

Nota sobre el último Teorema de Fermat y su demostración por Andrew Wiles

© P Kittl 1999

Facultad de Ciencias Físicas y Matemáticas
Universidad de Chile

RESUMEN

En esta nota se da una idea somera de la naturaleza del Último Teorema de Fermat y su reciente demostración. Se hace mención a las referencias históricas que marcan el proceso de su demostración por Andrew Wiles.

ABSTRACT

This comment gives a general idea of Fermat's Last Theorem and its recent. Here I mention some of the historic references that determine the process of its demonstration by Andrew Wiles.

El enunciado del último Teorema de Fermat (1601-1665) quedó anotado en un margen de su ejemplar de la Aritmética de Diofanto de Alejandría (150 A.C.) traducida al latín por Claude Gaspar Bachet (1581-1638) publicado en 1621. Este libro, con las numerosas notas marginales de Fermat, fue publicado en 1670 por su hijo Clemente Samuel. El enunciado del teorema dice que la ecuación

$$x^n + y^n = z^n \tag{1}$$

no tiene soluciones enteras para $n > 2$. Fermat afirma que tenía una demostración, pero se exime de darla argumentado que el margen es demasiado estrecho como para dárnosla.

Recientemente, en 1995, Wiles demostró este teorema. Para entender mejor este teorema veamos el caso $n=2$, para el cual existen soluciones enteras.

$$x^2 + y^2 = z^2 \quad (2)$$

Hagamos cuatro filas de números (esquema 1). En la primera van los números naturales $1, 2, \dots$; en la segunda sus **cuadrados** $1, 4, 9, \dots$; en la tercera la diferencia entre los cuadrados vecinos $3, 5, 7, \dots$; en la cuarta las diferencias de las diferencias $2, 2, \dots$

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	4	9	16	25	36	49	64	81	100	121	144	169	196
\	/	\	/	\	/	\	/	\	/	\	/	\	/
3	5	7	9	11	13	15	17	19	21	23	25	27	
\	/	\	/	\	/	\	/	\	/	\	/	\	/
2	2	2	2	2	2	2	2	2	2	2	2	2	2

Esquema 1.

Los elementos de la segunda fila se obtienen sumando al cuadrado la diferencia, que es la serie de números impares, y se obtiene el cuadrado siguiente. Si nos fijamos en el número $25=(5)^2$ vemos que se tiene:

$$144 + 25 = 169 \quad (3)$$

$$(12)^2 + (5)^2 = (13)^2$$

Es fácil generalizar esta fórmula obteniéndose:

$$(2n + 1)^2 + [2n \cdot (n + 1)]^2 = [2n \cdot (n + 1) + 1]^2 \quad (4)$$

que da una serie de soluciones enteras a la ecuación (2). La obtención de soluciones enteras en forma matemática y experimental puede hacerse con un computador.

En la serie de cuadrados $4, 9, \dots$, se busca para uno cualquiera de los cuadrados si el menor tiene alguno que sumado al primero da el cuadrado elegido. Por ejemplo, para $(5)^2 = 25$, tenemos:

$1 + 4 = 5$	$4 + 9 = 13$	$9 + 16 = 25$
$1 + 9 = 10$	$4 + 16 = 20$	$9 + 25 = 34$
$1 + 16 = 17$	$4 + 25 = 29$	
$1 + 25 = 26$		

Esquema 2

Solamente se obtiene el caso $(3)^2 + (4)^2 = (5)^2 = 9 + 16 = 25$. Se ve cómo fácilmente puede obtenerse los casos posibles para un cuadrado cualquiera. El caso general, es decir, la solución de la ecuación (2) cuando x , y , o z no tienen un divisor común es la siguiente:

$$\begin{aligned}x^2 + y^2 &= z^2 \\x &= u^2 - v^2 \\y &= 2 \cdot u \cdot v \\z &= u^2 + v^2\end{aligned}\tag{5}$$

u y v son **números primos** entre sí; uno de ellos es par y el otro impar. Si x , y , z tuvieran un divisor común, la ecuación podría escribirse como sigue:

$$(n \cdot x)^2 + (n \cdot y)^2 = (n \cdot z)^2\tag{6}$$

En tal caso, podría obtenerse una solución x , y , z , que conforman una solución reducida.

