}{1-2^{-m}+3^{-m}-4^{-m}+\ldots}=\frac{1.2.3\ldots(m-1)\,(2^{m}-1)}{(2^{m-1}-1)\,\pi^{m}}\cos\frac{m\pi}{2},$$

que después de un exámen atento, aparece como una forma de la ecuación funcional de la función ζ (s).

Lagrange como continuador de Fermat

El fino analista que supo trasladar los métodos analíticos al campo de la Física en su magistral tratado de "Mecánica Analítica", también trató, con la claridad del razonamiento preciso, algunos problemas fundamentales de Teoría de Números. Los trabajos más importantes son memorias publicadas entre 1766 y 1777, durante su periodo de Berlín. Sin duda se sintió atraído por los resultados de su antecesor Euler, que estudió cuidadosamente, y que trataban de cuestiones que Fermat había dejado abiertas. Ciertamente que Lagrange tuvo más éxito que Euler en la demostración de las conjeturas fermatianas. Como por otra parte, los métodos de Lagrange fueron de naturaleza puramente aritmético-algébrica, se le puede considerar, en lo referente a estas investigaciones, como el más directo continuador de la obra de Fermat.

En tres memorias importantes se ocupa Lagrange de cuestiones básicas en esta rama de la Matemática. En la "Solution d'un problème d'arithmétique" de 1768 trata de la llamada "Ecuación de Pell". En la "Démonstration d'un thèorème d'arithmétique" de 1770 demuestra el "Teorema de los cuatro cuadrados". En la tercera memoria "Recherches d'arithmétique", de 1773, seguramente la más importante, construye una "Teoría de las formas cuadráticas binarias" en el dominio de los números enteros. Es curiosa la imprecisión de los títulos de las memorias, con una simple alusión a la Aritmética.

La claridad de exposición y el adecuado razonamiento hace su lectura agradable. En general, el estilo de Lagrange corresponde al de una Matemática moderna. En particular la memoria relativa a las formas cuadráticas, constituye una teoría organizada referente a propiedades de los números enteros, en la que se recogen y relacionan unas proposiciones que no habían sido demostradas, y otras nuevas. Se trata, pues, de un capítulo, el primero escrito, de la que después Legendre llamaría Teoría de Números.

Daremos cuenta de estos trabajos, aunque por su importancia nos detendremos especialmente en el último.

Teoría lagrangiana de las formas cuadráticas binarias.

En su introducción a esta memoria, Lagrange mismo describe los resultados obtenidos. La traducción libre es la siguiente:

"Estas investigaciones se ocupan de los números que se pueden representar en la forma $Bt^2 + Ctu + Du^2$, en la que B, C y D son números enteros, e igualmente t y u números enteros pero indeterminados. En primer lugar, buscaré las formas que representan números, y veré que los divisores de estos números también pueden ser representados de esa manera. Daré después un método, con el cual se pueden reducir dichas formas a un número mínimo; daré una tabla que contenga a éstas, para uso práctico, y mostraré la utilidad de la tabla en la investigación de los divisores de un número. Finalmente demostraré varias proposiciones sobre números primos de la forma $Bt^2 + Ctu + Du^2$, de las que algunas son conocidas pero no demostradas, y las otras totalmente desconocidas".

Empleando una notación más frecuente, diremos que el problema que se trata de abordar es el de la representación de números enteros por formas cuadráticas binarias

$$q(x, y) = ax^2 + 2bxy + cy^2 ,$$

en las que a, b y c son coeficientes enteros y las variables x e y toman valores enteros.

Formas cuadráticas de esta clase son

$$x^2 + y^2 , \quad x^2 + 2y^2 , \quad x^2 + 3y^2 , \quad x^2 - dy^2 ,$$

ya consideradas por Fermat.

