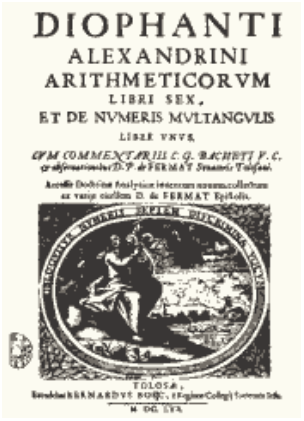
Acerca del Último Teorema de Fermat

Juana Contreras S.[1]
Claudio del Pino O.[2]

Instituto de Matemática y Física
Universidad de Talca



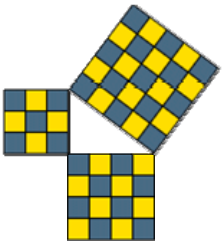
Los primeros antecedentes del llamado Ultimo Teorema de Fermat (UTF), como suele suceder, se remontan a la época de los griegos. Aproximadamente en el año 300 dC, Diofanto escribe su obra *Aritmética*, un tratado de 13 libros. En él hace uso del 0, de los números negativos, de fracciones e incorpora el uso de incógnitas. En el problema 8 del Libro II, plantea:

Encontrar números racionales x, y, z tales que

$$x^2 + y^2 = z^2 \qquad \textbf{(1)}$$

Es claro que:

- si existen números racionales que cumplan (1), también existen números enteros que la cumplen.
- una solución de números positivos de (1), se puede interpretar geométricamente como los lados de un triángulo rectángulo (*x* e *y* los catetos, y *z* la hipotenusa).



Un trío de enteros positivos que cumple (1) reciben el nombre de *ternas pitagóricas*[3]. Por ejemplo: 3, 4 y 5 es una terna pitagórica.

[1] e-mail: jcontres@utalca.cl
[2] e-mail: cdelpino@utalca.cl

[3] Las ternas pitagóricas eran conocidas por los babilonios casi 2000 años a.C., también las conocían los antiguos chinos, que las usaban para resolver problemas que involucraban triángulos rectángulos, e incluso hay monumentos megalíticos de Europa Occidental (en Irlanda, por ejemplo), construidos entre 4800 y 3000 a.C., que guardan esta relación. También en el antiguo Egipto, los "tiradores de cuerdas", que eran los encargados de subdividir las tierras luego de la crecida anual del río Nilo, utilizaban un procedimiento muy relacionado con este teorema. Según el historiador griego Herodoto, éste es el origen de la Geometría. Los tiradores tenían una cuerda con 12 partes iguales, separadas por nudos, que usaban para trazar ángulos rectos; usando la terna 3, 4, 5.

Teorema 1:
El conjunto de ternas pitagóricas es el conjunto de ternas de la forma

$$\left(n^2 - m^2, 2mn, n^2 + m^2\right)$$

donde n y m no tienen divisores comunes, $n > m$, con n y m de distinta paridad.

Demostración: Para empezar hagamos algunas observaciones:

Si *(a, b, c) es una terna pitagórica, (ka, kb, kc) también lo es.* Por lo tanto, las soluciones de (1) se pueden clasificar entre ternas que se obtienen como un múltiplo de una menor y las *ternas primitivas*, que no son un múltiplo de una terna menor.

Sobre la paridad. Si *(a, b, c)* es solución primitiva de (1), es decir si $a^2 + b^2 = c^2$, entonces:

- *a y b no pueden ser ambos pares*. En efecto, si $a=2s$ y $b=2t$, se tendría que $c^2=4(s^2+t^2)$. En tal caso c también sería par.
- *a y b no pueden ser ambos impares*. En efecto, si $a=2x+1$ y $b=2y+1$, se tendría que:

$$\begin{aligned} c^2 = a^2 + b^2 &= (2x+1)^2 + (2y+1)^2 \\ c^2 &= 4x^2 + 4x + 4y^2 + 4y + 2 \\ c^2 &= 4(x^2 + x + y^2 + y) + 2 \end{aligned} \qquad \textbf{(2)}$$

de donde 2 divide a c^2, de aquí se tendría que 2 divide a c. Entonces, 4 dividiría a c^2. Situación que contradice la relación (2).

