EL TEOREMA DE FERMAT

P. Báyer

1. Sus orígenes. El problema número 8 del Libro II de la Aritmética de Diofanto tiene el siguiente enunciado:

"Descomponer un cuadrado dado en dos cuadrados".

Si la respuesta a un problema no era única, Diofanto se limitaba a dar soluciones particulares, que obtenía gracias a una feliz elección de los datos. Veamos por ejemplo, cómo procede en el caso anterior. De entrada, se plantea resolver la ecuación

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

únicamente en el caso en que $z = 4$. Ensaya como valor de y uno de la forma $mx - 4$; tomando $m = 2$ y después de sustituir, encuentra como solución $x = 16/5$, $y = 12/5$, lo cual equivale a considerar la solución en enteros $x = 16$, $y = 12$, $z = 20$. Como es bien sabido, la solución general de la ecuación anterior la constituyen los enteros pitagóricos:

$$x = d(u^2-v^2), \quad y = 2duv, \quad z = d(u^2 + v^2),$$

en donde $d,u,v \in Z$ y $mcd(u,v) = 1$.

La Aritmética de Diofanto fue traducida al árabe en Persia en el siglo X y a través del mundo árabe llegó a España, pero permaneció ignorada en el resto de Europa hasta el siglo XV. **Regiomontanus (seudónimo del matemático** Johan Müller que responde a la latinización de Königsberg, su ciudad natal) encontró un manuscrito de dicha obra en Venecia en 1464. Posteriormente fueron hallados nuevos manuscritos y en 1575, en Basilea, aparecía la primera traducción latina editada. La primera edición que

incluía el texto griego junto a la versión en latín, fue hecha en París en 1621 por Claude-Gaspard Bachet de Méziriac; su título era: "Diophanti Alexandrini A. thmeticorum libri sex; et numeris multiangulis liber unus. Nunc primum graece et latine editi atque absolutissimis comentariis illustrati". Una edición muy cuidada de la obra de Diofanto fue hecha en Leipzig, en 1895, por Paul Tannery.

Pierre-Simon de Fermat (1601-1665) poseía un ejemplar de la edición Bachet de la Aritmética de Diofanto y, al lado del antes citado problema 8, escribió la siguiente nota:

"Por el contrario, es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados y, en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente. He encontrado una demostración realmente maravillosa, pero el margen del libro es demasiado estrecho para ponerla".

La imposibilidad de resolver en enteros, no nulos, la ecuación

$$x^n + y^n = z^n$$

para $n \geq 3$, se viene conociendo con el nombre de "el último Teorema de Fermat". Obviamente basta considerar los casos en que $n=4$ o bien $n = p$, siendo p un entero primo impar. De las tentativas hechas hasta hoy para superar la incomodidad de la estrechez de un margen, intentaremos hacer un breve resumen a continuación.

2. Resultados de Fermat. Si bien el ejemplar Bachet que Fermat poseía se perdió, las notas que en él escribiera fueron publicadas por su hijo, Samuel Fermat, en Tolosa, en 1670. Hoy pueden leerse en la edición de P. Tannery y Ch. Henry de sus obras completas. Es de notar que, el que puede considerarse fundador de la moderna Teoría de Números, no publicó prácticamente nada duran

te su vida. Ello, en opinión de A. Weil, se debió al aislamiento en que trabajaba. En una época en que los analistas tenían ya que luchar por defender sus prioridades, Fermat, a lo largo del siglo XVII, está practicamente sólo (como después, lo estaría Euler, en la primera mitad del siglo XVIII, hasta que no se produjo la incorporación de Lagrange).

En dichas notas, Fermat demuestra la imposibilidad de resolver en enteros la ecuación

$$x^4 - y^4 = z^2$$

que, obviamente, implica que la ecuación $x^4 = y^4 + z^4$ carece de soluciones enteras. Se llega a la antes citada ecuación, al intentar demostrar que no existe ningún triángulo rectángulo de lados enteros, cuya área sea el cuadrado de un número entero (un problema de "cuadratura de triángulos"). El método seguido en la demostración es el célebre método de Fermat, de descenso infinito (véase [7]).

