RESEÑA HISTÓRICA DE ALGUNOS PROBLEMAS EN TEORÍA DE NÚMEROS[1]

Diego Pareja Heredia. ***Universidad del Quindío.***

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Facsímil de la portada de la "**ARITMETICA**" de **Diofanto de Alejandría,** originalmente editada por *Bachet* en 1650. En la versión que se muestra se incluyen las notas marginales hechas por el famoso matemático francés **Pierre de Fermat,** entre las que figura el hoy llamado "**Último Teorema De Fermat**"

INTRODUCCIÓN

El propósito de este trabajo, es describir, en forma sucinta, la historia de algunos problemas centrales de la Teoría de Números. Muchos de ellos han ocupado la atención de matemáticos, y aficionados a las matemáticas por varias generaciones, y en determinados casos hasta por siglos. Entre estos problemas se destacan: la Conjetura de Golbach, el Último Teorema de Fermat, el Teorema de los Números Primos, el Problema de Catalán y el Décimo Problema de Hilbert.

---

[1] Este artículo fue publicado en la revista "MATEMÁTICA ENSEÑANZA UNIVERSITARIA", No. 18 Marzo de 1981. Ha sido editado y puesto al día por el autor en Octubre de 2007.

Gauss consideraba a *las matemáticas como la reina de las ciencias y a la teoría de números como la reina de las matemáticas*. Este calificativo dado por *Gauss* a la teoría de números, tiene plena justificación, si se tiene en cuenta que, la historia de las matemáticas la tiene como su columna vertebral y porque grandes matemáticos, desde la antigüedad hasta nuestros días, la han cultivado y mantenido como una de las áreas más fecundas del terreno matemático. Los problemas de la teoría de números tienen diferente grado de dificultad. Algunos son fáciles de plantear y fáciles también de resolver, como es el caso de establecer la infinidad de los números primos. Fue *Euclides,* quien, en forma por demás elegante, mostró que el conjunto de números primos es *infinito.*

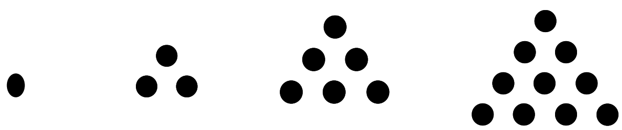
Hay problemas de fácil formulación aunque de muy difícil prueba. Ejemplos típicos de éstos, son la Conjetura de Golbach y el Último Teorema de Fermat. Hay un tercer grupo de problemas que se caracteriza por su difícil formulación e igualmente difícil prueba. A manera de ejemplo citamos aquí la siguiente proposición: Dos formas cuadráticas son congruentes en el campo racional si y sólo si son congruentes en los reales y en todos los cuerpos *p-ádicos.*

Los números enteros, materia prima de la teoría de números, tienen en conjunto, propiedades sumamente interesantes como veremos en el transcurso de la presente exposición. Empecemos por decir que cada entero en sí es interesante, pues si hubiese un conjunto de enteros positivos no interesantes, el menor de ellos ya sería de interés, contradiciendo su propia definición.

Godfrey Harold Hardy (1877-1947), el famoso matemático inglés, cuenta que en cierta ocasión comentó a *Ramanujan,* haber viajado en el taxi No. 1729, número éste, que en su opinión no tenía nada de interesante. El genio hindú le respondió: “Al contrario, 1729 es un numero muy especial, ya que es el primer entero positivo que puede expresarse como la suma de dos cubos, exactamente en dos formas diferentes”. En efecto, $1729 = 10^3+9^3 = 12^3+1^3$. El número $12^3 = 1728$, estudiado por *Ramanujan,* desempeña un papel importante en la teoría de formas modulares elípticas, área en la cual contribuyó profusamente.