La primera proposición que demestra Lagrange es:

"Sea r un divisor de un entero que puede ser representado en la forma $ax^2 + 2bxy + cy^2$, con $x = x_0$ e $y = y_0$, primos entre sí. Entonces r es representable por una forma $Ax^2 + 2Bxy + Cy^2$, con $x = X_0$ e $y = Y_0$ primos entre sí, siendo $AC - B^2 = ac - b^2$ ".

Si el entero m es representable por $ax^2 + 2bxy + cy^2$, con x e y primos entre sí, se dice que m es un *divisor* de $q(x,y)$. La expresión $\Delta = ac - b^2$ es el *determinante* de la forma.

Para exponer la teoría de la reducción de las formas cuadráticas es conveniente introducir la notación matricial, así se tiene:

$$q(x,y) = ax^2 + 2bxy + cy^2 = (x,y) \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Dos formas, $ax^2 + 2bxy + cy^2$ y $AX^2 + 2BXY + CY^2$ son *equivalentes* si existe una transformación

$$T = \begin{cases} X = \alpha x + \beta y \\ Y = \gamma x + \delta y \end{cases}$$

invertible, tal que es

$$\begin{pmatrix} A & B \\ B & C \end{pmatrix} = T^t \begin{pmatrix} a & b \\ b & c \end{pmatrix} T.$$

Si el determinante de T es 1, las formas son *propiamente equivalentes.*

Las definiciones de las formas *definidas, positivas* y *negativas,* e *indefinidas* son las acostumbradas. Además:

$q(x, y)$ es positiva si $\Delta > 0$ y $a > 0$
$q(x, y)$ es negativa si $\Delta > 0$ y $a < 0$,
$q(x, y)$ es indefinida si $\Delta < 0$.

Con esta nomenclatura y esta notación el "Teorema fundamental" de Lagrange, para la teoría de las formas cuadráticas, es

"Toda forma positiva g es propiamente equivalente a una forma *reducida*, que es una forma cuya matriz correspondiente $\begin{matrix} a & b \\ b & c \end{matrix}$ tiene sus términos que verifican las condiciones

$$-\frac{a}{2} < b \leqslant \frac{a}{2}; \quad a \leqslant c \quad y \quad 0 \leqslant b \leqslant \frac{a}{2} \text{ si } a = c.$$

La forma reducida está determinada univocamente por estas condiciones.

Además

$$a \leqslant 2\sqrt{\frac{\Delta}{3}},$$

donde Δ es el determinante de la forma g".

Consecuencia de las acotaciones anteriores para los coeficientes de las formas reducidas, es:

"Existe un número finito de clases de equivalencia propia, en el conjunto de las formas cuadráticas positivas binarias, para cada valor del determinante Δ".

A partir de las acotaciones de los coeficientes se pueden obtener todas las formas reducidas posibles para cada valor de Δ, y en consecuencia tabularlas.

Para las formas cuadráticas indefinidas, Lagrange da un teorema análogo de reducción:

"Una forma cuadrática indefinida es propiamente equivalente a una forma reducida, que es una forma cuya matriz $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ tiene sus términos que verifican las condiciones

$$|a| \leqslant |c| \qquad y \qquad |b| \leqslant \left|\frac{a}{2}\right|$$

En general, si una forma es indefinida, su reducida no está univocamente determinada".

Como en el caso de formas positivas, se puede construir una tabla de formas reducidas indefinidas.

La "Ley de reciprocidad cuadrática".

Esta ley es seguramente el resultado más original de la Teoría de números aritmético-algébrica en el siglo XVIII. Se encuadra en el marco de los temas preferidos por los investigadores de este periodo: la representabilidad de números enteros por formas cuadráticas binarias con variables y coeficientes enteros.

La historia de esta ley es la de la Teoría de números en la segunda mitad del siglo XVIII, y el interés no decayó en el siguiente. El deseo de encontrar lo que se esconde detrás de la ley, y de poner de manifiesto sus implicaciones en multitud de cuestiones, fue un tema clave en el interés de los matemáticos. Más adelante veremos que su generalización fue uno de los problemas abiertos, que Hilbert enunció en su famoso discurso inaugural del Congreso de París de 1900.