En una carta, sin fecha, Fermat afirma haber demostrado el caso $n = 3$, también por descenso infinito, pero esta demostración no pudo ser hallada.

3. Primeros intentos. Leonhard Euler (1707-1783) tomó como punto de partida de sus investigaciones aritméticas las, muchas veces enigmáticas, notas de Fermat. En su estudio del caso $n = 3$ de la citada ecuación, la demostración de Euler se iniciaba como sigue (cf. [15]): Sin restricción se puede suponer que $\text{mcd}(x,y,z) = 1$, que x e y son impares, y que z es par. Haciendo el cambio de variables $x + y = 2a$, $x - y = 2b$, $\text{mcd}(a,b) = 1$, y tras sustituir, se llega a la ecuación $2a(a^2 + 3b^2) = z^3$. Un sencillo cálculo prueba que $\text{mcd}(2a, a^2 + 3b^2) = 1$ o bien que $\text{mcd}(2a, a^2 + 3b^2) = 3$, en cuyo caso z debe ser un múltiplo de 3. La primera de estas dos citadas

posibilidades conduce a que debe existir un entero r, tal que $a^2 + 3b^2 = r^3$. Esta igualdad llevó a Euler a afirmar que <u>debían existir</u> enteros c, d, tales que

$$a + b\sqrt{-3} = (c + d\sqrt{-3})^3.$$

En la afirmación anterior se encuentra la idea germinal de la aritmética de los cuerpos de números. Euler procedía como si $Z[\sqrt{-3}]$ hubiera sido un anillo factorial. En efecto, en un tal caso, existirían elementos primos $\pi_i \in Z[\sqrt{-3}]$, tales que $a + b\sqrt{-3} = \varepsilon \pi_1^{s_1} \cdots \pi_k^{s_k}$, siendo $\varepsilon = \pm 1$ y $s_i \geq 1$; al tomar normas en la extensión $Q(\sqrt{-3})/Q$, y teniendo en cuenta que $mcd(a,b) = 1$, se obtendría que $a^2 + 3b^2 = p_1^{s_1} \cdots p_k^{s_k}$ siendo los elementos $p_i, 1 \leq i \leq k$, enteros primos distintos. Con lo cual, la igualdad $a^2 + 3b^2 = r^3$ obligaría a que s_i fuera múltiplo de 3 y por tanto, a que $a + b\sqrt{-3}$ fuera, efectivamente, un cubo en $Z[\sqrt{-3}]$.

Si bien $Z[\sqrt{-3}]$ no puede ser factorial, pues ya que no es enteramente cerrado, si que lo es su clausura entera, igual al anillo de las raices terceras de la unidad $Z[\zeta_3]$. Ello explica que posteriormente pudiera demostrarse el caso n = 3, partiendo de la idea dada inicialmente por Euler.

La solución de muchos de los problemas propuestos por Fermat, la dió Euler en el segundo de los volúmenes de que consta su obra "Vollständige Anleitung der Algebra", publicada en 1770. En 1774 se publicó una segunda edición, en francés, comentada por Lagrange.

Trabajando directamente en el anillo $Z[\zeta_3]$, Gauss, en su obra póstuma, dió otra demostración del caso n = 3 de la ecuación de Fermat. En 1825 Legendre y Direchlet probaron el caso n = 5, y en 1843 Lamé y V.A. Lebesgue, el caso n = 7.

4. Trabajos iniciales de Kummer. Ernst Eduard Kummer (1810-1893) entregó, en 1843, un manuscrito a Dirichlet en el que creía haber probado el caso general del Teorema de Fermat. Dirichlet le hizo notar que, para que su demostración fuera correcta, era necesario que en el anillo $Z[\zeta_p]$ de las raices p-ésimas de la unidad, no sólo todo elemento se expresara como producto de factores irreducibles, sino que además esta descomposición tenía que ser única; hecho improbable, sobre el cual tenía serias dudas.