La **sucesión** de los números primos:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots\tag{7}$$

puede obtenerse fácilmente con el método de la **criba de Eratóstenes** (275-194 A.C.).

Usando la sucesión (7) y las fórmulas (5) obtenemos la sucesión de soluciones reducidas:

$x = 3$	$y = 4$	$z = 5$	
$x = 5$	$y = 12$	$z = 13$	
$x = 15$	$y = 8$	$z = 17$	
$x = 7$	$y = 24$	$z = 25$	(8)
$x = 21$	$y = 20$	$z = 29$	
$x = 9$	$y = 40$	$z = 41$	
...	

Esta solución se puede estudiar en los tratados elementales de teoría de números de Rademacher y Toeplitz [1] y de Carmichael [2].

Todos estos tipos de investigaciones, tanto teóricas como numéricas se han aplicado al último Teorema de Fermat. Las investigaciones numéricas, con las últimas tecnologías computacionales no han podido encontrar una contradicción al teorema de Fermat. En tanto las investigaciones teóricas no lograron una demostración general sino para ciertos números particulares. Veamos cómo fue el desarrollo histórico de la búsqueda de la demostración general que finalmente obtuvo Wiles.

El primer paso para una demostración fue obtenida por Fermat para $n=4$, mediante el método conocido como **descenso infinito**. Aceptando que no

se cumple el teorema, se demuestra que se obtiene un absurdo, en este caso, el que los números enteros no tienen un mínimo [2]

Posteriormente, Leonard Euler (1707-1783), lo demostró para $n = 3$ introduciendo los enteros imaginarios, es decir números de la forma $p + q\sqrt{-1}$ [$p, q, (1,2,3,\dots)$].

Estas demostraciones se extienden a todos los números de la forma 3^m ó 4^m ($m=1, 2, 3,\dots$). Se vio entonces que sólo sería necesario probar el Teorema de Fermat para los números primos (3, 5, 7, 11, 13, 17, 19,...), puesto que todo número se puede expresar como producto de primos. Fue así entonces como Sophie Germain (1776-1831), propuso que se demostrara para los números primos de la forma $2p+1$ (3, 5, 7, 11, ...).

Peter Gustav Lejeune-Dirichlet (1805-1859) y Adrien Marie Legendre (1752-1833) probaron el teorema para $n = 5$ en 1825, y en 1839 Gabriel Lamé (1795-1870) lo prueba para $n = 7$ en forma simultánea con Augustin Louis Cauchy (1789-1857). De esta forma, en 1817 Lamé, proclama haber demostrado el teorema, y ambos dieron, antes de publicar la demostración, los fundamentos de la demostración que se basaba en la unicidad de la factorización de un número cualquiera en números primos. Como se trataba de **números imaginarios**, Ernest Edward Kummer (1810-1893) y Dimitri Mirimanoff mostraron que eso no se cumplía en este caso. Sin embargo esta demostración podía arreglarse, pero sólo hasta $n = 31$; para números menores de 100, en particular para $n = 37, 59, y 67$, no pudieron probarlo.

De esta forma es como termina lo que llamaremos etapa clásica de la demostración del teorema de Fermat.

En 1975 Andrew Wiles (1953-) comenzó a estudiar las **curvas elípticas** del tipo $y^2 = x^3 + ax^2 + b + c$, buscando obviamente las soluciones con números enteros.

Por ejemplo, $y^2 = x^3 - 2$ tiene por soluciones $5^2 = 3^3 - 2$, etc.

Cuál es el número E_p de soluciones?...Este problema es difícil porque este número es infinito. Sin embargo usando los **sistemas módulo p** , el número E_p resulta ser finito. Hay que recordar que un sistema módulo **p** es, por ejemplo:

$$p = 3 \quad 1, 2, 3, 3+1=1, 3+2=2, 3+3=3, 3+3+1=1,\dots \quad (9)$$

Así, para la ecuación $x^3 - x^2 = y^2 + y$, se tiene:

(10)

$$E_{p=1} = 1, E_{p=2} = 4, E_{p=3} = 4, E_{p=4} = 8, E_{p=5} = 4, E_{p=6} = 16, \\ E_{p=7} = 9, E_{p=8} = 16,\dots$$