La ley fue descubierta por Euler, enunciándola claramente, pero sin demostración. En un trabajo de 1783, después de dar cuatro proposiciones, en un teorema que resume los resultados, afirma lo que después Legendre llamó "Ley de reciprocidad cuadrática". Como dice Kronecker, muchos años antes conocía Euler la proposición, que con seguridad descubrió en el periodo 1744-1746, probablemente tras cuidadosos estudios de los resultados numéricos de laboriosos cálculos para los que tenía especial habilidad. En todo caso la prioridad en el descubrimiento de Euler, está fuera de toda duda.

Sin embargo una vez más en la historia de la Matemática, el nombre del autor queda eclipsado. Legendre redescubrió la ley en 1785, en el curso de unas investigaciones sobre la congruencia de Fermat, le dio un nombre expresivo y consiguió una formulación atrayente por medio de los símbolos que llevan su nombre.

La ley de reciprocidad cuadrática se refiere a los restos que dan los cuadrados de los números enteros al dividirlos por números primos.

Para precisar el sentido de esta ley conviene introducir algunas definiciones y símbolos.

Sea p un número primo impar y a un entero no múltiplo de p. Se forma la progresión aritmética indefinida

$$\ldots, a-kp, \ldots, a-2p, a-p, a, a+p, a+2p, \ldots, a+kp, \ldots .$$

Si alguno de sus términos es un cuadrado perfecto, se dice que a es un *resto cuadrático módulo* p: y si ninguno de los términos de la progresión es un cuadrado perfecto, se dice que a es un *no-resto cuadrático módulo* p. Con el lenguaje de congruencias, a es un resto cuadrático módulo p, si la ecuación de congruencia

$$x^2 = a \pmod{p}$$

tiene alguna solución. Cuando no existe solución alguna, a es no-resto cuadrático módulo p.

Como la progresión aritmética está determinada por los dos números a y p, al considerar que uno u otro sea fijo,se originan los dos problemas básicos que dominan toda la teoría de los restos cuadráticos.

1. Fijado un número primo p, determinar los números a que son restos cuadráticos módulo p, y los que son no-restos.

2. Fijado un número a, determinar aquellos primos p para los que a es un resto cuadrático módulo p, y aquellos para los que a es no-resto cuadrático módulo p.

El primer problema es de resolución fácil, aunque con frecuencia pesada. Euler y después Gauss dieron criterios para resolverlo. El segundo problema es mucho más difícil, y su resolución depende de la "Ley de reciprocidad", que cuando a es primo impar permite intercambiar los papeles que juegan a y p.

Sean p y q dos números primos impares. Se forman las dos progresiones aritméticas:

$$\ldots, q-kp, \ldots, q-2p, q-p, q, q+p, q+2p, \ldots, q+kp, \ldots,$$
$$\ldots, p-kq, \ldots, p-2q, p-q, p, p+q, p+2q, \ldots, p+kq, \ldots .$$

La "ley de reciprocidad cuadrática" asegura que "si en la primera progresión existe un cuadrado perfecto también existe en la segunda, salvo en el caso de que p y q sean de

la forma $4k+3$, pues entonces en una progresión existe un cuadrado perfecto y en la otra no existe.

Naturalmente que esta descripción, un poco euleriana, de la ley, está pidiendo una formulación más concisa, lo que se consigue con la notación simbólica de Legendre.

Para llegar a la ley de reciprocidad Legendre demostró una proposición previa, hoy conocida como *lema de Euler,* que enunciada con el lenguaje de congruencias dice:

"Sea p un primo impar. Un número a, no divisible por p, es resto cuadrático módulo p si, y sólo si, $a^{(p-1)/2} \equiv 1 \pmod{p}$".

