Una respuesta a la última hipótesis de Fermat

JOSÉ ANTONIO ESTRUGO ESTRUGO
Catedrático de Análisis Matemático y Matemática Financiera
Escuela Universitaria de Estudios Empresariales
Universidad Complutense de Madrid

1. CONJETURAS Y PROPOSICIONES

La Teoría de Números se caracteriza por contener, además de los teoremas fundamentales que integran sus principios científicos, una amplia gama de proposiciones y conjeturas marginales que no alcanzan la categoría de teoremas. Son proposiciones para las que no se ha encontrado una demostración general, o para las que, al verificarlas, se observa que se cumplen para determinados valores consecutivos de n (n=1, 2, 3...) pero fallan en algunos otros.

Estas particularidades de las proposiciones marginales hacen que dé la sensación de que el matemático pierde el tiempo investigando, cuando, a nuestro entender, pueden servir como punto de partida para dirigir la investigación en sentidos complementarios, como intentamos hacer al crear el «Taorema»*.

Hemos de resaltar que precisamente esas proposiciones y conjeturas son las que han tenido históricamente, y tienen en la actualidad, mayor resonancia entre matemáticos y aficionados. Esto parece deberse tanto a su reto desafiante tras siglos de investigación, como a los potentes recursos de análisis matemático que normalmente se han tenido que utilizar para demostrar enunciados aparentemente sencillos.

Por ejemplo, Gauss (1777-1855) formuló una conjetura sobre la distribución de los números primos que interpretó a través de la función logarítmica, tardándose cerca de un siglo en obtenerse una demostración por Hadamard y de la Vallée Poussin.

Uno de los casos más notables de estas proposiciones es la llamada «última hipótesis» de Fermat (1.601-1665), que todavía no ha sido resuelta, tras más de tres siglos y medio de investigación.

Según Eric Temple, esta última hipótesis ha prestado un gran servicio a las matemáticas. En efecto, ha instigado el desarrollo de la teoría de números algebraicos. Esta teoría influyó sobre algunos conceptos primor-

* *Definición de Taorema y sus aplicaciones a la Teoría de Números.* ESTRUGO ESTRUGO, J. A. Gaceta Matemática, 1.ª Serie, Tomo XXI, núms. 1 y 2, 1969.

diales, como por ejemplo, los números imaginarios en el álgebra, que luego han actuado directamente sobre la física matemática moderna.

Sobre esta base, Kummer ya había demostrado la hipótesis de Fermat en 1.850 para todos los exponentes menores que 100. Posteriores desarrollos, en los que ha intervenido incluso la informática, han superado los valores primos de p hasta 125.000. Sin embargo, Kummer no consiguió la generalización que pretendía.

Hasta ahora, todos los intentos de demostración general de que la ecuación $X^p + Y^p = Z^p$ es imposible, han tenido que distinguir dos casos: p no divide a ninguno de los números X, Y, Z; p divide uno de ellos. El segundo caso parece ser, con mucho, el más difícil.

Para el primer supuesto, J.B. Rosser demostró en 1.940 que la hipótesis era cierta para todos los exponentes primos impares que no rebasaran 41.000.000. Esto fué elevado en 1941 por D.H. Lehmer y E. Lehmer hasta 253.747.889.

Para la segunda posibilidad, el límite superior hasta 1950 era de 607 por H.S.Vandive.

En 1.983 Gerd Faltings consiguió demostrar el primer resultado general relacionado con este tema, aunque sólo fuera una conclusión parcial. Estableció que si la hipótesis de Fermat tiene soluciones, éstas son un número finito para un exponente mayor o igual que tres. Para llegar a este resultado, Faltings tuvo que demostrar previamente las verdades intuídas pero indemostradas de Mordell, Tate y Shaferevitch.

2. LA ULTIMA HIPOTESIS DE FERMAT

El análisis indeterminado tiene como finalidad investigar si ciertas ecuaciones de varias incógnitas admiten soluciones enteras y hallar su expresión general.

Diofanto de Alejandría, matemático del siglo IV, fué el primero en ocuparse de este problema. También Fermat se interesó en él, acerca del que enunció su proposición: Hallar todos los triángulos rectángulos cuyos lados tienen medidas expresadas en números enteros, es decir, resolver en números enteros la ecuación indeterminada:

$$X^2 + Y^2 = Z^2$$

Resuelta de forma elemental esta ecuación, aparece la pregunta de si un cubo puede ser la adición de dos cubos y, en general, si un número elevado a una potencia cualquiera puede ser la suma de dos potencias del mismo grado.