S. Ramanujan (1887-1920) ***G. H. Hardy (1877-1947)***

Los enteros positivos tuvieron singular importancia en la filosofía de la escuela pitagórica (siglos VI-III A.C.). Para *Pitágoras* todo era números y el número era la única vía de llegar a la esencia de las cosas. Los enteros positivos fueron clasificados como *femeninos (pares) y masculinos (impares).* A los primeros números se les asociaron atributos humanos. Por ejemplo, el 2 significaba *opinión,* el 4 *justicia (*por ser el primer cuadrado perfecto), el 5 *matrimonio* (suma de par e impar). El uno no era considerado estrictamente como un número, si no como el *"divino generador de todos los números".* De otra parte, para los pitagóricos, el uno era el punto, la recta el dos, una superficie el número tres y el cuatro estaba ligado a los sólidos. De la suma de estos, aparecía el número diez, el *tetractys*, considerado por ellos como potencia sagrada y omnipotente. El diez estaba clasificado entre los números triangulares. Estos números, como todos los números conocidos como poligonales, se obtenían a partir de arreglos geométricos del tipo que muestra la figura.



$\mathbf{T_1=1}$, $\mathbf{T_2=1+2}$, $\mathbf{T_3=1+2+3}$, $\mathbf{T_4=1+2+3+4}$,… $\mathbf{T_n=1+2+3+\ldots+n} = \frac{n(n+1)}{2}$

LAS TRIPLAS PITAGÓRICAS Y EL ÚLTIMO TEOREMA DE FERMAT.

Hay suficiente evidencia como para creer que los babilonios del II milenio antes de Cristo, conocían un procedimiento para obtener soluciones enteras de la ecuación

$$\mathbf{x^2+y^2=z^2} \qquad (*)$$

En efecto, en los años 40, fueron interpretadas por *O. Neugebauer y A. J. Sachs,* varias tablillas babilónicas de contenido matemático entre ellas, la Nº 322 de la colección Plimpton, en la cual aparecen muchas triplas pitagóricas (*a, b, c)* que satisfacen (*). La tripla *(3, 4, 5)* es una de ellas. Esta tripla pudo haberse encontrado por ensayo y error, pero no podría decirse lo mismo de la tripla,

(4961, 6480, 8161)

Que también aparece en la tablilla 322. Esto muestra que la cultura babilónica poseía probablemente la fórmula parra encontrar valores que satisficieran la ecuación diofantina (*). En el libro XII de los "Elementos" de Euclides se describe el método para hallar todas las triplas pitagóricas primitivas que resuelven la ecuación mencionada. En notación moderna la solución puede expresarse así:

$$(**) \quad x = 2uv, \quad y = u^2-v^2, \qquad z = u^2+v^2$$

Donde u y v son enteros positivos de diferente paridad (uno par, el otro impar), $u > v$ y u, v primos entre sí. Que (x, y, z), dados en (**) satisfacen (*), se obtiene directamente de la identidad algebraica:

$(u^2 + v^2)^2 = (u^2 - v^2)^2 + (2uv)^2$, donde $x^2 = (2uv)^2$, $y^2 = (u^2 - v^2)^2$, $z^2 = (u^2 + v^2)^2$.

La proposición más nombrada y quizás con el mayor número de demostraciones erróneas en la historia de las matemáticas, es el llamado *Último Teorema de Fermat.* **PIERRE DE FERMAT** (1601-1665), aunque jurista, logró su fama como matemático de gran creatividad. Al margen de su copia del libro "*Aritmética"*, escrito por *Diofanto* y editado por *Bachet* en 1650 (véase facsímil de la portada al comienzo del artículo), Fermat escribió:

> "*Descomponer un cubo en dos cubos, una cuarta potencia o en general una potencia en dos potencias de la misma denominación, por encima de dos, es imposible. Yo he encontrado una maravillosa prueba de este hecho, pero el margen es demasiado estrecho para contenerla*".

