NOTAS MATEMATICAS

UN TEOREMA DE FERMAT, SIN CONSECUENCIAS

VICTOR E. CARO
Ex-Rector de la Facultad de Matemáticas e Ingeniería de la Universidad Nacional y Profesor de la misma.

Fermat se consagró durante muchos años al cultivo de las matemáticas, en los ratos que le dejaban libres sus deberes de celoso magistrado y corresponsal cumplidísimo, y sus aficiones de poeta y erudito. Tuvo, según parece, el propósito de recoger en un libro el fruto de sus originales investigaciones y sus comentarios a Diofante, mas no lo llevó a cabo y murió sin haber publicado una línea. Su hijo se encargó de dar a luz sus papeles y apuntes, y muchos años después, quienes recogieron la bandera de las ciencias exactas, se dieron a descifrar sus enigmas y a demostrar las peregrinas proposiciones con que enriqueció la teoría de los números, campo favorito de sus andanzas intelectuales.

Todos sus teoremas resultaron verdaderos, con excepción de uno relativo a los números primos, del cual, por otra parte, él mismo no se hallaba muy seguro, pues al comunicárselo a Pascal, le dice: "La demonstration en est trés malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement". Permanece también aún sin demostración plena, pero no desmentido, hasta ahora, el que en la historia de las matemáticas se denomina: *el último teorema de Fermat.*

Respecto de las sendas que transitaba su espíritu y de los secretos que poseía este gran artista de los números, es poco lo que se sabe; pero si hemos de atenernos a su propio testimonio, y a los resultados obtenidos, debemos reconocer que eran "sutilísimos" y "maravillosos". Cómo procedía, por ejemplo, para decidir, tras breve inspección, si un número dado era o no primo? Euler y Gauss le daban a esta cuestión gran importancia, pero ninguno de los dos pudo hallar el secreto buscado.

Queda un documento de Fermat en que explica el método que él llama del "descenso". Es una carta, sin fecha, cuyo original reposa en la biblioteca universitaria de Leyde. Veamos en ella cómo aplica su método a la demostración del siguiente teorema que da motivo a esta nota: *Todo número primo de la forma* $4h+1$ *puede descomponerse en la suma de dos cuadrados.*

Dice Fermat: "Si existe un número primo, tomado a discreción, que exceda en la unidad a un múltiplo de 4, y que no esté formado por dos cuadrados, habrá otro número primo de la misma naturaleza menor que el propuesto, y luégo un tercero aún menor, etc. Así, descendiendo, se llega al número 5, que es el más bajo entre los de ese género, el cual se seguiría no estar compuesto de dos cuadrados, lo que no es cierto, por donde debe inferirse, por reducción al imposible, que todos los de esta clase están formados por dos cuadrados. Hay infinidad de cuestiones de esta naturaleza".

Fermat amplió después el teorema anterior así: *Todos los números primos de la forma* $4h+1$, *lo mismo que todas sus potencias, pueden descomponerse en la suma de dos cuadrados.*

Vamos por partes. Tomemos la segunda potencia, con lo cual entramos en el dominio de los números *pitagóricos*. Bien sabido es que llevan este nombre los números enteros y positivos que, por ternas, satisfacen a la ecuación:

$$a^2 + b^2 = c^2 \qquad (A)$$

tales como:

$$3^2 + 4^2 = 5^2$$

ó

$$8^2 + 15^2 = 17^2$$

los cuales corresponden a lados conmensurables de un triángulo rectángulo.

Antes de investigar las condiciones que deben cumplir a, b y c para que verifiquen la ecuación (A), debe observarse: 1º Si a y b tienen un factor común p éste lo será también de c y la ecuación puede simplificarse hasta que a b y c sean primos relativos, dos a dos. 2º Es fácil mostrar que a y b no pueden ser ambos impares, pues si lo fueran, su suma no correspondería a un cuadrado. Así, pues, uno de los catetos a o b debe ser par, y el otro y la hipotenusa, impares.

Ahora le cedo la palabra al sabio expositor y matemático alemán, de la Universidad de Gotinga, Félix Klein, muerto no há mucho, quien se expresa así:

"Vamos a tratar ahora de los *números pitagóricos*, utilizando la intuición espacial en una for-

ma algo diferente (1). En lugar de la ecuación

$$a^2 + b^2 = c^2 \qquad (1)$$

cuyas soluciones enteras se trata de hallar, consideremos la ecuación

$$x^2 + y^2 = 1 \qquad (2)$$

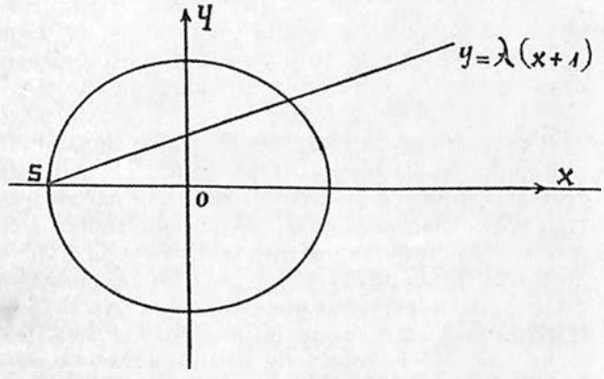
que se deduce de (1) poniendo

$$\frac{a}{c} = x \qquad \frac{b}{c} = y \qquad (3)$$

con lo cual el problema queda reducido a determinar todos los pares de números racionales (x, y) que satisfacen a la (2).

"Partimos de la representación geométrica de todos los puntos racionales (x, y), es decir, de todos los puntos de coordenadas racionales x é y que llenan el plano xy densamente en todas sus partes. La ecuación $x^2 + y^2 = 1$ representa, en ese plano, el *círculo unidad*, cuyo centro es el origen, de modo que nuestro problema se reduce al de ver cómo va pasando esta circunferencia entre los puntos racionales, cuyo conjunto es denso en todas partes, y, en particular, cuáles de estos puntos contiene. Algunos de estos puntos son conocidos, desde luego los de intersección con los ejes; entre éstos vamos a fijarnos especialmente en el

$$S \quad (x = -1,\ y = 0)$$



"Imaginemos todos los rayos que parten de S los cuales están representados por la ecuación

$$y = \lambda (x + 1) \qquad (4)$$

y llamémoslos *racionales* o *irracionales*, según que el valor del parámetros correspondiente λ sea o no racional; se verifica entonces el siguiente doble teorema: *Todo punto racional de la circunferencia se proyecta desde S según un rayo racional; y recíprocamente, todo rayo racional que parte desde S corta a la circunferencia en un punto racional.*

"El teorema directo es inmediato. El recíproco se demuestra por cálculo directo, sustituyendo en la ecuación (2) el valor de y dado por la (4); se obtiene así la abscisa del punto de intersección resolviendo la ecuación:

$$x^2 + \lambda^2 (x^2 + 1)^2 = 1$$

o sea

$$(1+\lambda^2) x^2 + 2\lambda^2 x + \lambda^2 - 1 = 0$$

"Una solución $x = -1$ de esta ecuación es la ya conocida, correspondiente a la intersección S; el valor de la otra se deduce por un pequeño cálculo,

$$x = \frac{1-\lambda^2}{1+\lambda^2} \qquad (5\,a)$$

y sustituyéndolo en (4) se obtiene la ordenada correspondiente

$$y = \frac{2\lambda}{1+\lambda^2} \qquad (5\,b)$$

y estas expresiones demuestran que, en efecto, el segundo punto de intersección es racional si corresponde a un valor racional de λ.

"Los dos teoremas, directo y recíproco, que acabamos de demostrar, pueden enunciarse también así: *Todos los puntos racionales de la circunferencia están representados por las fórmulas (5) en las que λ puede tomar cualquier valor racional.*

"Con esto queda resuelto el problema y sólo falta pasar a los números enteros.

"Para ello ponemos:

$$\lambda = \frac{n}{m}$$

donde m y n designan números enteros, y sustituyendo en las fórmulas (5) se obtiene:

$$x = \frac{m^2 - n^2}{m^2 + n^2} \qquad y = \frac{2mn}{m^2 + n^2}$$

como conjunto de todas las soluciones racionales de la ecuación (2). Por consiguiente, todas las soluciones enteras de la primera ecuación (1), es decir, todos los números pitagóricos, están dados por las siguientes fórmulas:

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

obteniéndose todas las soluciones compuestas de números primos entre sí, cuando se atribuyen a m y n todos los pares de números primos entre sí. Tenemos, pues, con esto, una deducción muy intuitiva de este resultado, que de otro modo hubiera parecido muy abstracta".

Hé aquí algunos resultados:

Para	$m=2$	y $n=1$	$3^2+4^2=5^2$
»	$m=3$	y $n=2$	$5^2+12^2=13^2$
»	$m=4$	y $n=3$	$7^2+24^2=25^2$
»	$m=5$	y $n=2$	$21^2+20^2=29^2$

Los números pitagóricos pueden dividirse en tres clases: 1º aquellos en que a y b difieren en una unidad, como en el 1º y 4º ejemplo de los anteriores; 2º aquellos en que $c - b = 1$: 1º 2º y 3er. ejemplos; y 3º los restantes.

Cada clase tiene sus propiedades interesantes y curiosas. No las menciono siquiera por no alargar esta nota.