Fermat contestó negativamente a esta pregunta en 1.637 en una anotación marginal, escrita en latín, en el libro «Obras de Diofanto» que acababa de ser editado y enriquecido con comentarios de Bachet de Méziriac, que traducida al castellano, significa:

«No es posible dividir un cubo en dos cubos, ni un bicuadrado en dos bicuadrados y, de manera general, una potencia cualquiera de exponente superior a dos en dos potencias de la misma especie. He descubierto una demostración notable de esta proposición, pero no cabría en el margen»

Por desdicha esta demostración general nunca se encontró.

Fermat sólo dejó el principio del método que empleó para los bicuadrados: Por reducción al absurdo. Consiste en demostrar que, si la ecuación fuera posible, se podría deducir de ella otra con la misma forma pero con números X, Y y Z menores y, de esta forma, sucesivamente, lo que sería imposible ya que los números que fueran solución se suponen siempre no nulos.

Fermat llamó a esta metodología «Descenso Infinito», sin entrar en mayores detalles, en una carta dirigida a su amigo Carcavi, conservada en la biblioteca de Leiden. Siguiendo las indicaciones de Fermat, Frenicle de Bessy, otro amigo del matemático, reconstruyó la demostración en su «Tratado de los triángulos rectángulos en Números», publicado en 1676.

3. REDUCCION DEL CAMPO DE INVESTIGACION

3.1. En relación con las bases

Dada la ecuación indeterminada

$$X^n + Y^n = Z^n \qquad (1)$$

si el máximo común divisor de (X, Y, Z) es r, dividiendo (1) entre r^n, obtenemos

$$X_1^n + Y_1^n = Z_1^n \qquad (2)$$

Siendo ahora el máximo común divisor de X_1, Y_1, Z_1 igual a 1, serán primos entre sí. Sin embargo, si dos números cualquiera de ellos tuviera un mismo factor común, sustituídos en (2), obligarán al tercero a contenerlo también, por lo que X, Y, Z tienen que ser primos dos a dos. De aquí que, fijado un número primo cualquiera, sólo puede contenerlo como factor uno de los tres.

De lo anterior se deduce que del grupo (X, Y, Z) uno de ellos tiene que ser par y los otros dos impares.

3.2. Limitación de Talbot

La desigualdad $(X + Y)^n > X^n + Y^n = Z^n$ es manifiesta. Si extraemos la raiz n-ésima de los extremos, obtendremos $X + Y > Z$. También, como

$Z > X$ y $Z > Y$, resulta, por adición que $2Z > X + Y$, lo que nos permite escribir

$$Z < X + Y < 2Z \tag{3}$$

limitación deducida por Talbot y usada por él para demostrar que, si Z es un número primo, (1) es imposible.

3.3. Reducción acerca de exponentes

Bastaría hacer la demostración para los casos en que el exponente fuera cuatro y para aquel en que el exponente fuera p, un número primo impar.

a. En el primer caso, si el exponente no es divisible por ningún primo impar, será una potencia de dos. Pero como se supone mayor de dos, tiene que ser cuatro o divisible por cuatro, $n = 4m$, pudiendo escribirse

$$(X^m)^4 + (Y^m)^4 = (Z^m)^4 \tag{4}$$

Pero esta ecuación es imposible, señalado por Fermat y demostrado por Frenicle de Bessy.

b. Demostrada la imposibilidad del primer caso, nos queda estudiar aquél en el que exponente es un número primo impar.

Suponiendo n divisible por un número primo impar p, $n = mp$, se obtiene

$$(X^m)^p + (Y^m)^p = (Z^m)^p \tag{5}$$

Por consiguiente, en lo sucesivo, analizaremos la posibilidad de la ecuación

$$X^p + Y^p = Z^p$$

para p primo impar.

4. PROPIEDADES Y TEOREMAS BASICOS

4.1. Metodología

Como indicamos en la introducción, pese a los esfuerzos realizados por eminentes matemáticos a lo largo de siglos de investigación, queda aún pendiente por resolver, del amplio enunciado inicial, la imposibilidad de la ecuación

$$X^p + Y^p = Z^p,$$

para X, Y, Z, primos entre si dos a dos con exponente p primo impar, habiéndose conseguido, además, ya en estas condiciones, su demostración para numerosos casos particulares.

A nuestro entender, hemos resuelto el problema, utilizando un artificio, de forma que dicha solución queda condicionada al cumplimiento de una propiedad elemental de divisibilidad algebraica.