Han pasado tres siglos desde entonces y la demostración para el teorema sólo vino a encontrarse finalizando el siglo XX, con los trabajos de Andrew Wiles de la Universidad de Princeton. Es poco probable que Fermat conociera una demostración, más si se tiene en cuenta que, usando el método del descenso infinito, él demostró el teorema para el caso de cuartas potencias. La lucha por demostrar el Último Teorema de Fermat ha contribuido a crear todo un cuerpo de nuevas teorías, como es el caso de la teoría de cuerpo ciclotómicos y la teoría de ideales, iniciada en los trabajos de *Ernest Kummer (1810-1893).* Kummer probó el teorema para todos los primos regulares, pero aunque estos primos son empíricamente más abundantes que los irregulares, nadie ha podido mostrar su infinitud. Esto contrasta con el hecho de que es relativamente fácil demostrar que el conjunto de primos irregulares es infinito.

Simbólicamente el Último Teorema de Fermat, afirma que la ecuación diofantina

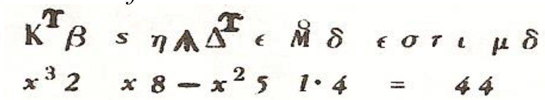
$$x^n + y^n = z^n$$

no tiene soluciones (*no triviales*) enteras, para n mayor que dos. Soluciones triviales se encuentran tomando una o todas las variables iguales a cero.

Una ecuación diofantina es una ecuación del tipo

$$P\,(x_1, x_2, \ldots, x_n) = 0$$

Donde P es un polinomio con coeficientes enteros y las indeterminadas, $x_1, x_2, \ldots, x_n$ toman valores enteros. Las ecuaciones diofantinas deben su nombre a *Diofante de Alejandría* (Siglo II de nuestra era), uno de los últimos matemáticos griegos que hizo aportes a la teoría de números. En su obra *"Aritmética",* ya mencionada, trata la solución de ecuaciones indeterminadas, e introduce un simbolismo especial que reduce en forma considerable la escritura de expresiones matemáticas. Esta forma de escribir enunciados matemáticos se conoce hoy como, *álgebra sincopada*. Un ejemplo ilustrativo, es la forma como *Diofanto* escribe la ecuación: $2x^3 + 8x - (5x^2 +4) = 44$, como:



La notación se explica en virtud de lo siguiente:

K^Υ Es una abreviatura de K^Υ *B* O Σ *(Kubos," cubo")*

ς Es una abreviatura de *αριθμος* *(Aritmos," número")*

⋔ Es una combinación de Λ e *I* en la palabra ΛΕ*I*ΨΣΙΣ *(Leipsis, " carencia").*

Δ^Υ Es una abreviatura de Δ^Υ NAMIS (Dinamis, "potencia").

$\overset{\circ}{M}$ Es una abreviatura de MONAΔEZ (Monades, "unidades")

Єστι ("es igual a") se deriva de la palabra *ι σ ο s* (isos, "igual")

Las letras β, δ, Є, η, μ se usan aquí para representar los números 2, 4, 5, 8 y 40 respectivamente.

Euclides merece sitial de honor en la teoría de números, puesto que a él debemos el primer estudio más o menos sistemático de algunas propiedades de los números enteros positivos. En el libro X de los "*Elementos*", Euclides prueba la infinitud de los números primos; presenta un algoritmo (*Algoritmo de Euclides*) para determinar si dos números son o no primos entre sí, y además, como ya mencionamos, encuentra en términos de los parámetros u y v la solución general de la ecuación $\mathbf{x^2+y^2=z^2}$.

Gauss y el Teorema de los Números Primos

Carl Friedrich Gauss (1777-1855)**,** uno de los más grandes matemáticos de todos los tiempos, descubrió en 1792 que los números primos no están caprichosamente distribuidos en el conjunto de los números enteros, sino que al contrario, siguen invariablemente una ley en cuanto a su densidad. Esta ley se conoce como el Teorema de los Números Primos.