La no existencia de soluciones enteras de la ecuación $x^p + y^p = z^p$, p entero primo ≥ 3, en las que $p \nmid x\,y\,z$ se conoce con el nombre de primer caso del Teorema de Fermat. El segundo caso se presenta al considerar las posibles soluciones en las que $p \mid z$.

La demostración de Kummer, en el caso de factorización única, parte de las consideraciones siguientes. Introduciendo una raíz primitiva p-ésima de la unidad, $\zeta = \zeta_p$ la ecuación de Fermat puede ponerse bajo la forma

$$\prod_{i=1}^{p-1} (x+\zeta^i y) = z^p \ .$$

En el primer caso del Teorema de Fermat se demuestra que, si $i \not\equiv j \pmod p$, los elementos $x+\zeta^i y$, $x+\zeta^j y$ carecen de factores comunes no triviales. Así si $Z[\zeta]$ es un anillo factorial, deben existir, en particular, elementos α_i , $\varepsilon_i \in Z[\zeta]$, ε_i unitarios, de forma que

$$x+\zeta y = \varepsilon_1 \alpha_1^p$$

$$x-\zeta z = \varepsilon_2 \alpha_2^p \ .$$

La simultaneidad de ambas igualdades se demuestra que es contradictoria. A su vez, el elemento $1-\zeta$ es siempre irreducible en $Z[\zeta]$ y p admite la descomposición $p=(1-\zeta)^{p-1}\varepsilon$, siendo ε un ele-

mento unitario de $Z[\zeta]$. Así, en el segundo caso, si $z = p^k z_0$ $k \geq 1$, $p \nmid z_0$, la ecuación de Fermat puede escribirse en la forma

$$x^p + y^p = (1-\zeta)^{k(p-1)} \varepsilon^p z_0^p .$$

Se demuestra, en el caso de factorización única, que esta igualdad es asimismo contradictoria (véase [4]).

En 1847 Lamé, intentando demostrar el caso general del Teorema de Fermat, cae en el mismo error que Kummer, de suponer la fatorialidad de $Z[\zeta_p]$. Ello es advertido por Cauchy, quien, usando un algoritmo de división por medio de la norma, cree haber demostrado que tales anillos son euclídeos y por tanto, factoriales. Más tarde, el propio Cauchy se daría cuenta de que su demostración era incorrecta.

La no factorialidad de ciertos anillos de la forma $Z[\sqrt{d}]$ ya había sido advertido por Lagrange, revisando los trabajos de Euler. Usando la teoría de formas cuadráticas de Gauss, Kummer demuestra que en $Z[\zeta_{23}]$ tampoco puede llevarse a cabo una teoría de divisibilidad como en el caso de Z. Todos los esfuerzos de Kummer para superar tal dificultad quedan plasmados en una serie de artículos, aparecidos entre 1845 y 1847, y que son la base de la actual Teoría de ideales. La falta, en general, de descomposición única en factores primos en los anillos $Z[\zeta_p]$ es evitada mediante descomposiciones de "números ideales" en producto de "números primos ideales", de manera única (ideales, respectivamente ideales primos, en la terminología actual). El conocimiento preciso de las reglas de descomposición de un entero como producto de números primos ideales, llevaría a Kummer a un estudio equivalente al del cálculo de todas las valoraciones de un cuerpo de raices de la unidad.