Observa además, que si se verifica esta última condición, la ecuación $x^2 \equiv a \pmod{p}$ tiene una solución positiva menor que $p/2$.

Fue con ocasión de este resultado cuando Legendre introduce sus conocidos símbolos, como el mismo lo comenta:

"Hemos demostrado que si a es un número cualquiera y p es un número primo impar no divisor de a, la cantidad $a^{p-1} - 1$ es siempre divisible por p (congruencia de Fermat.) Siendo esta cantidad producto de dos factores $a^{(p-1)/2} + 1$ y $a^{(p-1)/2} - 1$, forzosamente uno u otro ha de ser divisible por p, por lo que la cantidad $a^{(p-1)/2}$ dividida por p dará siempre el resto -1 o el $+1$. Como cantidades análogas a $a^{(p-1)/2}$ aparecerán con frecuencia en el curso de nuestras investigaciones, emplearemos el carácter abreviado $\left(\frac{a}{p}\right)$ para indicar el resto que da $a^{(p-1)/2}$ al dividirlo por p, y que según lo dicho sólo puede ser $+1$ o -1. Cuando $\left(\frac{a}{p}\right) = +1$, se dice que a es resto cuadrático de p, que como se ha visto es la condición para que la ecuación $x^2 = a \pmod{p}$ tenga solución; cuando $\left(\frac{a}{p}\right) = -1$, se dice que a es no-resto cuadrático de p".

Obsérvese que en la definición expuesta, Legendre procede indirectamente introduciendo los símbolos a través del lema de Euler.

La definición directa es la siguiente:

"Si p es un primo impar, y a un entero cualquiera, el símbolo de Legendre, correspondiente a p, que se representa por $\left(\frac{a}{p}\right)$, es una aplicación del conjunto Z de los números enteros en el conjunto $\{+1, -1, 0\}$, definida por

$$\left(\frac{a}{p}\right) = \begin{cases} +1, \text{ si } a \text{ es un resto cuadrático módulo } p, \\ -1, \text{ si } a \text{ es un no-resto cuadrático módulo } p, \\ 0, \text{ si } a \text{ es múltiplo de } p. \end{cases}$$

Entre las cómodas propiedades de estos símbolos, deducidas de su misma definición, está la de su carácter multiplicativo respecto de a, para cada p fijo.

El empleo de los símbolos de Legendre permite presentar la ley en una forma que efectivamente pone de manifiesto la propiedad de reciprocidad que le da nombre:

"Si p y q son dos primos impares distintos, es

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\,,,$$

Legendre dio una demostración incompleta de su ley, pues en el trascurso de la misma, se vio obligado a admitir, sin prueba, que si p es un primo de la forma 4n+1, se puede siempre encontrar otro primo q de la forma 4n+3 tal que $\left(\frac{p}{q}\right) = -1$. Este resultado es cierto, como consecuencia de un célebre teorema de Dirichlet, demostrado en 1837, que dice:

"Si en la progresión aritmética a, a+h, a+ 2h, . . . , a+ nh, . . . , a y h son primos entre sí , existen infinidad de números primos en la progresión".

Algunos autores franceses denominan *conjetura de Legendre* a esta proposición.

Hasta hoy se han dado más de 150 demostraciones de la ley de reciprocidad cuadrática. El propio Gauss, que fue el primero que la demostró correctamente a los 18 años, dio no menos de ocho. La última, de la que tenemos noticia, es de M. Gerstenhaber, y se titula "The 152nd proof of the law of quadratic reciprocity".

Para la demostración de la ley de reciprocidad, es evidente que no se requiere el potente teorema de Dirichlet. Gauss demostró en un lema que el carácter de resto cuadrático de un entero a no múltiplo de un módulo primo impar p, está determinado por $(-1)^m$, donde m es el número de restos que exceden a p/2, al dividir por p los términos de la sucesión a, 2a, 3a, ..., $\frac{p-1}{2}$ a. Este lema permite calcular cada uno de los símbolos $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$, de donde se deduce la ley de reciprocidad sin gran dificultad.