Teorema de los Números Primos. Si $\pi(x)$ representa el número de primos en el intervalo $[1, x]$, entonces $\pi(x)$ es asintóticamente igual a $x/\log x$. *(logx* significa aquí, logaritmo natural de x). Más exactamente

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(A\log x + B)} = 1.$$

Gauss llegó a esta conclusión al comparar la integral,

$$\int_a^b \frac{dx}{\log x} \quad .$$

Con el número de primos que puede haber en el intervalo [*a, b*]. El observó por ejemplo, que el número de primos en el intervalo entre 2600000 y 2700000 es de 6762, número éste, muy próximo a la integral de arriba; cuyo valor para *a*=2600000 y *b*=2700000 es de 6761.332. Hay sobrada razón entonces, para asignarle a *Gauss* la prioridad del descubrimiento de este teorema. No obstante, debe reconocerse que, quien primero enunció la conjetura que condujo al teorema, fue *Adrien Marie Legendre* (1752-1833), en la forma:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(A\log x + B)} = 1 .$$

Donde A y B son constantes.

Gauss fue un perfeccionista en todo; solamente cuando obtenía un resultado muy pulido, permitía su publicación. Su dogma siempre fue: "PAUCA SED MATURA" (poco, pero maduro). Esto explica, por qué muchos resultados atribuidos a él, no fueron publicados en vida del autor. Algunos de éstos se encontraron en su diario, otros más, se obtuvieron de la correspondencia que mantuvo con científicos contemporáneos.

Carl f. Gauss (1777-1855)

P. L. Tchebycheff (1821-1894), el matemático ruso más brillante del siglo XIX, estuvo muy cerca de la demostración del teorema de los números primos. En efecto, él logró demostrar que de existir el límite de $\pi(x)/(x/\log x)$, cuando $x\to\infty$, éste debe ser necesariamente uno. En 1860, B. *Riemann* (1826-1866) estudió el Teorema de los Números Primos en conexión con la función:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad , \qquad s > 1$$

Conocida como función zeta de Riemman, dando origen, a una de las áreas más fértiles de las matemáticas, la *teoría analítica de números*. Riemann logró extender ζ a todo el plano complejo como una función meromorfa, y se inmortalizó al proponer la hipótesis de que la función zeta ζ, tiene sus ceros no triviales (los triviales están en los enteros pares negativos) en la recta *Re*(*s*) = *x*= *1/2.* Esta hipótesis no ha podido aún establecerse definitivamente, aunque todo cero encontrado satisface la hipótesis.

El Teorema de los números primos fue demostrado en forma definitiva por *Jacques Hadamard* (1865-1963) e independientemente por *Charles J. de la Vallée-Poussin* (1866-1962) en 1896. La prueba no es nada elemental y para lograrla se requiere el conocimiento de la Teoría de Variable Compleja. En 1948, el matemático noruego *Atle Selberg* (1917-2007), *Medalla Fields* 1950 y el matemático húngaro *Paul Erdös* (1913-1993), descubrieron una demostración que no usa teoría de variable compleja, pero sí, una gran cantidad de pasos, que hacen de ella, una prueba tediosa y complicada.

La afición de Gauss por la teoría de números se manifestó tempranamente. Un día de 1785, un maestro de escuela alemán, con el propósito de mantener ocupados a sus pupilos, les asignó la tarea de sumar los primeros cien números naturales, esto es, 1+2+…+100. Hay una fórmula para ello, que el profesor conocía, pero los alumnos de segundo elemental, presumiblemente no. Con esto en mente, el profesor esperaba mantener ocupados a sus estudiantes por lo menos una hora. Sin embargo, uno de los alumnos, Carl Frederich Gauss, casi al minuto presentaba la respuesta correcta: 5*050.* Gauss, a esa edad ya conocía la fórmula.