§. Evolución de las ideas de Kummer. Al intentar Dedekind extender la teoría de la divisibilidad de Kummer a anillos de la forma $Z[\sqrt{d}]$, d entero no divisible por ningún cuadrado, ve que ello sólo es posible si $d \equiv 2 \pmod 4$ ó $d \equiv 3 \pmod 4$. En otras palabras, un tal anillo debía ser enteramente cerrado. Aparecía así por primera vez, la noción de elemento entero sobre un anillo. Fue realmente una suerte que en las investigaciones iniciales de Kummer, $Z[\zeta]$ fuera precisamente el anillo de los enteros de $Q[\zeta]$.

Veamos, con un sencillo ejemplo, como se resuelve la falta de unicidad en las descomposiciones, por medio de la teoría de ideales. En $Z[\sqrt{-5}]$ consideremos las dos descomposiciones

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1-2\sqrt{-5}).$$

Los elementos $3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ son irreducibles en $Z[\sqrt{-5}]$ y sin embargo el 3, por ejemplo, no divide ni a $1+2\sqrt{-5}$, ni a $1-2\sqrt{-5}$. Teniendo en cuenta las reglas de descomposición en un cuerpo cuadrático (véase, por ejemplo [4]), deben existir ideales primos p_i en $Z[\sqrt{-5}]$ tales que los ideales principales generados por los anteriores elementos se expresen en la forma:

$$(3) = p_1 p_2 \qquad (7) = p_3 p_4$$
$$(1+2\sqrt{-5}) = p_1 p_3 \qquad (1-2\sqrt{5}) = p_2 p_4 .$$

Con ello $(21) = p_1 p_2 \cdot p_3 p_4 = p_1 p_3 \cdot p_2 p_4$ y el ideal principal (21) pasa a tener una descomposición única.

En 1871, Dedekind, en el suplemento al texto de Direchlet "Vorlesungen über Zahlentheorie", probó la existencia y unicidad de descomposición de un ideal en producto de ideales primos en el anillo de los enteros de cualquier cuerpo de números. Lasker, en 1905, se preocupó de la existencia de tales descomposiciones

en los anillos de polinomios $\mathbb{C}[X_1,\ldots,X_n]$. Introduce la noción de ideal primario, ya implícita en la obra de Dedekind, y ve que en dicho anillo todo ideal puede expresarse como intersección de ideales primarios. E. Noether , en 1921, probaba que la existencia de una tal descomposición resulta de la condición de cadena ascendente, apareciendo de este modo la noción de anillo "noetheriano" y en 1927, daba la caracterización axiomática de los anillos en los que era válida una descomposición "al modo de Kummer", de todo ideal en producto único de ideales primos. Estos eran los anillos noetherianos, enteramente cerrados y tales que todo ideal primo no nulo era maximal, es decir, los que hoy llamamos anillos de Dedekind.

El paso de la teoría de ideales a la teoría de valoraciones sería hecho por Krull en 1931.

6. El concepto de número de clases. La medida en que un anillo de Dedekind deja de ser factorial, la da su número de clases. Sea A un tal anillo y M el monoide de los ideales de A (con la operación de producto), por medio de la introducción de los ideales fraccionarios, M puede incluirse, de manera natural, en un grupo. Si K es el cuerpo de fracciones de A, un ideal fraccionario es, por definición, un A-submódulo de K finitamente generado; un tal ideal puede escribirse en la forma $x^{-1}b$, siendo b un ideal de A ordinario y x, un elemento de A no nulo. El conjunto I de todos los ideales fraccionarios del anillo de Dedekind A, mediante la operación de producto, tiene estructura de grupo y, obviamente, contiene a M. Los ideales fraccionarios de la forma yA, $y \in K^*$, constituyen un subgrupo P de I, llamado de los ideales principales. El cociente I/P es el grupo de las clases de A. Su cardinal, representado usualmente por $h(A)$, o simplemente por h, es el llamado número de clases del anillo A. La condición $h = 1$ se presenta si y sólo si todos los ideales de A son principales y es equivalente, por ser A de Dedekind, a la facto-

rialidad de A. Cuando A es el anillo de los enteros de un cuerpo de números K, h se denomina simplemente el número de clases de K.