El artificio indicado parte de un principio lógico: «Una supuesta igualdad numérica no es cierta si al dividir sus dos miembros por un mismo número, no nulo, se obtienen resultados contradictorios»

Al aplicar dicho artificio en la igualdad fundamental $X^p + Y^p = Z^p$, tomando como divisor común el formado por $X + Y$, nos ha llevado a estudiar con más detenimiento la ley del resto de Ruffini, para el caso particular de la divisibilidad de su primer miembro

$$\frac{X^p + Y^p}{X + Y}$$

descubriendo dos formas de ser entera, lo que nos ha permitido llegar a la solución del problema con carácter general.

A fin de evitar la discontinuidad en la lectura, relacionamos a continuación el conjunto de propiedades y teoremas que nos han servido de base para el desarrollo del trabajo y que, en su caso, aparecerán demostrados en los Apéndices los no intercalados en el texto.

4.2. Propiedades que se utilizarán

I

En la ecuación diofántica $X^p + Y^p = Z^p$, (siendo p número primo impar), X, Y, Z deben ser primos entre sí dos a dos, uno de ellos par y los dos restantes impares.

II

Sin quitar generalidad, podemos admitir que

$$X < Y < Z$$

III

Aplicando la congruencia de Fermat, a cada valor de los tres números de la ecuación

$$X^p + Y^p = Z^p \qquad (6)$$

podemos considerar evidente la congruencia

$$X^p + Y^p - Z^p \equiv X + Y - Z \text{ (mód p)} \tag{7}$$

válida para cualquier valor de X, Y, Z.

Si admitimos la igualdad (6), podremos escribir

$$X + Y - Z \equiv 0 \text{ (mód p)}$$

cuyas soluciones son

a) $X + Y - Z = 0$
b) $X + Y - Z = kp$

o lo que es lo mismo

a) $Z = X + Y$
y b) $Z + kp = X + Y$

La primera solución, a), da un valor $Z = X + Y$ que no satisface la desigualdad de Talbot, $Z < X + Y$.

La segunda, b), suministra un valor plausible,

$$Z + kp = X + Y \tag{8}$$

que consideramos *igualdad fundamental.*

En ella, al ser $Z > Y$, entonces

$$kp < X \tag{8'}$$

para que se cumpla dicha igualdad, debiendo, además, ser k un número par.

IV

Igualmente el número Z o el formado por X + Y no pueden ser números primos, ya que la ecuación

$$X^p + Y^p = Z^p$$

no sería posible en cada caso.

V

La relación

$$\frac{Z^p}{X + Y}$$

no es entera si Z o X + Y son números primos, puesto que, de acuerdo con la limitación de Talbot, $Z < X + Y < 2Z$, si Z fuera primo, todos los números comprendidos entre Z y 2Z son primos con él, encontrándose entre ellos X + Y; y si la suma X + Y fuera un número primo, lo serían con él todos sus inferiores, donde figura Z>1.

5. TEOREMAS

5.1. Teorema 1

Si el cociente de dos números enteros

$$\frac{T}{Q}$$

es mixto, es decir, formado por una parte entera N y otra fraccionaria

$$\frac{R}{Q}$$

y los términos de esta última tienen un (m.c.d.) = d (d < Q), entonces

$$\frac{T}{Q}$$

también tendrá como (m.c.d) a d.

En general, el número T > Q será múltiplo de Q si el (m.c.d.) de ambos es Q, en cuyo caso la fracción será entera. Si el (m.c.d.) < Q resultaría semimúltiplo y la fracción simplificada tendría sus términos primos entre sí. [Como ejemplo de este segundo caso, si la fracción fuera 40 / 14, el (m.c.d) sería 2 y la fracción simplificada sería 20 / 7, primos entre sí).

Para demostrarlo, basta llamar R' y Q' a los cocientes de R y Q por d, con lo que podemos escribir

$$\frac{T}{Q} = N \pm \frac{R}{Q} = N \pm \frac{R'd}{Q'd} = \frac{(NQ' \pm R')\,d}{Q'd}$$

y comparando el primer y último término, vemos que tanto T como Q admiten como divisor a d, quedando las fracciones simplificadas

$$\frac{T'}{Q'} = N \pm \frac{R'}{Q'}$$

primas entre sí, ya que los cocientes de dos números divididos por su (m.c.d.) son primos entre sí.

5.2. Teorema 2

Es evidente que si el (m.c.d.) de R y Q es la unidad, entonces T y Q son primos entre sí.