Parece muy probable que los intentos repetidos de Gauss para hallar nuevas demostraciones de la ley de reciprocidad estaban motivados por su deseo de encontrar métodos que permitieran la generalización de la ley a congruencias de orden superior. Resultados notables consiguió para la ley de reciprocidad bicuadrática, que publicó en 1832, fecha que deja muy atrás al siglo XVIII.

Terminamos volviendo a la alusión a los problemas que Hilbert proponía al estudio de los matemáticos de nuestro siglo. Traducimos literalmente:

"Se pide demostrar, en el caso de un cuerpo de números cualquiera, la ley de reciprocidad de los restos de las potencias de grado r, donde r designa un número primo impar, o también cuando r es una potencia de 2 o la de un número primo impar. Creo que se podría establecer la ley y descubrir los métodos esenciales necesarios para su demostración, generalizando convenientemente la teoría que he demostrado a propósito del cuerpo de las raíces r-ésimas de la unidad, y de mi teoría de los cuerpos relativamente cuadráticos".

El problema todavía está ahí, para quien quiera hacer Historia.

Sumas de cuatro cuadrados

La proposición 3ª de la relación fermatiana, que dice:

"Todo número entero y positivo es suma de cuatro cuadrados de números enteros, entre los que no se excluye el cero", no se ha considerado en un primer término de la panorámica de la Teoría de Números en el siglo XVIII, pero se trata de una antigua y sorprendente proposición, una perla en la Historia de la Matemática.

Diofanto ya consideraba como cierto que todo entero positivo es un cuadrado o suma de 2, 3 o 4 cuadrados de números enteros positivos, lo que equivale a la proposición enunciada. En 1621, el matemático francés Bachet fue el primero que enunció esta propiedad en forma de teorema y comprobó que era cierta hasta el número 325.

Es interesante la opinión de Descartes sobre esta proposición:

"En lo referente a este teorema, que sin duda es uno de los más bellos que se pueden encontrar en el de Teoría de Números, no conozco ninguna demostración, y juzgo que será tan difícil que no he intentado buscarla".

Fermat aseguró que podía demostrarlo por el método del "descenso infinito", pero como en otros casos no dio detalles. En carta que escribió a su buen amigo Pascal en 1654, le expone un esquema de la demostración en cinco pasos, que son otras tantas propoisiciones, cuatro incluídas en la relación fermatiana, sin otra indicación aclaratoria.

Euler buscó con empeño la solución, y como cuestión no resuelta la contempló durante cuarenta años. Para Lagrange estaba reservado el éxito, pues en 1770 consiguió la demostración. Ciertamente que Euler le había preparado el camino, probando dos lemas básicos, y posteriormente simplificó la demostración de Lagrange. Esta, que no sigue el esquema trazado por Fermat, es seguramente la más sencilla de las conocidas.

El primer lema de Euler, publicado en 1743 es la identidad

$$(a^2+b^2+c^2+d^2)\,(p^2+q^2+r^2+s^2)=x^2+y^2+z^2+v^2\ ,$$

en la que

$$\begin{aligned} x &= ap+bq+cr+ds\ ,\\ y &= aq-bp+cs\ \pm dr\ ,\\ z &= ar\pm bs-cp\ \mp dq\ ,\\ v &= as\mp br\pm cq-dp\ , \end{aligned}$$

que expresa:

"El producto de dos sumas de cuatro cuadrados de números enteros, es una suma de cuatro cuadrados de números enteros".

En virtud de este lema, el problema planteado de descomponer un número entero en suma de cuatro cuadrados, basta considerarlo en el caso de que es primo el número dado.

