Revista INTEGRACION
Departamento de Matemáticas UIS
Vol. 10, No. 1, enero-junio 1992

Una Conjetura Elemental Equivalente al Ultimo Teorema de Fermat

ALVARO GARDEAZABAL QUINTERO *
CARLOS VASCO URIBE **

1. Introducción

Todo matemático que haya experimentado la atracción de la teoría de los números naturales y enteros, cuando tiene un momento de sinceridad confiesa que ha gastado largas horas tratando de probar la conjetura que llamamos "Ultimo Teorema de Fermat" (en adelante "UTF"). Por supuesto que al llamar "teorema" a dicha conjetura estamos asumiendo por respeto al genio de Fermat la improbable existencia de esa "demostración maravillosamente exacta" que no cabía en la margen de su ejemplar de la Aritmética de Diofanto.

Infortunadamente, la probabilidad de que una pretendida demostración de esa conjetura resista el análisis es tan baja, que ya ninguna revista especializada recibe manuscritos que intenten demostrar el UTF (el presente trabajo no pretende hacerlo). Las publicaciones sobre el estado actual de la investigación en esta área se limitan a los resultados obtenidos para ciertos exponentes, y a las conjeturas relacionadas con el UTF. Pero no dan ninguna indicación de las horas, y tal vez años, de trabajo que precedieron a esos resultados, de los callejones sin salida, ni de las ideas que inspiraron la invención de métodos, técnicas, lemas y teoremas.

Uno de los coautores de esta nota (AGQ) ha trabajado durante muchos años en la demostración del UTF. La Revista Javeriana publicó en dos ocasiones algunos ejercicios demostrativos suyos relacionados con el tema, revisados por el P. Wladimiro Escobar, S.J. (No. 479, octubre de 1981, pp. 357-370, y No. 494, mayo de 1983, pp. 341-354). Esta tercera publicación intenta presentar a los lectores de la Revista INTEGRACION una conjetura elemental que relaciona el UTF con cierta propiedad específica de divisibilidad entre algunos parámetros de la ecuación de Fermat, mostrando a la vez las ideas que inspiraron esta conjetura y las líneas informales de razonamiento que llevaron a la demostración formal del resultado.

* Abogado Javeriano; profesor de matemáticas elementales y financieras; exasistente de Dirección del Instituto Geofísico de los Andes Colombianos.

** Profesor Titular de la Universidad Nacional de Colombia, Departamento de Matemáticas y Estadística.

Los autores esperamos que así el lector no sólo se anime a intentar demostrar esta nueva conjetura aparentemente más simple, sino que explore otras relaciones que pueden producir nuevas conjeturas. Ojalá el lector llegue algún día a esa meta altamente improbable: a una demostración del UTF, a ser posible una demostración elemental, en el sentido de que se haga con las herramientas matemáticas de las que disponía Fermat hacia 1640.

2. La ecuación general de Fermat

Es claro que en la ecuación general de Fermat,

$$a^n + b^n = c^n$$

figuran explícitamente cuatro parámetros, a,b,c,n, los cuales pueden restringirse a los números enteros positivos. En el tratamiento propuesto en este artículo es conveniente introducir un quinto parámetro d, dependiente de a,b,c, que llamaremos "la diferencia" entre la suma a+b y el número c. Definimos pues la diferencia d así:

$$a + b = c_d$$

Para el caso n=1, la ecuación de Fermat se reduce a

$$a + b = c.$$

Para este caso n=1, d=0.

Esta ecuación particular para el caso n=1 tiene un número infinito de soluciones que yacen en el primer octante, y sobre el plano

$$a + b - c = 0 .$$

Para el caso n=2, la ecuación de Fermat es

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

por lo cuante tenemos d > 0.

En este caso la ecuación de Fermat tiene un número infinito de soluciones enteras positivas, las llamadas "triplas pitagóricas" (a, b, c), que han sido abundantemente estudiadas. Todas ellas yacen por supuesto en el primer octante, y sobre la cónica

$$a^2 + b^2 - c^2 = 0$$

Llamemos a estas soluciones "triplas 2-pitagóricas" para resaltar el parámetro n=2, y así poder generalizar a las tripas n-pitagóricas, que serían las soluciones enteras positivas a la ecuación de Fermat

$$a^n + b^n = c^n$$

Cada múltiplo de una tripla n-pitagórica satisface también la ecuación respectiva, y por lo tanto el estudio puede reducirse a las triplas primitivas o simplificadas, en las cuales (a,b,c)=1.