Para esta época, Goro Shimura (1926-1958) y Yutaka Taniyama (1927-) estudiaron las simetrías de las formas modulares que cubren un espacio -por ejemplo- hiperbólico. Estas formas modulares contienen un número infinito de elementos básicos i . Cada uno de estos elementos básicos consiste en diferentes cantidades. M_i denota la cantidad del i -ésimo elemento básico. Por ejemplo, $M_1 = 1, M_2 = 2, M_3 = 4, \dots$ Shimura - Taniyama estudiaron la conjetura de que a cada forma modular le corresponde una curva elíptica y viceversa. Esta correspondencia se establece por la identidad de las sucesiones M y E :

$$M_1 = E_1, M_2 = E_2, \dots \quad (11)$$

En 1984, Gerhard Frey probó que si se puede probar la conjetura de Taniyama y Shimura, el teorema de Fermat estaba probado, lo que logró demostrando que se verifica lo siguiente:

$$A^N + B^N = C^N \Leftrightarrow Y^2 = X^3 + (A^N - B^N) X^2 - A^N B^N \quad (12)$$

De esta manera fue como entre 1984 y 1995, Wiles enfocó sus estudios a la forma de probar la conjetura de Taniyama y Shimura, lográndolo en 1995 con una cantidad muy grande de cálculos y cadenas lógicas, entre las cuales se distingue la *geometría diferencial*.

Una forma sencilla de ver la conexión del Teorema de Fermat con la geometría se obtiene tomando coordenadas homogéneas. Así que dividiendo la ecuación (1) por z^n se tiene:

$$\left(\frac{x}{z}\right)^n + \left(\frac{y}{z}\right)^n = 1 \quad (13)$$

Aquí $\mathbf{x} = \frac{x}{z}$ y $\mathbf{h} = \frac{y}{z}$ son dos coordenadas homogéneas, llamadas de esta forma por cuanto son adimensionales. Además, como z es mayor que x o y , tanto ξ como η tienen valores mayores que cero y menores que uno, es decir: $0 \leq \mathbf{x} \leq 1, 0 \leq \mathbf{h} \leq 1$. Así que la ecuación (13) se transforma en

$$\mathbf{x}^n + \mathbf{h}^n = 1 \quad (14)$$

En la fórmula (14), ξ es un cociente de números enteros que se denominan números o fracciones racionales. Veremos que pasa con η de acuerdo con el Teorema de Fermat. Cuando $n=1$, $\mathbf{h} = 1 - \mathbf{x}$ y a cada fracción racional ξ corresponde una η . La ecuación, $\mathbf{x} + \mathbf{h} = 1$, corresponde a una línea recta como se aprecia en la figura 1. Esta recta pasa por todas las fracciones

racionales. En otras palabras, establece una correspondencia biunívoca entre todas las fracciones racionales del intervalo $0 \leq x \leq 1$ con el intervalo $0 \leq h \leq 1$. Esta recta pasa por los puntos $(x = 0, h = 1)$ y $(x = 1, h = 0)$, como es el caso para todo n .