Bajo un lenguaje distinto, concretamente con el de la teoría de las formas cuadráticas, la idea de número de clases se encuentra explícita en la obra de Gauss "Disquisitiones Arithmeticae", publicada en Leipzig en 1801. La idea de ideal fraccionario se encuentra ya en la obra de Kummer, quien, en 1847, prueba la finitud de h en los cuerpos ciclotómicos. La finitud de h para un cuerpo de números arbitrario, aparece ya en el antes citado texto de Dirichlet.

7. Primos regulares y primos irregulares. Sea ahora h el número de clases del cuerpo ciclotómico $Q[\zeta_p]$, p entero primo ≥ 3. La demostración del Teorema de Fermat en el caso en que $h = 1$, fue extendida por Kummer en 1847 a todos los primos p tales que $p \nmid h$ (véase [4]). Ello condujo a Kummer a clasificar los primos en regulares y en irregulares, de modo que un primo $p \geq 3$ es regular si y sólo $p \nmid h$, siendo h el número de clases de $Q[\zeta_p]$. Para tener una idea de en qué grado este resultado mejoraba el primitivo resultado de Kummer, mencionaremos que entre los primos $p < 100$, sólo el 3,5,7,11,13,17 y 19 dan número de clases igual a uno, mientras que únicamente el 37,59 y el 67 son primos irregulares. El entusiasmo inicial de Kummer le llevó a titular su artículo: "Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ". Digamos que, hasta hoy en día, no se ha logrado probar que el conjunto de primos regulares sea infinito. Sin embargo, como más adelante se comentará, se sabe que es infinito el de los primos irregulares. En todos los intervalos estudiados dominan los primos regulares sobre los irregulares.

Dos preguntas quedaban formuladas tras estos resultados de Kummer:

1) ¿Cómo reconocer si un primo era o no regular?

2) ¿Cómo debía procederse en el caso irregular?

De ambas nos ocuparemos a continuación. Para responder a la primera de ellas, se imponía un estudio más profundo del número de clases; para dar una idea de cómo se abordó, tenemos que dar un paso atrás en el tiempo.

8. La función zeta. Es bien sabido que la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{R},$$

es convergente si $s>1$ y divergente si $s \leq 1$. Escribamos, de acuerdo con la notación introducida por Riemann, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, si $s>1$. El cálculo de $\zeta(2)$ aparece propuesto en 1650 en un texto de Pietro Mengoli, profesor de mecánica de Bolonia. Tras diversas tentativas hechas por Wallis, Leibnitz y Daniel Bernouilli, en 1734, Euler, usando por primera vez productos infinitos, dió el resultado

$$\zeta(2) = \frac{\pi^2}{6}.$$

En 1737 obtenía Euler la siguiente descomposición en producto infinito

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}}, \qquad s > 1,$$

en donde el producto se extiende a todos los enteros primos, y en 1740 daba el valor de la función ζ en todos los enteros positivos pares:

$$\zeta(2m) = \frac{(-1)^{m-1} B_{2m} (2\pi)^{2m}}{2(2m)!} \quad , \quad m \in Z, \quad m > 0,$$

siendo B_{2m} números racionales, los llamados números de Bernouilli. Vienen dados por el desarrollo en serie siguiente:

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{m=2}^{\infty} \frac{B_m}{m!} x^m \quad , \quad |x| < 2\pi .$$

Fácilmente se ve que $B_{2m+1} = 0$, si $m \geq 1$.