El segundo lema de Euler, publicado en 1759, dice:

"Para cada p primo, la ecuación de congruencia

$$1+x^2+y^2=0 \quad (\text{mód. } p)\ ,$$

siempre tiene solución (x, y) con $0<x<p/2$ y $0<y<p/2$ "

Su demostración elemental se consigue por sustitución de todos los valores enteros para x e y permitidos por las últimas desigualdades.

Obsérvese que este lema también admite el siguiente enunciado:

"Para cada p primo existe un múltiplo $m.p$ de p que se puede descomponer en una suma de cuatro cuadrados de la siguiente forma

$$1+x^2+y^2+0^2\ ,,$$

El camino ya está trazado, y el paso siguiente será hallar el mínimo múltiplo de p, para el que es posible la descomposición en cuatro cuadrados. La demostración del teorema

consiste, simplemente, en ver que tal mínimo múltiplo de p se obtiene para $m = 1$. Los dos lemas siguientes conducen a este resultado:

"Para cada primo impar p, existe un entero positivo impar $m < p$, tal que $m.p$ es una suma de cuatro cuadrados".

"Si p es primo y m entero impar, con $1 < m < p$, tales que $m.p$ es una suma de cuatro cuadrados

$$m.p = x^2 + y^2 + z^2 + v^2 ,$$

entonces existe un entero positivo $m_1 < m$ tal que $m_1 . p$ es una suma de cuatro cuadrados

$$m_1 . p = x_1^2 + y_1^2 + z_1^2 + v_1^2 \cdot "$$

La propiedad de la representación de un número entero como suma de cuatro cuadrados fue completada por Legendre, en 1785, al demostrar que:

"Todo número entero que no sea de la forma $4^r (8k + 7)$ es suma de tres cuadrados".

El teorema de que todo número entero y positivo se puede representar como suma de cuatro cuadrados, está demostrado, aunque no se conoce el número de representaciones posibles que admite cada número en una suma de esta forma. Como decíamos, en la Antigüedad ya se suponía cierta esta mágica propiedad, y Bachet y Fermat la enunciaron como proposición perteneciente a una teoría deductiva. Los tres grandes matemáticos del siglo XVIII colaboraron para convertirla en un teorema. Hoy día, esta bella proposición todavía nos sorprende, y continuamos buscando qué se esconde detrás de ella, y nos preguntamos ¿por qué bastan sólo cuatro cuadrados?.

BIBLIOGRAFIA

Obras originales

EULER, L.– *Opera Omnia.* Los volumenes 1, 2 y 3.
Introductio in Analysis infinitorum. Opera Omnis. Vol. 8.

FERMAT, P.– *Oevres.* Vol. 2.

LAGRANGE, J.L.– *Oevres.* Los volumenes 1 y 3.

LEGENDRE, A.M.– *Théorie des Nombres.* Reimp. Blanchard, París 1955.

Obras de tipo histórico

DICKSON, L.E.– *History of the Theory of Numbers.* Reimp. Chelsea New York, 1974.

DIEUDONNE, J.– *Abrégé d'Histoire des Mathématiques 1700-1900.* Hermann, París 1978, Vol. 1.

KLINE, M.– *Mathematical Thought from Ancient to Modern Times.* Oxford, 1972.

Otras obras relacionadas con el tema

APOSTOL, T.M.– *Introducción a la Teoría analítica de números.* Trad. Ed. Reverté, 1980.

BOREVITCH, Z,I. y CHAFAREVITCH, I.R.– *Théorie des Nombres.* Trad. Gauthier-Villars, París 1967.

EDWARDS, H.M.– *Fermat's Last Theorem.* Springer 1977.

HASSE, H.– *Vorlesungen über Zahlentheorie.* Springer 1950.

SCHARLAU, W. y OPOLKA, H.– *From Fermat to Minkowski.* Springer 1985.

WEIL, A.– *Number Theory. An approach through history.* Birkhäuser, 1983.

The HILBERT problems.– Proc. Symp. in Pure Math. Vol. 28, Amer. Math. Soc. Providence (R.I.), 1976.