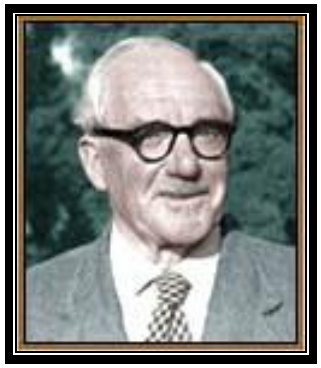
Cuando a Gauss se le comentó en una ocasión, que alguien afirmaba que el Teorema de Wilson nunca podría ser demostrado por falta de notación apropiada, dijo: "No son notaciones, sino nociones lo que se requiere" y demostró el teorema de inmediato. Una visión del Teorema de Wilson afirma que si se divide $(p-2)!$ por p, el residuo debe ser necesariamente 1. A la edad de 24 años, Gauss publicó el primer tratado sobre teoría de números, titulado "*Disquistiones Arithmeticae".* En él aparece por primera vez un estudio sistemático de las congruencias y además varias pruebas del *Teorema de Reciprocidad Cuadrática.*

El Problema de Catalan y la Conjetura de Goldbach

El problema de Catalan es otro ejemplo de un problema de fácil formulación pero de muy difícil prueba. Este tiene que ver con potencias de enteros, digamos, los cuadrados: 1, 4, 9,…, cubos: 1, 8, 27,… cuartas potencias: 1, 16, 81..., etc. Hace más de cien años, el matemático belga Eugène Catalan (1814-1894), conjeturó que las únicas dos potencias de enteros, que difieren en 1, son 2^3 y 3^2, esto es 8 y 9. El problema se puede expresar en términos de ecuaciones diofantinas en los siguientes términos. No existe soluciones enteras, diferentes de $x=3$, $y=2$, $u=2$, y $v=3$ para la ecuación diofantina:

$$x^u - y^v = 1, \text{ con } x > 0;\ y>0;\ u>1;\ v>1.$$

Solamente hasta hace muy poco el matemático inglés Alan Baker (Medalla Fields 1970), logró probar la conjetura, salvo para un número finito de casos. Sin embargo el número de casos excepcionales, aunque finito es demasiado grande para verificarlo con ayuda del computador. Recientemente el matemático suizo Preda Mihailescu[2] logró resolver en forma afirmativa este centenario y difícil problema.



John E. Littlewood (1885-1977)

En 1742, *Christian Golbach* (1690-1764), en carta dirigida a *Euler,* propuso el siguiente problema:

Conjetura de Golbach: *Todo número par mayor o igual que 4 se puede expresar como la suma de dos primos y todo número impar mayor que 8 es representable como la suma de a lo más tres primos impares.*

Todos los esfuerzos por demostrar la conjetura, resultaron fallidos hasta 1937, cuando el matemático soviético I. *M. Vinogradov,* demostró que todo impar mayor que cierta constante N_o (Constante de Vinogradov) se puede expresar como suma de a lo más tres números primos y consecuentemente todo par debe poderse expresar como suma de a lo más 4 primos. Una cota superior encontrada para N_o, es 10^{350000}. Este número aunque grande, es comparativamente pequeño en relación con otro número que aparece en conexión con $\pi(x)$ y conocido como número de Skewes y corresponde a:

$$10^{10^{10^{34}}}$$

Este número según Hardy era el mayor número natural conocido, usado con un propósito especial. El número de Skewes representa una cota superior debajo de la cual existe al menos un natural, tal que

$$\pi(x) > \int_2^x \frac{dt}{\log t} = Li(x)$$

Se había conjeturado que el número de primos en el intervalo [1 *,* x] *siempre* era menor o

[2] Un estudio histórico y detallado de la solución puede verse en:
METSANKYLA, J. CATALAN'S CONJECTURE: ANOTHER OLD DIOPHANTINE PROBLEM SOLVED. BULLETIN (New Series) OF THE AMERICAN MATHEMATICAL SOCIETY.
Volume 41, Number 1, Pages 43-57. Article electronically published on September 5, 2003

igual que *Li*(x). La conjetura tenía por soporte el hecho de que todos los valores calculados satisfacían la desigualdad. Sin embargo a comienzos del siglo, *J. E. Littlewood* (l855-1977), probó que hay infinitos naturales que violan la conjetura. Curiosamente, Littlewood no logró mostrar ninguno en particular. En la década de 1930 su discípulo *S. Skewes* encontró que existe al menos un número natural, menor que la cota anotada arriba para el cual la conjetura no se cumple. Esta cota se ha ido bajando, hasta obtenerse en 1.65×10^{1165}, debajo de la cual existe un natural tal que $\pi(x) > Li\ (x)$.