En lo que sigue tendré que valerme de mis propios recursos, pues no conozco lo que se ha

(1) *Matemática elemental desde un punto de vista superior*, Madrid, 1927, págs. 54-56.

escrito sobre el particular. Voy a indicar el camino que he seguido para llegar a los resultados anteriores y de ahí partir adelante, mediante el empleo de cantidades complejas, eficaces auxiliares de investigación, especialmente en este campo de la teoría de los números, cosa que suena un poco a paradoja.

Se trata de hallar dos cuadrados cuya suma sea un cuadrado; y esto es lo que se obtiene precisamente cuando se multiplican dos complejas conjugadas y el producto se eleva al cuadrado.

Sean:

$$\alpha = m + n\,i \qquad (6)$$
$$\alpha' = m - n\,i$$

dos imaginarias, cuyos elementos m y n son enteros. El producto $\alpha\alpha'$ teniendo en cuenta que $i^2 = -1$ nos da:

$$\alpha\alpha' = m^2 + n^2 \qquad (7)$$

y el cuadrado

$$(\alpha\alpha')^2 = (m^2 + n^2)^2 \qquad (8)$$

Por otro lado tenemos:

$$\alpha^2 = (m^2 - n^2) + 2\,m\,n\,i$$
$$\alpha'^2 = (m^2 - n^2) - 2\,m\,n\,i$$

Estas dos cantidades son conjugadas y su producto es la suma de dos cuadrados reales y positivos:

$$\alpha^2\alpha'^2 = (\alpha\alpha')^2 = (m^2 - n^2)^2 + (2\,m\,n)^2 \qquad (9)$$

Igualando los segundos miembros de (8) y (9), se obtiene i el resultado buscado:

$$(m^2+n^2)^2 = (m^2-n^2)^2 + (2mn)^2$$

y llamando c, a y b cada paréntesis:

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

De aquí partimos. Elevando (7) al cubo se encuentra:

$$(\alpha\alpha')^3 = (m^2 + n^2)^3 \qquad (10)$$

Pero, por otra parte, tenemos:

$$\alpha^3 = m^3 - 3\,m\,n^2 + i(3\,m^2\,n - n^3)$$
$$\alpha'^3 = m^3 - 3\,m\,n^2 - i(3m^2\,n - n^3)$$

De donde, observando que estas cantidades son conjugadas:

$$\alpha^3\,\alpha'^3 = (\alpha\alpha')^3 = (m^3 - 3\,m\,n^2)^2 + (3m^2\,n - n^3)^2 \qquad (11)$$

Igualando (10) y (11) resulta:

$$(m^2 + n^2)^3 = (m^3 - 3\,m\,n^2)^2 + (3\,m^2\,n - n^3)^2$$

fórmula que nos da las ternas de números enteros que satisfacen a la ecuación:

$$c^3 = a^2 + b^2$$

Siguiendo el mismo derrotero, hallamos:

$$(m^2 + n^2)^4 = (m^4 - 6\,m^2\,n^2 + n^4)^2 + (4\,m^3 n - 4\,m\,n^3)^2$$

Aquí se descubre ya la ley de formación, basada en el binomio de Newton, que es la roca granítica sobre la cual se apoya el edificio de las matemáticas modernas.

Para obtener la fórmula general:

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

siendo p un entero cualquiera, debemos hacer:

$c = m^2 + n^2$

$a =$ términos impares del desarrollo de $(m+n)^p$ con signos alternados.

$b =$ términos pares del desarrollo de $(m+n)^p$ con signos alternados.

Hé aquí dos cuadros ilustrativos:

$13 = 3^2 + 2^2$	$5 = 2^2 + 1^2$
$13^2 = 12^2 + 5^2$	$5^2 = 3^2 + 4^2$
$13^3 = 9^2 + 46^2$	$5^3 = 2^2 + 11^2$
$13^4 = 120^2 + 119^2$	$5^4 = 7^2 + 24^2$
$13^5 = 117^2 + 598^2$	$5^5 = 41^2 + 38^2$

De lo expuesto y de la inspección de estos ejemplos se deduce un procedimiento práctico, cuya deducción, siguiendo un precepto de Descartes, dejo al lector.

A estos mismos resultados debió de llegar Fermat por medios harto diferentes de los que he señalado, pues en su tiempo las imaginarias apenas empezaban a asomar en el horizonte. Por esos medios muy suyos que se llevó a la tumba, descubrió otras leyes y formuló otros teoremas tan originales e interesantes como escasos de utilidad inmediata, porque la ciencia o el arte que se ha llamado la teoría de los números —según frase célebre de un matemático alemán— es una especulación que tiene por único objeto el honor del espíritu humano.

El Mochuelo, enero 1937.