5.3. Teorema 3

Z no puede ser múltiplo de p (M(p)), pues haciendo en

$$X^p + Y^p = Z^p$$

la sustitución de Schier, que consiste en llevar a la anterior el valor de X en (8), se obtendría

$$(Z + kp - Y)^p + Y^p = Z^p$$

cuyo desarrollo nos llevaría a la igualdad

$$(Z + kp)^p - Z^p = p\,(Z + kp)\,XY\,[M(Z + kp) + Y^{p-3}]$$

y si Z = M(p), desarrollando el primer miembro,

$$(Z + kp)^p - Z^p = \binom{p}{1} Z^{p-1}(kp) + \binom{p}{2} Z^{p-2}(kp)^2 + \ldots (kp)^p = M(p^p)$$

y al ser el segundo miembro $M(p^2)$, resultaría una igualdad imposible en números enteros.

5.4. Teorema 4

Conociendo que kp < X puede hallarse una limitación de la expresión

$$\frac{Z^p}{Z + kp}$$

sustituyendo kp por Z ó 0, se obtiene

$$\frac{Z^{p-1}}{2} < \frac{Z^p}{Z + kp} < Z^{p-1}$$

6. NUEVO ENFOQUE DEL PROBLEMA Y SU SOLUCION

Fijados dos números enteros, X, Y, que sean primos entre sí, elevémoslos a la potencia p, primo impar, y sumémoslos. Se tendrá

$$X^p + Y^p = M \tag{9}$$

En esta igualdad, al no tener X e Y factores comunes, la suma de sus potencias, M, será primo con respecto a los dos, resultando los tres primos entre sí, dos a dos.

En efecto, pues si M contuviera un factor igual en X obligaría a que Y lo tuviese también, no siendo entonces primos entre sí. Lo mismo ocurriría si el factor común fuera en Y.

Al ser p primo impar, la (9) admite el desarrollo

$$X^p + Y^p = (X + Y)(X^{p-1} - X^{p-2}Y + X^{p-3}Y^2 - \ldots - X\,Y^{p-2} + Y^{p-1}) = M \tag{10}$$

que demuestra que M no puede ser un número primo ya que, al menos, consta de tres factores al no poder ser X+Y primo (Propiedad IV)

Si existiese un número entero Z que cumpliera la condición

$$Z^p = M \tag{11}$$

al ser $Z = \sqrt[p]{M}$, debería contener todos los distintos factores primos que figuran en M, con sus exponentes divididos por p, quedando primo con X y con Y.

En resúmen, para que Z sea entero, M debe poseer una descomposición factorial de la forma

$$M = r_1^{k1p}\, r_2^{k2p} \ldots r_i^{kip} \qquad (\text{todas las } k \geq 1), \tag{12}$$

y en consecuencia

$$Z = r_1^{k1}\, r_2^{k2} \ldots r_i^{ki} \tag{13}$$

bastando que un solo factor no tenga un exponente p, o múltiplo de p, para que Z no sea entero.

Si sustituímos (11) en (9) y dividimos ambos miembros por X +Y, o por su igual Z+kp, que constituye la igualdad fundamental, podemos escribir sucesivamente,

supuesta igualdad

$$X^p + Y^p = Z^p \tag{14}$$

dividida por un mismo número X+Y = Z+kp

$$\frac{Z^p + Y^p}{X + Y} = \frac{Z^p}{X + Y} = \frac{Z^p}{Z + kp} \tag{15}$$

El primer miembro de (15) es una relación completa que sabemos es siempre un número entero, siendo suficiente que una cualquiera de las dos igualdades restantes no sea entera, o siéndolo, no estuviera comprendida dentro de las limitaciones establecidas, o demostrar que no sea posible que lo sea, para afirmar que la última hipótesis de Fermat es cierta con carácter general.

Por la ley del resto de Ruffini sabemos, en principio, que el primer miembro de (15)

$$\frac{X^p + Y^p}{X + Y} \tag{16}$$

que constituye una relación completa, es un número entero, no siéndolo, sin embargo,

$$\frac{X^p - Y^p}{X + Y} \tag{17}$$

por lo que debemos investigar qué relación existe en la primera (16) entre los dos elementos considerados por separado.

$$\text{En (16), el resto } R = (-Y)^p + Y^p = 0 \tag{18}$$
$$\text{En (17), } R = (-Y)^p - Y^p = -2Y^p \neq 0 \tag{19}$$