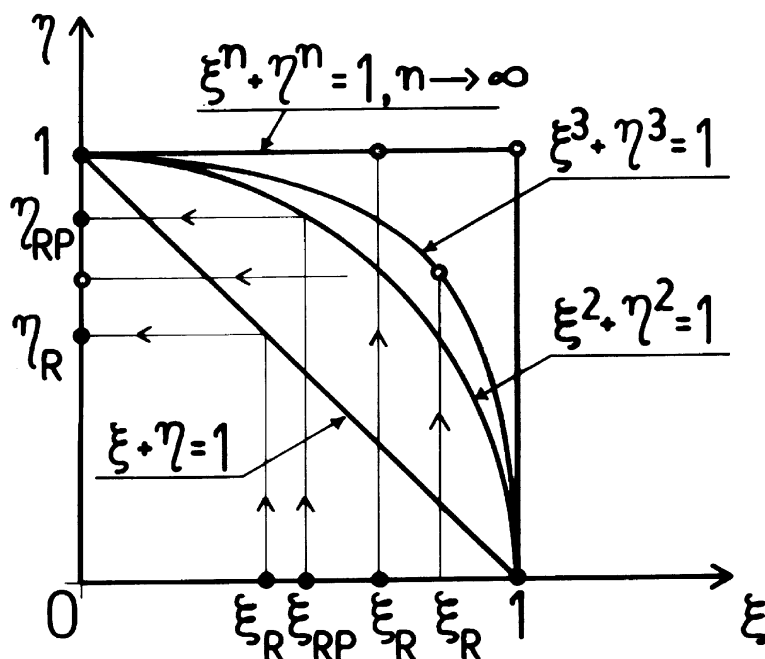


Figura 1: Representación gráfica de la ecuación de Fermat $x^n + y^n = z^n$. Tomando variables homogéneas $0 \leq x = \frac{x}{z} \leq 1$,

$0 \leq h = \frac{y}{z} \leq 1$ queda $x^n + h^n = 1$. Esta ecuación representa una recta que pasa por todos los racionales cuando $n=1$; un círculo que pasa solo por los racionales Pitagóricos, cuando $n=2$; una elipse generalizada cuando $n>2$, que no pasa por ningún racional. Cuando n es muy grande tiende a un segmento $\eta=1, 0 \leq \xi \leq 1$, que no contiene ningún racional (segmento de Dirichlet).

En el caso de $n=2$, la ecuación (14) se convierte en:

$$x^2 + h^2 = 1 \tag{15}$$

Esta es la ecuación de un círculo, donde todos los puntos equidistan del centro ($x = 0, h = 0$) y esta distancia es uno. Recuerde el Teorema de Pitágoras. Estas fracciones se obtienen de las soluciones reducidas (8), dividiendo por z:

$$\begin{aligned}
 x &= \frac{3}{5} & h &= \frac{4}{5} \\
 x &= \frac{5}{13} & h &= \frac{12}{13} \\
 x &= \frac{15}{17} & h &= \frac{8}{17} \\
 x &= \frac{7}{25} & h &= \frac{24}{25} \\
 \dots & & \dots &
 \end{aligned}
 \tag{16}$$

Entre las fracciones, el círculo solo pasa por estas fracciones racionales pitagóricas. Cuando n es mayor que 2, el teorema de Fermat afirma que tomando ξ valores racionales los η no pueden tomar el valor de ninguna fracción racional. Los η serán todos irracionales. Se denominan fracciones irracionales aquellas que se forman por adiciones, multiplicaciones, divisiones y extracción de raíz a partir de los racionales. Por ejemplo, para n=3, se tiene:

$$x^3 + h^3 = 1 \text{ y } \eta = \sqrt[3]{1 - \xi^3}
 \tag{17}$$

Cuando η es muy grande ($n \rightarrow \infty$), las curvas tienden a acercarse al segmento superior $0 \leq x \leq 1, \eta=1$. Pero este segmento superior no tiene ningún punto racional y se denomina recta de Dirichlet. En geometría mostramos que el teorema de Fermat consiste en afirmar que la figura que representa ecuación (13), para n=1, pasa por todos los racionales; para n=2, pasa por los racionales pitagóricos; para $n \geq 2$, no pasa por ningún racional.

Esto no pudo demostrarse en dos dimensiones y fue necesario pasar a 4 dimensiones, dándole a x e y valores complejos. La figura 1 es una sección de la superficie en 4 dimensiones cuando se anulan los puntos imaginarios.

En los libros de Singh y Aczel [3,4], que recomendamos calurosamente, se refiere con más detalles y en forma muy amena toda la historia, así como también se encuentra bibliografía más moderna y especializada. Aquí sólo tratamos de dar una ligera idea de lo que pasó y a qué se refiere el último teorema de Fermat, considerado como uno de los grandes desafíos de la matemática.

Este teorema resistió 300 años antes de ser demostrado y se lo consiguió gracias a un *isomorfismo* con propiedades geométricas. Es un ejemplo más de que muchas propiedades matemáticas se han desarrollado a

través de un isomorfismo entre la geometría y otra rama, en este caso, la teoría de números. Se pensó alguna vez que pertenecía a la clase de proposiciones matemáticas que no pueden ser probadas o negadas.

Otro caso fue el estudio de las soluciones de la ecuación de quinto grado, realizado por Felix Klein (1849-1925), quien las sistematizó y que se obtienen a través de *funciones modulares elípticas*, a través de los *grupos de simetría del icosaedro* [5].