Por lo tanto, a y b tienen distinta paridad. Supongamos: a par, b impar (de donde c es impar)

Como a es par, sea $a = 2k$.

Como $a^2 = c^2 - b^2 = (c+b)(c-b)$, se tiene que $(2k)^2 = (c+b)(c-b)$, de donde

$$k^2 = \frac{c+b}{2} \cdot \frac{c-b}{2}$$

Como $\frac{c+b}{2}$ y $\frac{c-b}{2}$ no tienen factores comunes, cada uno de ellos es un cuadrado perfecto.

Por lo tanto: $\frac{c+b}{2} = n^2$ y $\frac{c-b}{2} = m^2$. Despejando c y b, se obtiene:

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

y como $a^2 = 4k^2 = 4\, m^2\, n^2$, se obtiene que $a = 2\, m\, n$. ■

Luego del teorema anterior se tiene que, existen infinitas ternas pitagóricas primitivas y además se dispone de una fórmula que permite encontrar algunas de ellas. En el siguiente recuadro se listan algunas ternas pitagóricas:

m	n	$n^2 - m^2$	$2mn$	$n^2 + m^2$
1	2	3	4	5
1	4	15	8	17
1	6	35	12	37
2	3	5	12	13
2	5	21	20	29
3	4	7	24	25

Aproximadamente, en el año 1620 la obra *Aritmética* de Diofanto es traducida al latín. Pierre de Fermat[4], un abogado Francés que se dedicó por hobby a las matemáticas, en sus ratos de *ocio* lee esta obra y va anotando, en el mismo libro, algunas observaciones. En el problema 8, del Libro 2, Fermat se pregunta, si existirán enteros positivos x, y, z tales que $x^3 + y^3 = z^3$, $x^4 + y^4 = z^4$, etc. La respuesta que el propone es:

"*No es posible dividir un cubo en dos cubos, un bicuadrado en dos bicuadrados y, de manera general, una potencia cualquiera de exponente superior en dos potencias de la misma especie*"

Usando la notación actual:

"La ecuación[5] $x^n + y^n = z^n$ no tiene soluciones enteras positivas para $n>2$"

Además anota en un margen del libro: *"He descubierto una demostración verdaderamente hermosa de este resultado, pero este margen es demasiado estrecho para contenerla"*[6]

Este resultado fue conocido más tarde como el *Ultimo Teorema de Fermat* (UTF) y se transformó en uno de los problemas más abordados por la comunidad de los matemáticos tanto profesionales como aficionados, y al mismo tiempo en uno de los problemas más difíciles de resolver.

En lo que sigue se hacen algunas consideraciones generales y particulares sobre el UTF.

Observación: Para demostrar el UTF, bastaría demostrarlo para cada uno de los siguientes casos:

[4] A pesar de no dedicar todo su tiempo al estudio de la matemática, fue un matemático destacado, haciendo aportes cruciales al avance de esta ciencia. Entre otros aportes, descubrió la geometría analítica (2 y 3 dimensiones), antes de Descartes (solo para 2 dimensiones), el cálculo antes de Newton y Leibniz e inventó el cálculo de probabilidades (junto a Pascal).

[5] En lo sucesivo nos referiremos a esta ecuación, como la *ecuación de Fermat.*

[6] Existe consenso en la comunidad matemática, que la demostración que pensó tener Fermat, era incorrecta.

a) Para $n = 4$
b) Para n un número primo impar.

En efecto: Si el exponente n en la ecuación de Fermat no es divisible por ningún primo impar, n debe ser una potencia de 2. Como n es mayor que 2, n debe ser un múltiplo de 4. Por lo tanto, $n=4m$, y la ecuación de Fermat se podría escribir como:

$$(x^m)^4 + (y^m)^4 = (z^m)^4$$

Luego, una solución de la ecuación de Fermat para un n del tipo comentado, nos llevaría a una solución para $n=4$.