No es muy conocido el resultado, pero la observación de los tres términos de la ecuación de Fermat sugiere la prueba de que los tres elementos de una tripla primitiva son también primos entre sí dos a dos: (a,b) = 1, (a, c) = 1, (b, c) = 1.

En adelante estudiaremos únicamente posibles triplas n-pitagóricas primitivas (a, b, c), que por lo tanto cumplen las cinco condiciones:

$$a^n + b^n = c^n;\ (a,b,c) = 1;\ (a,b) = 1;\ (a,c) = 1;\ (b,c) = 1$$

Para muchos enteros n > 2 se ha logrado demostrar que no puede existir ninguna tripla n-pitagórica, y en los casos restantes no ha sido posible hasta ahora hallar ninguna. El UTF afirma precisamente que en general para n > 2 no existen triplas n-pitagóricas. Se puede también mostrar, para probar el UTF, que es suficiente verificar que no puede existir una tripla p-pitagórica con un primo impar p.

3. La heurística

Si disponemos las ecuaciones de Fermat ordenándolas verticalmente en grado descendente hasta n=2, y horizontalmente según la magnitud a+b+c de las triplas n-pitagóricas primitivas, obtenemos un cuadro así:

$n = 2m + 1$	$a^n + b^n = c^n$		
$n = 2m$	$a^n + b^n = c^n$		
$n = 4$	$a^4 + b^4 = c^4$	?	
$n = 3$	$a^3 + b^3 = c^3$	?	
$n = 2$	$a^2 + b^2 = c^2$	$3^2 + 4^2 = 5^2$	$5^2 + 12^2 = 13^2$...

CUADRO 1.- Tabla de ecuaciones de Fermat

La pista heurística que se siguió en el presente estudio fue la siguiente:

> Cualquier propiedad de divisibilidad que se dé en el nivel n=2 entre los parámetros a, b, c, d, se dará también en los niveles superiores n > 2.

Veamos por qué se eligió esta pista. En primer lugar, porque parece un principio muy plausible, ya que los factores primos de la base, de los cuales dependen las condiciones de divisibilidad, no cambian en absoluto al elevar esa base al cuadrado, al cubo o a cualquier potencia entera. Y en segundo lugar, porque al explorar algunas propiedades de divisibilidad se encontraron interesantes generalizaciones del caso n=2 al caso n=p, con p un primo impar.

4. Las conjeturas

Llamemos "Primera Conjetura para n=2", que abreviamos "PC(2)", a la siguiente proposición:

PC(2): Si $a^2 + b^2 = c^2$, entonces d es par.

Esta conjetura resultó ser correcta:

Si (a,b,c) es una solución de la ecuación de Fermat,

$$d^2 = a^2 + b^2 + c^2 + 2ab - 2ac - 2bc = 2c^2 + 2ab - 2ac - 2bc;$$

d^2 es pues divisible por 2, y por lo tanto d también lo es. La primera conjetura resulta pues ser un teorema, que puede también probarse directamente examinando todos los casos posibles de paridad de a, b, c, y deduciendo de todos ellos que d tiene que ser par.

Generalicemos ahora la primera conjetura al caso de cualquier primo impar p, y llamémosla "PC(p)":

PC(p): Si $a^n + b^n = c^n$, y n = p, p un primo impar, entonces d es par.

Esta conjetura resulta también ser un teorema, que puede probarse por el binomio de Newton, o por consideraciones de paridad. Dejamos esa prueba como el proverbial ejercicio par el lector.

Reformulemos PC(2) como un segunda conjetura para n=2, SC(2), de manera que aparezca expresamente el parámetro n, y así permita otra genealización:

SC(2): Si $a^n + b^n = c^n$, y n = 2, entonces 2|d.

Obviamente esta es la misma PC(2), y por lo tanto un teorema. La generalización a un primo impar p es:

SC(p): Si $a^n + b^n = c^n$, y n = p, p un primo impar, entonces p|d.

Esta segunda conjetura también resulta ser un teorema, que puede probarse por el binomio de Newton o por aritmética módulo p.

Si esta propiedad de divisibilidad del parámetro d se propaga del 2 a cualquier primo impar p, podemos explorar otras propiedades de divisibilidad del caso conocido n=2, y generalizar luego a los primos impares. La tercera conjetura para el caso n=2, TC(2), es la siguiente:

TC(2): Si $a^n + b^n = c^n$, y n = 2, entonces (c,d) = 1.

He aquí una demostración de que la tercera conjetura también es un teorema par el caso n = 2:

Sabemos que $a^2 + b^2 = c^2$, y d = a + b - c. Luego a + b = c + d.