Punteros de Interés

Para un análisis más profundo se recomienda leer el artículo contenido en la siguiente página WEB:http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html

Bibliografía

Rademacher, H. y Toeplitz, O., "Números y Figuras", Alianza Editorial, Madrid, 1970.
Carmichael, R. D., "The Theory of numbers and Diophantine Analysis", Dover, N.Y., 1959.
Singh, S., "Fermat's Enigma", Walker, N.Y., 1997.
Aczel, A. D., "Fermat's last theorem", Dell, N.Y., 1997.
Klein, Félix, "Elementary Mathematics from an Advanced Stand point, I, Arithmetics, Algebra, Analysis", Dover, N.Y., 1947.

Glosario

Números Primos: El que sólo es divisible por el mismo y por la unidad, como 5, 17, 23, etc.

Cuadrado: Todo número que es el producto de dos números iguales enteros, como $4=2 \times 2=2^2$, $9=3 \times 3=3^2$, etc.

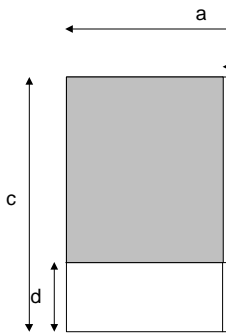
Criba de Eratóstenes: Nombre dado por Eratóstenes a un método de su invención para encontrar números primos menores o iguales a uno dado n . Se escriben los números 1 y 2 y la sucesión natural de los impares 3, 5, 7, ..., $n \leq r$. Se empieza a tachar de tres en tres a partir de $3^2=9$ inclusive; luego de cinco en cinco partiendo de $5^2=25$, y así se sigue hasta tachar de p en p , siendo p el menor número que cumple la condición $p^2 > r$. Los números primos contenidos en la primera centena son los que no están tachados.

									0	1	2	3	4	5
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8	9	0					

Descenso Infinito: Si puede probar algo para un número, eso está probado para un número menor y así siguiendo. En el caso de la ecuación de Fermat para $n=4$, éste probó que si existe una terna de soluciones debe existir una terna menor y así siguiendo. En el caso de los números enteros positivos, esto es un absurdo, luego es absurdo que exista una solución.

Por contrario se tiene la inducción finita; si algo es válido para un número significa que es válido para el siguiente y si ese algo es válido para el número uno, es válido para todos los números. Sería el ascenso infinito. Piénsese en una fila de soldaditos de plomo; si se cae el primero se comienzan a caer todos. Sería un método matemático para acabar con el militarismo.

Números Imaginarios: Son aquellos cuyo cuadrado es negativo, se denotan con la letra i . Así que $i^2 = -1$, por lo tanto $i = \sqrt{-1}$. Estos números imaginarios pueden ser complejos y constar de una parte real y otra imaginaria, por ejemplo $3+4i$, donde 3 y 4 son números enteros. Se multiplican de la siguiente forma: $(3+4i) \times (1+2i) = 3 \times 1 + 3 \times 2i + 4i \times 1 + 4i \times 2i = 3 + 6i + 4i - 8 = -5 + 10i$. Recordemos la regla de los signos para la multiplicación algebraica, $++ = +$, $+- = -$, $-- = +$, $-+ = -$. Esta regla se puede justificar con ayuda de una figura geométrica $(a - b) \cdot (c - d) = ac - ad - bc + bd$.



Cuando las partes del número complejo son enteros nos encontramos con enteros imaginarios o enteros complejos

Factorización de números imaginarios: Todo número admite ser descompuesto en factores primos, como por ejemplo $360 = 2^3 \times 3^2 \times 5$, y de una única manera. Esto se denomina Teorema Fundamental de la Aritmética y fue demostrado por Euclides en el libro IX de sus Elementos. Este teorema no es cierto para los números complejos, por ejemplo: $6 = 2 \times 3 = (1 + i\sqrt{5}) \times (1 - i\sqrt{5}) = 1 - i\sqrt{5} + i\sqrt{5} - i^2 \sqrt{5} \cdot \sqrt{5} = 1 + 5 = 6 = (2 + i\sqrt{2}) \cdot (2 - i\sqrt{2})$.