Riemann, en 1860, en su estudio sobre la distribución de los números primos, ve que la función $\zeta(s)$ se prolonga analíticamente a una función meromorfa del plano, con un único polo, de residuo igual a uno, en $s = 1$. De manera paralela, Dedekind introduciría la función zeta para un cuerpo de números arbitrario K:

$$\zeta_K(s) = \sum_{\mathfrak{b}} \frac{1}{N(\mathfrak{b})^s} \quad , \quad s > 1,$$

en donde el sumatorio se extiende a todos los ideales del anillo de los enteros de K y $N = N_{K/Q}$ indica la norma. Para una tal función es válida también una descomposición en producto infinito

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \quad , \quad s > 1,$$

en donde el producto se extiende ahora a todos los ideales primos de K. Por prolongación analítica se obtiene también una función meromorfa del plano, con un único polo en $s = 1$ y con residuo dado por

$$\lim_{s \to 1} (s - 1) \zeta_K(s) = \varkappa h \quad ,$$

siendo $\varkappa$ una constante no nula que depende de K y h el número de

clases de K.

9. Resultados de Kummer 1850. Haciendo uso de la correspondiente función zeta, Kummer , ayudado por resultados obtenidos previamente por Dirichlet, ve que el número de clases h del cuerpo ciclotómico $Q[\zeta_p]$. admite una descomposición

$$h = h_1 \, h_2$$

siendo h_1, h_2 enteros ≥ 1, y de forma que h_2 es igual al número de clases del cuerpo real maximal $Q[\zeta_p + \zeta_p^{-1}]$, contenido en $Q[\zeta_p]$.

En 1850 Kummer demostró que si $p \geq 3$ es un entero primo tal que $p \nmid h_1$, entonces $p \nmid h_2$ y que p dividía a h_1 si y sólo si p dividía a alguno de los numeradores de los números de Bernouilli B_{2m}, para $1 < 2m \leq p-3$. Escribiendo $B_{2m} = P_{2m}/Q_{2m}$, en donde P_{2m}, Q_{2m} son enteros y $m.c.d(P_{2m}, Q_{2m}) = 1$, se obtenía de esta forma el siguiente:

Criterio de regularidad de Kummer.- Un entero primo $p \geq 3$ es regular si y sólo si $p \nmid P_2, P_4, \ldots, P_{p-3}$.

Puesto que los números de Bernouilli pueden calcularse de forma recurrente, quedaba así contestada la primera de las preguntas antes formuladas.

La Academia Francesa de Ciencias había ofrecido un premio de 3.000 francos de oro para el matemático que lograra dar una demostración general del Teorema de Fermat, o por el contrario, probara su falsedad. En 1850 concurrieron al premio cinco memorias, declarándose desierto. Otro tanto ocurrió en 1853, presentándose entonces once memorias. Una tercera convocatoria tuvo lugar en 1857. La Academia decidió entonces, puesto que las memorias presentadas no reunían los méritos suficientes, otorgar el premio a E.E. Kummer, aunque no era aspirante al mismo, "... pour ses belles recherches sur les nombres complexes composés de racines de l'unité et de nombres entiers" (C.R. Acad. Sci., Paris, XLIV, 158 (1857)).

10. El caso irregular. En 1915, K.L. Jensen probó que existían infinitos primos irregulares de la forma $4n+3$. En 1954, L. Carlitz dió una demostración sencilla del resultado, más débil, de la existencia de infinitos primos irregulares. La demostración de la existencia de infinitos primos irregulares se basa en un teorema de von Staudt-Clausen que afirma que, para todo entero $m \geq 1$, existe un entero $G(m)$ tal que

$$B_{2m} = G(m) - \left(\frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_r}\right),$$

siendo $p_1, \ldots, p_r$ todos los enteros primos distintos para los cuales $2m \equiv 0 \pmod{(p_i - 1)}$. Obsérvese que, mientras que los divisores de P_{2m} son difíciles de hallar, los de Q_{2m} los proporciona el resultado anterior.