Para ello, hagamos la división

$$\frac{X^p}{X + Y}$$

considerando los p primeros términos del cociente

$$\frac{X^p}{X + Y} = X^{p-1} - X^{p-2}Y + X^{p-3}Y^2 - \ldots + Y^{p-1} - \frac{Y^p}{X + Y} = N - \frac{Y^p}{X + Y}$$

lográndose averiguar que las dos relaciones incompletas suman un número entero N, al ser

$$N = \frac{X^p}{X + Y} + \frac{Y^p}{X + Y} \tag{20}$$

De lo anterior (20) se deduce que ambas relaciones incompletas tienen que ser simultáneamente enteras o ambas fraccionarias. (21)

Para el caso de que las dos relaciones incompletas sean enteras,

$$\frac{X^p}{X+Y} = n_e \qquad y \qquad \frac{Y^p}{X+Y} = n'_e$$

se verificará

$$X^p = (X+Y)\, n_e$$
$$Y^p = (X+Y)\, n'_e$$

señalándonos que tanto X^p como Y^p tienen un factor común $(X + Y)$, no siendo entonces primos entre sí, contrario a la hipótesis inicial (9) de que X e Y sean números primos entre sí. Además, su diferencia

$$\frac{X^p - Y^p}{X+Y}$$

resultaría entera, no cumpliéndo la ley del resto (19).

Dado, así pues, que las relaciones incompletas enteras no satisfacen el problema, estudiemos el supuesto de que las relaciones incompletas sean fraccionarias, o sea, que (15),

$$\frac{Z^p + Y^p}{X+Y} = \frac{Z^p}{Z+kp}$$

pero entonces, el primer miembro,

$$\frac{X^p + Y^p}{X+Y}$$

sigue siendo un número entero [(20) y (21)] y el segundo

$$\frac{Zp}{Z+kp}$$

como relación incompleta fraccionaria, no lo es.

En la comparación del grupo (X, Y, Z) en la ecuación inicial $X^p + Y^p = Z^p$, dicho grupo está constituído por tres números primos entre sí dos a dos, pero en (15) aparecen en una relación por cociente

$$\frac{Z^p}{X+Y} = \frac{Z^p}{Z+kp}$$

que da lugar a dos situaciones diferentes, como son: Que X e Y sean impares o que ambos sean de distinta paridad, que debemos estudiar por separado.

Al ser iguales los números X + Y y Z + kp, tendrán idéntica composición factorial, lo que permite considerarlos indistintamente.

Por tanto:

1. Si X e Y son impares, su suma es un número par, debiendo serlo también Z, figurando en numerador y denominador como único factor común una potencia de 2, que al simplificar dividiendo ambos términos por su (m.c.d.) quedarían primos entre sí [5.1. Teorema 1 y (8')].

2. Si X e Y fueran de distinta paridad, X + Y sería impar y lo mismo Z, resultando un cociente no entero, al serlo de factores primos impares y distintos.

En conclusión, y como anticipamos en el apartado 4.1. Metodología, el artificio

$$\frac{X^p + Y^p}{X + Y} = \frac{Z^p}{Z + kp}$$

podría tener dos posibles soluciones enteras, habiendose demostrado en este capítulo 6 que:

a. Si las relaciones incompletas de dicho artificio fueran enteras, el resultado no cumpliría la hipótesis inicial, X e Y son primos entre sí, ni la ley del resto de Ruffini.

b. Si las relaciones incompletas fueran fraccionarias, el resultado sería contradictorio: Una supuesta igualdad con un miembro entero y el otro fraccionario.

Por lo tanto, este artificio, al no tener solución posible,demuestra que la igualdad $X^p + Y^p = Z^p$, dividida por un mismo número, da resultados contradictorios, confirmando así, con carácter general, la última hipótesis de Fermat

$$X^p + Y^p \neq Z^p$$

7. APENDICES

7.1. Congruencia de Fermat

Se verifica que, para p número primo impar,

$$(x_1 + x_2)^p = x_1^p + x_2^p \text{ (mód p)}.$$

Como generalización:

$$(x_1 + x_2 + \ldots + x_a)^p = x_1^p + x_2^p + \ldots + x_a^p \text{ (mód p)}$$

y haciendo $x_1 = x_2 = \ldots = x_a = 1$, obtendremos

$$a^p \equiv a \text{ (mód p)}$$

siendo a un número cualquiera.