Ecuación Elíptica: Se denomina así porque se origina al tratar de determinar la longitud de un arco de elipse. Esta elipse es una curva que se puede obtener como los puntos cuyas distancias a dos puntos fijos cumplen la condición de que su suma es constante. Una elipse se traza fácilmente con dos clavos a los que se ata un hilo, en el que se hace resbalar un lápiz.

Sistemas módulo p: Son aquellos sistemas que cumplen la aritmética del reloj, en el cual $12^h + 3^h = 15^h = 3^h$. Este ejemplo es a módulo 12. Así que el número, por ejemplo 15, se divide por el módulo $\frac{15}{12} = 1 + \frac{3}{12}$ y el resto, es decir 3, es el valor del número módulo 12.

En general se trata de una operación o elemento que no modifica un sistema. Por ejemplo, el módulo de la suma es el cero, y el de la multiplicación es el uno. Así, $3+0=3$, y $3 \times 1=3$.

Como operación en geometría puede ser una traslación que no modifica una figura. Así, si un cuadrículado que cubre todo un plano infinito, lo trasladamos paralelamente a sus lados en una cantidad igual a la cuadrícula, el nuevo cuadrículado cubre exactamente al anterior. Si a la cuadrícula se la gira, alrededor de un vértice o del centro de una cuadrícula, noventa grados ocurre lo mismo: la nueva cuadrícula se superpone a la anterior. Exhibe entonces el cuadrículado tres simetrías, dos traslaciones y una rotación.

Simetrías de formas modulares: En el espacio común, un punto está determinado por tres números y cuando es llenado con diferentes formas, como ladrillos, exhibe un número limitado de simetrías. En el espacio de cuatro dimensiones, un punto está determinado por cuatro números y en ese espacio se le puede llenar con ladrillos de diferentes formas en un número ilimitado, como sus simetrías. Cada una de estas formas, con un número ilimitado de simetrías, se denominan formas modulares y pueden estar formadas por un número M_p de ingredientes diferentes. El espacio puede ser llenado con $M_1=1$, $M_2=3$, $M_3=6$, $M_4=10$, $M_5=15$, $M_6=21$, $M_7=28$, $M_8=36$, $M_9=45$, $M_{10}=55$, $M_{11}=66$, $M_{12}=78$, $M_{13}=91$, $M_{14}=108$, $M_{15}=126$, $M_{16}=146$, $M_{17}=166$, $M_{18}=188$, $M_{19}=210$, $M_{20}=236$, $M_{21}=264$, $M_{22}=294$, $M_{23}=326$, $M_{24}=360$, $M_{25}=396$, $M_{26}=434$, $M_{27}=474$, $M_{28}=516$, $M_{29}=561$, $M_{30}=608$, $M_{31}=656$, $M_{32}=708$, $M_{33}=762$, $M_{34}=818$, $M_{35}=876$, $M_{36}=936$, $M_{37}=1000$, $M_{38}=1068$, $M_{39}=1138$, $M_{40}=1212$, $M_{41}=1288$, $M_{42}=1368$, $M_{43}=1452$, $M_{44}=1540$, $M_{45}=1626$, $M_{46}=1716$, $M_{47}=1808$, $M_{48}=1900$, $M_{49}=1986$, $M_{50}=2076$, $M_{51}=2160$, $M_{52}=2248$, $M_{53}=2334$, $M_{54}=2424$, $M_{55}=2508$, $M_{56}=2596$, $M_{57}=2680$, $M_{58}=2766$, $M_{59}=2856$, $M_{60}=2940$, $M_{61}=3028$, $M_{62}=3114$, $M_{63}=3200$, $M_{64}=3288$, $M_{65}=3372$, $M_{66}=3460$, $M_{67}=3546$, $M_{68}=3636$, $M_{69}=3720$, $M_{70}=3808$, $M_{71}=3890$, $M_{72}=3972$, $M_{73}=4056$, $M_{74}=4140$, $M_{75}=4224$, $M_{76}=4308$, $M_{77}=4386$, $M_{78}=4464$, $M_{79}=4548$, $M_{80}=4630$, $M_{81}=4716$, $M_{82}=4800$, $M_{83}=4884$, $M_{84}=4968$, $M_{85}=5052$, $M_{86}=5136$, $M_{87}=5220$, $M_{88}=5304$, $M_{89}=5388$, $M_{90}=5472$, $M_{91}=5556$, $M_{92}=5640$, $M_{93}=5724$, $M_{94}=5808$, $M_{95}=5892$, $M_{96}=5976$, $M_{97}=6060$, $M_{98}=6144$, $M_{99}=6228$, $M_{100}=6312$.