Respecto a la densidad relativa:

$$\lim_{n \to \infty} \frac{\text{Nº de primos irregulares} \leq n}{\text{Nº de primos regulares} \leq n},$$

se ha conjeturado que era igual a $\frac{1}{2}$ (Kummer), igual a 1 (Hensel) o igual a $e^{1/2} - 1 \doteq 0{,}6487$ (Siegel). Digamos al respecto que en 1874, Kummer había examinado todos los primos $p \leq 163$, encontrando 29 regulares y 8 irregulares. H.S. Vandiver, en 1930, mediante un calculador manual, llegó hasta el 617, encontrando 74 primos regulares y 38 irregulares. En 1955, Vandiver, D.H. Lehmer, E. Lehmer, J.L. Selfridge y C.A. Nicol con un ordenador SWAC llegaron hasta el 4001, encontrando 334 primos regulares y 216 irregulares. En 1975, W.Johnson, con un ordenador PDP-10, examinó todos los primos $p < 30.000$, de los cuales 1971 han resultado ser regulares y 1273 irregulares. El cociente $1273/1971 \doteq 0{,}6459$ parece dar la razón a Siegel.

Si p es un primo irregular y $p \mid P_{2k}$ para cierto k tal que

$1 < 2k \leq p-3$, se dice que (p, 2k) es un par irregular. Fijado p, el número de tales pares se llama el índice de irregularidad de p. Dado un primo p próximo a 30.000, en el programa de Johnson, saber si es regular o irregular, y en este caso determinar su índice de irregularidad, requiere un tiempo de unos 22 minutos.

En su intento de responder a la segunda de las preguntas anteriormente formuladas, Kummer, en 1857, creyó haber encontrado un criterio que le permitía demostrar el Teorema de Fermat en los casos p = 37, 59, 67. En 1920, Vandiver advirtió que la demostración de Kummer no era del todo correcta. Sin embargo, pudo corregirse y ello condujo a la publicación , 1954, por parte de Vandiver, D.H. Lehmer y E. Lehmer del siguiente criterio para el caso irregular:

Teorema.- Sea p un primo irregular y supongamos que $P = rp + 1$, sea un primo satisfaciendo $P < p^2 - p$. Sea t un entero tal que $t^r \not\equiv 1 \pmod{P}$. Para cada par irregular (p,2k), formemos el producto

$$N_{2k} = t^{-rd/2} \prod_{b=1}^{m} (t^{rb} - 1)^{b^{p-1-2k}}$$

en donde $m = (p-1)/2$ y $d = \sum_{n=1}^{m} n^{p-2k}$. Si, para todos los pares irregulares se verifica que $N_{2k}^r \not\equiv 1 \pmod{P}$, entonces el Teorema de Fermat es válido para el exponente p.

El criterio ha sido aplicado por Johnson para todos los primos irregulares < 30.000, con éxito. En todos los casos ha bastado tomar $t = 2$ y el menor primo P con las condiciones requeridas.

11. Algunas conjeturas. En 1934 Vandiver conjeturó que el segundo factor del número de clases, h_2, no era nunca divisible por p y probó, bajo la hipótesis $p \nmid h_2$, que el primer caso del Teorema de Fermat era válido. Dicha conjetura se verifica

para todos los primos $p < 30.000$. Sin embargo, una conjetura anterior que afirmaba que h_2 era siempre igual a 1, fue desmentida en 1965 por Ankeny, Chowla y Hasse.

En 1959, K. Iwasawa, en su estudio de las extensiones Γ de un cuerpo de números algébricos, probó que si $p^{e(n)}$ es la máxima potencia de p que divide al número de clases del cuerpo ciclotómico $Q\,[\zeta_{p^n+1}]$, existían tres enteros $\mu_p \geq 0$, $\lambda_p \geq 0$ y ν_p, tales que

$$e(n) = \mu_p p^n + \lambda_p n + \nu_p \ ,$$

para todo n suficientemente grande. Si p es regular, se sabe que $\mu_p = \lambda_p = \nu_p = 0$. Los invariantes ciclotómicos de Iwasawa han sido calculados para todos los primos $p < 30.000$, obteniéndose en todos los casos que $\mu_p = 0$ y $\lambda_p = \nu_p$ = índice de irregularidad de p. Lo cual parece suficiente... para emitir una conjetura.