Si el exponente n es divisible por un primo impar p, se tendría que $n=pm$, y como

$$(x^m)^p + (y^m)^p = (z^m)^p$$

una solución de la ecuación de Fermat para un n de este tipo, nos llevaría a una solución para un exponente primo impar.

La observación precedente, muestra que $n=4$ es un exponente especial, para abordar el UTF.

Existe consenso en que lo único que logró Fermat, con respecto a su llamado UTF, es su comprobación para $n=4$. Para ello, tomó (¿o creó?) un método nuevo de demostración llamado *método de descenso infinito*.

El principio de inducción matemática, se puede presentar de la siguiente manera:

> "*Si una proposición P(n) es válida para algún entero positivo, entonces existe un entero positivo que es el menor que satisface P(n)*".

Ahora bien, si es posible probar que partiendo del supuesto que una proposición $P(n)$ es válida para un entero positivo r, se puede deducir que ella también es válida para un entero positivo s, con $s<r$; se tendría claramente una contradicción con el principio de inducción matemática recién señalado. Esta contradicción prueba que la proposición $P(n)$ no se cumple para ningún entero positivo. Esta forma de abordar un problema es conocido como *método de descenso infinito*.

Para ilustrar este método, lo usaremos para dar una demostración poco conocida del clásico resultado:

Teorema 2: $\sqrt{2}$ es un número irracional.

Demostración (indirecta): Supongamos lo contrario, es decir, asumamos que $\sqrt{2}$ es racional. Luego, deben existir dos enteros positivos a_1 y b_1, tales que:

$$\sqrt{2} = \frac{a_1}{b_1}, \qquad \textbf{(3)}$$

$$\text{con } 1 < \frac{a_1}{b_1} < 2 \qquad \textbf{(4)}$$

Ahora bien, como claramente $\frac{1}{\sqrt{2}-1} = \sqrt{2}+1$, sustituyendo (3) en el lado izquierdo y luego despejando el término $\sqrt{2}$ del lado derecho, se obtiene que:

$$\sqrt{2} = \frac{2b_1 - a_1}{a_1 - b_1} \qquad \textbf{(5)}$$

Por lo tanto, llamando a_2 al numerador y b_2 al denominador en (5), tenemos que

$$\sqrt{2} = \frac{a_2}{b_2}$$

con $2b_1 - a_1 < a_1$ y $a_1 - b_1 < b_1$, relaciones que se deducen de (4).
Luego, por el método del descenso infinito, queda demostrado que $\sqrt{2}$ es irracional. ■

Para demostrar el UTF para el caso n=4, se parte demostrando el siguiente:

Teorema: La ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras positivas.

Demostración (indirecta): Supongamos que existen *x*, *y*, *z* enteros positivos, sin factores comunes, que satisfacen la ecuación propuesta. Como la ecuación puede ser escrita: $(x^2)^2+(y^2)^2=z^2$, se tiene que x^2, y^2, *z* constituyen una terna pitagórica. Luego, del teorema 1, se tiene que existen enteros *p* y *q*, sin factores comunes y de distinta paridad, tales que:

$$x^2 = p^2 - q^2 \qquad \textbf{(6)}$$

$$y^2 = 2pq \qquad \textbf{(7)}$$

$$z = p^2 + q^2 \qquad \textbf{(8)}$$

Como *p* y *q* tienen distinta paridad, se puede suponer que *p* es impar y *q* par.
Ahora bien, como 2*pq* es un cuadrado (7), se tiene que:

$$q = 2u^2 \qquad \textbf{(9)}$$

$$p = v^2 \qquad \textbf{(10)}$$

Como de (7) se tiene que *x*, *q*, *p* son también una terna pitagórica, nuevamente por el teorema 1, existen enteros positivos *r* y *s*, tales que:

$$x = r^2 - s^2 \qquad \textbf{(11)}$$

$$q = 2rs \qquad \textbf{(12)}$$

$$p = r^2 + s^2 \qquad \textbf{(13)}$$

De (9) y (12) $u^2 = rs$, luego:

$$r = g^2 \quad \textbf{(14)}$$

$$s = h^2 \quad \textbf{(15)}$$

Combinando (10), (13), (14) y (15), se obtiene que:

$$g^4 + h^4 = v^2 \quad \textbf{(11)}$$

Como por (10) $p^2 = v^4$, usando (8) se obtiene que $v < z$.

Por lo tanto, partiendo de una solución de $x^4+y^4=z^2$, hemos comprobado que existe otra solución $g^4 + q^4 = v^2$, con $v < z$. Luego, usando el *método de descenso infinito*, podemos concluir, finalmente, que la ecuación estudiada no tiene soluciones enteras. ■

Observación: Usando métodos similares al anterior, que tienen como base el método de descenso infinito, también es posible comprobar que otras ecuaciones, como por ejemplo $x^4 - 8y^4 = z^2$, tampoco tienen soluciones enteras y positivas.

Usando el Teorema precedente, se puede deducir fácilmente el UTF para el caso n=4:

Corolario: La ecuación de Fermat para n=4: $x^4 + y^4 = z^4$, no tiene soluciones enteras positivas.

Demostración: Resulta claro que, si la ecuación de Fermat para n=4 tiene una solución, ella genera una solución de la ecuación del Teorema precedente, observando que:

$$x^4 + y^4 = (z^2)^2$$

■

Comentarios finales:

Desde la presentación por Fermat de su llamado UTF, se realizaron innumerables intentos para demostrarlo, pero lo único que se lograba (en el mejor de los casos) era su comprobación para algunos casos particulares de n. Por ejemplo, en algunos escritos de Fermat se encontró una demostración para n=4, Euler en el año 1753 lo comprobó para n=3, Dirichlet en el año 1825 para n=5, Lamé y Cauchy en el año 1839 para n=7. Kummer en el año 1857 lo demuestra para casi todos los n menores que 100. Avanzando más rápido en el tiempo, llegamos al año 1983, cuando el matemático alemán Faltings logra probar que para n>4, la ecuación de Fermat, de tener soluciones, tiene solo una cantidad finita de ellas.

A. Wiles

Esta historia se cierra finalmente en el año 1993, más de tres siglos después de Fermat, año en el cual el matemático inglés Andrew Wiles logra finalmente una demostración completa del UTF, usando matemática muy avanzada y resultados importantes de muchos otros matemáticos. A. Wiles se conoció y se interesó en el UTF a los 10 años. Más tarde, luego de

trabajar muchos años y finalmente obtener una demostración del UTF, dijo: "*No hay otro problema que signifique lo mismo para mi. Yo he tenido el raro privilegio de hacer realidad en mi vida adulta, el sueño que había tenido en mi niñez. Yo sé que es un raro privilegio, pero si uno puede lograrlo, es la recompensa más grande que uno puede imaginar*"

Bibliografía

[1] Hardy, G. H. y Wright, E. M., *An introduction to the theory of numbers*, Claredon Press - Oxford, 1985.

[2] Ore, O., *Number theory and its history*, Mc Graw-Hill, 1948.

[3] Stewart, B. M., *Theory of Numbers*, The Macmillan Company, 1965.

[4] Vinogradov, I., *Fundamentos de la teoría de números*, Editorial Mir, Moscú, 1977.

[5] http://usuarios.lycos.es/somriure/pitag.htm
Interesante sitio de Internet, contiene un estudio detallado sobre las ternas pitagóricas.

[6] http://www.elementos.buap.mx/num38/pdf/fermat.pdf
Sitio Internet con el artículo *El enigma de Fermat*, de John Lynch.