Espacio hiperbólico: En geometría existen tres tipos de espacios: el euclidiano común, en el cual por un punto dado se pueden trazar una y sólo

una paralela; el elíptico, donde no se puede trazar ninguna paralela y el hiperbólico, con un número ilimitado de paralelas.

De estos espacios se pueden dar modelos comprensibles en tres dimensiones, pero los de cuatro dimensiones son más fáciles de entender por sus propiedades.

Sucesión: Conjunto ordenado de números según una cierta ley. Dichos números son los términos de la sucesión. Ejemplo: 2, 4, 6, ..., $2n$, ...

Geometría Diferencial: La que estudia las propiedades de las figuras muy próximas (en el entorno) de uno de sus puntos (elementos generales).

Isomorfismo: Correspondencia biunívoca entre los elementos de dos grupos abstractos. Esta correspondencia hace que a cada elemento de un grupo corresponde uno y sólo uno del otro. Por ejemplo, a cada número n le corresponde un solo par $2n$. A cada punto del espacio geométrico le corresponde una y solo una triada de números (x,y,z) .

Clase de las proposiciones que no pueden ser probadas o negadas: En la lógica formal se entiende por proposición a toda expresión de la cual se puede decir sin ambigüedad si es verdadera o falsa. Gödel demostró que existen proposiciones de las cuales se conoce un número finito de casos ciertos (como sucedía con el teorema de Fermat) pero no puede hacerse una demostración general de que son ciertas o falsas.

Funciones modulares elípticas: Las funciones elípticas aparecieron para resolver el problema de determinar la longitud de un arco de elipse. La elipse es un círculo achatado según una cierta proporción fija. Es el conjunto de puntos cuyas distancias a dos puntos fijos da una suma constante. Uniendo esos dos puntos con una recta se corta a la elipse en un punto. Otro punto cualquiera de la elipse se determina por el ángulo que forma la recta primera con otra que partiendo del punto, lo una con uno los puntos fijos. Así que la longitud del arco esta determinada por dos parámetros, el ángulo y el porcentaje de achatamiento. Este porcentaje está ligado a un número que se llama módulo de las funciones elípticas. Aquellas funciones que se pueden reducir a combinaciones de funciones elípticas con el mismo módulo, se denominan modulares elípticas. Estas funciones pueden formar una ecuación algebraica que tiene las mismas propiedades de simetría que el icosaedro y que es de quinto grado. Aparece la incógnita x elevada a la potencia cinco.

Grupo de Simetrías del Icosaedro: Un poliedro es un cuerpo limitado por polígonos situados en planos distintos, que forman el contorno del poliedro, y

cada una de las cuales es una cara de éste; los lados y los vértices son aristas y vértices del poliedro. Aquel poliedro con aristas, caras y ángulos entre caras iguales se denomina poliedro regular. Pitágoras descubrió que sólo son cinco: Tetraedro, Octaedro, Icosaedro, Cubo y Dodecaedro, delimitados por triángulos, cuadrados y pentágonos.

El icosaedro está formado por veinte triángulos y tiene simetrías tales que girando alrededor de un eje se superpone consigo mismo. Una ecuación de quinto grado tiene las simetrías de un icosaedro y se puede resolver por funciones modulares elípticas. Así como una de segundo grado se puede resolver por extracción de la raíz cuadrada.

Pablo Kittl es Profesor titular en el Departamento de Ingeniería Mecánica de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. Profesor titular en diversas universidades latino-americanas. Fellow de la American Academy of Mechanics, miembro correspondiente de la Academia Chilena de Ciencias, miembro de la Sociedad Científica Argentina, miembro de la American Association for the Advancement of Science, miembro de la Sociedad Chilena de Física. En los últimos treinta años ha trabajado en metalurgia, microscopía, cementos, materiales biológicos, fibrocementos y fatiga. Actualmente trabaja en mecánica de fractura y en resistencia probabilística de materiales. Ha publicado más de 150 trabajos.