En el caso particular en que a sea distinto de múltiplo de p, entonces

$$a^{p-1} \equiv 1 \text{ (mód p)}$$

La propiedad anterior nos permite deducir el siguiente teorema:

Dados dos números X e Y $\neq$ M(p) y siendo p un número primo impar, se verificará

$$X^{p-1} - Y^{p-1} = M(p)$$

En efecto, se tiene sucesivamente

$$X^{p-1} - Y^{p-1} = X^{p-1} - 1 - (Y^{p-1} - 1) = M(p)$$

Por tanto, se verifica la descomposición

$$\begin{aligned} X^{p-1} - Y^{p-1} &= (X + Y)\, M(p) \qquad \text{si } X + Y \neq M(p) \\ &= (X + Y)\, M \qquad \text{si } X + Y = M(p) \end{aligned}$$

7.2. Números Pitagóricos. Caso de $X^4 + Y^4 = Z^4$

De la identidad

$$\left| \frac{a^2 + b^2}{2} \right|^2 = (ab)^2 + \left| \frac{a^2 - b^2}{2} \right|^2 \tag{22}$$

se deducen las siguientes proposiciones:

1. La ecuación indeterminada

$$Z^2 = X^2 + Y^2$$

puede resolverse siempre en números enteros positivos primos entre sí, aplicando la fórmula (22) y haciendo

$$Z = \frac{a^2 + b^2}{2} : X = ab : Y = \frac{a^2 - b^2}{2}$$

siendo a, b números enteros positivos impares, primos entre sí y a > b.

2. Se puede demostrar elementalmente que la ecuación

$$X^4 + Y^4 = Z^4 \tag{23}$$

no tiene solución X, Y, Z en números enteros distintos de cero.

Admitamos, en primer lugar, que la ecuación

$$X^4 + Y^4 = Z^2 \tag{24}$$

sea resoluble en números enteros primos dos a dos y que (X_0, Y_0, Z_0) sea una solución, no existiendo otra con valor Z menor que Z_0, obtenemos de (22)

$$Z_0^2 = \frac{a^2 + b^2}{2} \quad : X_0^2 = ab : Y_0^2 = \frac{a^2 - b^2}{2}$$

de donde se deduce que podemos hacer

$$a = \alpha^2 \quad , \quad b = \beta^2$$

siendo α y β números impares primos entre sí. Hacemos

$$\alpha + \beta = 2\gamma \quad , \quad \alpha - \beta = 2\delta$$

$$\left| \frac{Y_0}{2} \right|^2 = \gamma\,\delta\,(\gamma^2 + \delta^2)$$

y como γ, δ, $\gamma^2 + \delta^2$ son cuadrados, poniendo ahora

$$\gamma = X_1^2 \quad , \quad \delta = Y_1^2 \quad , \quad \gamma^2 + \delta^2 = Z_1^2$$

obtenemos

$$Z_1^2 = X_1^4 + Y_1^4$$

y como

$$Z_1^2 = \frac{\alpha^2 + \beta^2}{2} = \frac{a + b}{2} = \frac{Y_0^2}{a - b} < Z_0^2$$

resulta que $Z_1 < Z_0$, contrariamente a lo supuesto. Por lo tanto, (24) no tiene solución, por ser contraria a la hipótesis.

Válida esta negativa para cualquier valor de Z, lo será para todos los Z que sean cuadrados, resultando, como corolario, la imposibilidad de (23).

8. BIBLIOGRAFIA

DICKSON, L. E.: *History of the theory of numbers.* Vol. 2. Diophantine Analysis. 1966.

CIPOLLA, MICHELE: *Enciclopedia delle matematiche elementari.* Vol. 1. Parte 1. Teoria delle Númeri, Analisis Indeterminata. 1930.

CARMICHEL, R. D.: *The theory of numbers and diophantine analysius.* 1915.

GOT, THEÓPHILE: *Las grandes corrientes del pensamiento matemático. Un enigma matemático: el último teorema de Fermat.* 1948 (trad.).

NIVEN y ZUCKERMAN: *Introducción a la teoría de los números.* 1969 (trad.).

SCHIER, OTTO; SITZUNGSBER: *Uber die auflösung der unbestimmten gleichung* $X^n + Y^n = Z^n$ *in rationalen zahlen.* Akad. Wiss. Wien (Math.), 81, II, 1880, 392-8.

TEMPLE BELL, ERIC: *La reina de las matemáticas.* Sigma, tomo 4, pág. 101.

WESTREN-TURMBULL, HERBERT: *Los grandes matemáticos.* Sigma, tomo IV, pág. 84.

CASTELLET, MANUEL: *Fermat, el reto no resuelto por las matemáticas.* La Vanguardia, 20-XII-1987.