Se han encontrado únicamente dos primos (< 30.000), el 12.613 y el 15.737, con índice de irregularidad igual a 4 y ninguno, de índice ≥ 5. Se sospecha que el índice de irregularidad no está acotado, pero no se ha podido probar hasta hoy que existan infinitos primos irregulares de índice ≥ 2.

12. Epílogo. Paul Wolfskehl dejó a la Academia de Ciencias de Göttingen en 1907, un legado de 100.000 marcos como premio para quien lograra demostrar el Teorema de Fermat. Aunque como decía el profesor L.J. Mordell, haya otras maneras más sencillas de hacer dinero, recordamos que el plazo de presentación de trabajos expira el 13 de Septiembre del año 2.007.

BIBLIOGRAFIA

[1] Ankeny, N.C., Chowla,S., Hasse,H.: On the class-number of the maximal real subfield of a cyclotomic field. J.Reine Angew. Math. 217 (1965), 217-220.

[2] Ayoub, R.: Euler and the zeta function. Amer. Math. Monthly 81 (1974), nº 10, 1067-1068.

[3] Ball, W.W.R.: A Short Account of the History of Mathematics. Dover Publ., 1960.

[4] Borevitch,Z.I., Shafarevitch,I.R.: Théorie des Nombres. Gauthier-Villars, 1967.

[5] Bourbaki, N. : Éléments d'Histoire des Mathématiques. Hermann, 1969.

[6] Carlitz, L.: Note on irregular primes. Proc. Amer. Math. Soc. 5 (1954), 329-331.

[7] Dickson, L.E.: History of the Theory of Numbers, vol. II. Chelsea, 1919, Reimpr. en 1971.

[8] Diofanto de Alejandría: Aritmética. Col. Científicos griegos. Aguilar, 1970.

[9] Dirichlet, P.G.L., Dedekind,R.: Vorlesungen über Zahlentheorie. Chelsea, 1893, 4ª ed. Reimpr. en 1968.

[10] Gauss, C.F.: Disquisitiones Arithmeticae. Trad. inglesa de A.A. Clarke. Yale University Press, 1966.

[11] Iwasawa, K.: On Γ-extensions of algebraic number fields. Bull. Amer. Math. Soc. 65 (1959), 183-226.

[12] Johnson, W.: Irregular Primes and Cyclotomic Invariants. Math. Comput. 29 (1975), nº 129, 113-120.

[13] Kummer,E.E.: Collected Papers, Vol. I. Ed. por A. Weil. Springer, 1975.

[14] Lehmer, D.H., Lehmer, E., Vandiver, H.S.: An Application of high-speed computing to Fermat's last Theorem. Proc. Nat. Acad. Sci. U.S.A. 40 (1954), 25-33.

[15] Mordell, L.J.: Tow papers on Number Theory. Deutscher Verlag der Wissenschaften, 1972.

[16] Selfridge, J.L., Nicol, C.A., Vandiver, H.S.: Proof of Fermat's last Theorem for all prime exponents less than 4002. Proc. Nat. Acad. Sci. U.S.A. 41 (1955), 970-973.

[17] Siegel, C.L.: Zu zwei Bermerkungen Kummers. Nachr. Acad. Wiss. Göttingen 6 (1964), 51-57.

[18] Vandiver, H.S.: On Kummer's memoir of 1857 concerning Fermat's last Theorem. Proc. Nat. Acad. Sci. U.S.A. 6 (1920), 266-269.

[19] Vandiver, H.S.: Fermat's last Theorem and the second factor in the cyclotomic class number. Bull. Amer. Math. Soc. 40 (1934), nº 2, 118-126.

[20] Weil, A.: Two Lectures on Number Theory, Past and Present. Enseignement Math. (2) 29 (1974), 87-110.