UN PROBLEMA DE HILBERT Y LA INFINITUD DE LOS PRIMOS GEMELOS.

David Hilbert (1862-1943)

David Hilbert (1862-1943) propuso en el Congreso Internacional de Matemáticas, celebrado en París en 1900, 23 problemas, el décimo de los cuales pregunta por la existencia de un algoritmo para determinar si una ecuación diofantina tiene o no solución. El problema sólo vino a resolverse en 1970 con el trabajo brillante del matemático soviético *Yuri Matyasevich*, quien probó la no existencia de tal algoritmo. Un algoritmo es un proceso que en un número finito de pasos conduce a un resultado determinado. El trabajo de *Matyasevich* fue la culminación de todo un cuerpo de ideas desarrollado por *Julia Robinson, Hilary Putnam y Martin Davis* en relación con funciones recursivas y computabilidad. Los números de Fibonacci dieron la clave en el trabajo de Matyasevich para la solución del décimo problema de Hilbert.

Como indicamos antes, son muchos los problemas abiertos de difícil solución en la Teoría de Números. Para terminar nuestros ejemplos, mencionemos la conjetura de la infinitud de los primos gemelos, esto es, de pares de primos de tipo p, $p+2$, como son por ejemplo: 3, 5: 11, 13; 17, 19; etc. Como consecuencia de esto podría concluirse que todo número par es expresable como la diferencia de números primos en infinitas formas. Recientemente, el matemático chino *Jungrun-Chen,* demostró una versión más débil del problema que nos ocupa. Específicamente, *Chen* probó que existen infinitas parejas de números impares consecutivos, p, $p+2$, tal que p es primo y $p+2$ es producto de a lo más dos factores primos.

CONCLUSIÓN

Las ramas más antiguas de las matemáticas son la geometría y la teoría de números. A diferencia de la geometría clásica de Euclides, de las rectas y de los círculos, considerada exhausta como ciencia investigativa, la Teoría de Números es, y seguirá siendo, un área fecunda, pletórica de problemas abiertos, y de continuos desafíos, tanto para el docto y el genio, como también para el matemático aficionado. El análisis diofantino (estudio de soluciones e ecuaciones diofantinas) está lleno de problemas fascinantes, mucho de ellos de vieja data y otros con corta pero brillante historia, como ocurre con el décimo problema de Hilbert, descrito antes.

BIBLIOGRAFIA

1) Edwards, H. Fermat's Last Theorem. Springer-Verlag. Berlin, Heidelberg, New York. 1977.

2) Eves. H. W. An Introduction to the History of Mathematics. Holt Reinhardt & Winston. New York.

3) Neugebauer, O., Sachs, A. Mathematical Cuneiform Texts. American Oriental Society. New Haven. 1945.

4) Pareja H., Diego. Srinivasa Ramanujan. Matemática-Enseñanza Universitaria. No. 4. Nov. 1977.

5) Pareja H., Diego. David Hilbert y su Escuela. Matemática-Enseñanza Universitaria. No. 7. Nov. 1978.

6) Pareja H., Diego. Comentarios Bio-Bibliográficos. Matemática-Enseñanza Universitaria. Nos. 9,11 y 12.

7) Pareja H., Diego. Temas de Historia de las Matemáticas. Versión para Internet que aparecerá en: www.matematicasyfilosofiaenelaula.info.

8) Ribenboim, P. 13 Lectures on Fermat's Last Theorem. Springer-Verlag. Berlin, Heidelberg, New York. 1980

9) Steen, L. A., ed. Mathematics Today. Twelve Informal Essays. Springer-Verlag. 1978

10) Zagier, D. The First 50 Million Prime Number. The Mathematical Intelligencer. Vol. 0. 1977.