Estudiemos los cuadrados de ambos miembros, restándoles ordenadamente los miembros de la ecuación de Fermat para n = 2:

$$(a + b)^2 - (a^2 + b^2) = (c + d)^2 - c^2,$$

$$2ab = 2cd + d^2 .$$

Pero d es par, o sea que podemos escribir $d = 2d_1$, para d_1 entero positivo.

Por lo tanto, $2ab = 2cd + 2dd_1$. Dividiendo esta última igualdad por 2d obtenemos

$$(ab/d) = c + d_1 .$$

Luego d|ab, pues el resultado $c + d_1$ es un entero positivo. Por lo tanto, d, que no puede ser igual a 1, pues es par, tiene la totalidad de sus factores en común con a, o con b, o parte de ellos con a y el resto con b. Luego (c,d) = 1, pues de lo contrario, d tendría un factor común con a y c, o con b y c, lo cual es imposible para una tripla primitiva.

Formulemos ahora la tercera conjetura ya generalizada al caso p:

TC(p:) Si $a^n + b^n = c^n$, y n = p, p un primo impar, entonces (c,d)=1.

Como era de esperarse, no hemos podido demostrar que la tercera conjetura es un teorema para el caso n = p, p un primo impar, pero sí podemos demostrar que, a pesar de su extrema simplicidad, esta

ltima conjetura es equivalente al último teorema de Fermat:

Teorema: TC(p) es equivalente a UTF.

(a) Probemos que UTF implica TC(p).

La prueba se basa en la semántica usual de la conectiva "si..., entonces". Supongamos que UTF es verdadero. No hay pues ninguna tripla p-pitagórica para $p > 2$, y por lo tanto el antecedente de TC(p) siempre es falso. Luego la implicación TC(p) siempre es verdadera, y UTF implica TC(p).

(b) Probemos ahora que TC(p) implica UTF.

Es interesante observar que la prueba recuerda la estrategia favorita de Fermat, el "método de descenso infinito".

Supongamos que se cumple la ecuación de Fermat para cierta tripla n-pitagórica (a, b, c) con $n = p$, un primo impar: $a^n + b^n = c^n$.

Como n es impar, el cociente notable usual nos permite decir que el resultado de la división de $a^n + b^n$ por $a + b$ es un entero positivo; llamémoslo F_o:

$$(a + b)F_o = c^n \ ;$$

Pero como $a + b = c + d$,

$$F_o c + F_o d = c^n \ .$$

Dividamos toda la igualdad por c:

$$F_o + (F_o d/c) = c^{n-1} \qquad (1)$$

El segundo término $F_o d/c$ tiene que ser entero; por la hipótesis TC(p) sabemos que $(c,d) = 1$, luego $c \mid F_o$.

Llamemos F_1 al cociente entero positivo F_o/c:

$$F_o = F_1 c$$

Sustituyendo en (1) obtenemos:

$$F_1 c + F_1 d = c^{n-1}$$

Por consideraciones similares, obtendremos sucesivamente:

$$F_2 c + F_2 d = c^{n-2}$$

$$F_3 c + F_3 d = c^{n-3}, \text{ etc.}$$

Finalmente, obtendremos:

$F_n c + F_n d = c^{n-n}$, o sea $F_n c + F_n d = 1$, lo cual es absurdo.

Luego si se asume TC(p), la ecuación de Fermat no puede cumplirse para ningún primo impar p, y esto implica UTF■

BIBLIOGRAFIA

El lector interesado seriamente en la teoría de números en general y en el "último teorema de Fermat" en particular, hallará abundante material al respecto en las siguientes obras:

BORÉVICH Z.I., SHAFARÉVICH I.R. Number Theory. Academic Press, New York, 1965.

DICKSON Leonard Eugene. History of the Theory of Numbers (3 volúmenes, 1919). Reimpreso por Chelsea Publishing Co., New York, 1966.

EDWARDS G. Fermat's Last Theorem: a genetic introduction to algebraic number theory. New York, 1965.

LE VEQUE W.J. Reviews in Number Theory (6 volúmenes). AMS, Providence, RI, 1974.

RIBENBOIM P. 13 Lectures on Fermat's last theorem. New York, 1979.

SIERPINSKI Waclaw. Elementary Theory of Numbers. Panstwowe Wydawnictwo Naukowe, Warszawa, 1964.

VINOGRADOV IVAN M. Fundamentos de la teoría de los números. Mir, Moscú, 1977.