"El último Teorema de Fermat y el problema de la existencia de factorización única en ciertos sistemas de números"

Silvia Etchegaray - Patricia Konic

Introducción

La construcción de estructuras algebraicas, produjo en el desarrollo del álgebra no sólo una transformación en su dominio de estudio, que hasta fines del siglo XIX había sido la resolución de ecuaciones, sino también una perspectiva diferente para su posterior evolución. Como consecuencia de estas originales ideas que le dieron una fecundidad sorprendente al Algebra, la misma resultó renovada en todas sus tendencias. Desde fines del siglo XIX los nuevos trabajos ya no están dominados por la preocupación de las aplicaciones en la resolución de ecuaciones, sino que comienzan a orientarse cada vez más al estudio de las estructuras algebraicas en si mismas, problema fundamental del Algebra actual.

En este artículo se explicitarán algunos procedimientos específicos del trabajo matemático que se constituyen en un aporte esencial para el desarrollo de la **teoría algebraica de números.** Este proceso se centrará en la presentación de resultados de la Teoría de divisibilidad en Sistemas de Números que abarcan al conjunto de los números enteros. Además, y con el fin de rescatar al desarrollo histórico del conocimiento matemático como iluminador para la detección de tales procederes específicos, se determinará en primer lugar al **"Ultimo Teorema de Fermat"**, como el problema donde tiene su origen, el tema planteado.

Desarrollo. El problema propuesto por Diofanto de Alejandría (250a d.C), en su Arithmética: **¿Habrá tres números tal que la suma de los cuadrados de dos de ellos sea el cuadrado del tercero?** O sea en notación moderna:

$\exists$ x, y, z $\in$ Nat / $x^2 + y^2 = z^2$?, fue retomado y generalizado por Pierre Fermat (1601-1665) quien tomó contacto con la obra diofantina en el año 1621. Según sus propias palabras **"es imposible para un cubo ser suma de dos cubos, para una cuarta potencia ser suma de dos cuartas potencias, o en general para un número que es potencia mayor que dos ser suma de dos números de esta misma potencia"**, o sea: no existen x, y, z $\in$ Z / $x^n + y^n = z^n$ todos no nulos si n>2[1], proposición conocida como el **Ultimo teorema de Fermat.** Los intentos de resolución de esta conjetura, en sus inicios, se centraron en la intención de extender el conjunto de los números enteros a nuevos conjuntos de números con la condición de que ellos preserven las propiedades fundamentales que permiten desarrollar la teoría de la divisibilidad en *Z*.

Con el propósito de que el lector comience a percibir la importancia del uso de nociones básicas de la teoría de la divisibilidad en *Z* , es que, para el abordaje de la problemática planteada, en primer lugar se desarrollará una demostración del problema planteado por Diofantino.

Para tal fin se utilizará una noción elemental de la teoría de números: el resto de dividir un número entero por un número natural, el que se denotará por $r_n(a)$, con a$\in$Z,

---

[1] Las ternas (± k, 0 = k) (0, ± k = k) con signos convenientes y, k entero son soluciones a la ecuación de Fermat.

$n \in N$ y se hará uso de las siguientes propiedades:

$$r_n(a+b) = r_n(r_n(a) + r_n(b)) \; [1] \quad r_n(a^2) = r_n(r_n(a))^2 \; [2]$$

Evidentemente para la solución de la ecuación, es suficiente encontrar la ternas coprimas *(x, y, z)* que la satisfagan. Esta reducción del problema asegura que *x, y, z* no pueden ser simultaneamente números pares. Tampoco pueden ser todos impares. Para esto, consideremos, por un lado, los restos al dividir por 4 de la ecuación original:

$$r_4(x^2+y^2) = r_4(z^2) \rightarrow \quad r_4(r_4(x^2) + r_4(y^2) = r_4(z^2) \quad \rightarrow$$

$$[1] \qquad\qquad [2]$$

$$r_4(r_4(r_4(x))^2 + r_4(r_4(y))^2) = r_4(r_4(z))^2 \quad [3]$$

y por otro lado consideremos la siguiente relación:

Si x es par vale que:

$r_4(x)$	$r_4(x^2)$
0	0
2	0

y, si x es impar vale lo siguiente:

$r_4(x)$	$r_4(x^2)$
1	1
3	1

lo cual aplicado a *[3]* produce la siguiente contradicción: *1+1=1*. Por lo tanto al menos uno de los tres números enteros *x, y o z* debe ser par. Sin embargo z no puede ser el número par, pues análisis similar al anterior nos conduce nuevamente a la contradicción, *(1+1=0)*.

En consecuencia y sin pérdida de generalidad se supone que x es par e y, z impares.

Además se sabe que $x^2 = z^2 - y^2 = (z-y)(z+y)$,

o equivalentemente $(x/2)^2 = (z-y)/2 \,.\, (z+y)/2$ [4]

Cabe destacar que $(z-y)/2$ y $(z+y)/2$ son coprimos pues,

$((z-y)/2 , (z+y)/2)$ divide a $((z-y)/2 + (z+y)/2)$ [5] y

$((z-y)/2 , (z+y)/2)$ divide a $((z-y)/2 - (z+y)/2)$ [6]

entonces por [5] $((z-y)/2,(z+y)/2)$ divide a z ,y además

por [6] $((z-y)/2,(z+y)/2)$ divide a y, lo que implica que: $((z-y)/2,(z+y)/2) = 1$.

Por lo tanto retomando [4] y por la propiedad de factorización única en producto de primos que poseen los números enteros garantizada por el Teorema Fundamental de la Aritmética, ambos números son cuadrados, o sea:

$$(z-y)/2 = \alpha^2 \qquad y \qquad (z+y)/2 = \beta^2$$

Luego $$z = \alpha^2 + \beta^2 \,, \quad y = \beta^2 - \alpha^2 \,, \quad x = 2\alpha.\beta$$

lo que necesariamente implica que α y β tienen distinta paridad. Pues si tuviesen la misma paridad, debido a que elevados al cuadrado la paridad se mantiene, su suma y su diferencia daría como resultado un número par. Recíprocamente dando valores enteros positivos a α y β, coprimos y de distinta paridad, se obtienen todas las ternas positivas que resuelven la ecuación diofantina con la condición x,y,z coprimos debido a que:

$$x^2 + y^2 = (2\alpha\beta)^2 + (\beta^2-\alpha^2)^2 = (\alpha^2 + \beta^2)^2 = z^2$$

La solución general es $x = d\ 2\ \alpha\beta$, $y = d(\beta^2 - \alpha^2)$, $z = d(\alpha^2 + \beta^2)$.

Ahora bien, retomando la conjetura que nos ocupa, para avanzar en su resolución basta considerar $n=4$[2] ó **n un primo impar**. Esto es así pues si la conjetura vale para algún n, vale entonces para todo múltiplo de él, ya que:

si $m=nt$, $t \in Z$ $X^m + y^m = z^m$, implica $(x^n)^t + (y^n)^t = (z^n)^t$.

En el tratamiento del caso $n=3$ se rescatará **el procedimiento** utilizado por el gran matemático del siglo XVII Euler[3], más allá de que éste haya cometido uno de los errores más frecuentes en las múltiples formas de tratar de demostrar la famosa conjetura: **creer que en nuevos conjuntos de números, por él utilizados era verdadera la unicidad en la factorización que asegura el Teorema Fundamental de la Aritmética y por ende todos los resultados de divisibilidad que de él se deducen.**

En este caso Euler , trabajó con el anillo de números complejos de la forma $a+b\sqrt{-3}$, $a,b \in Z$, tratando de generar en ese conjunto una aritmética similar a la del anillo Z, no dándose cuenta que $Z(\sqrt{-3})$ no admite factorización única, ya que por ejemplo el número 4 se puede factorizar como: $4 = 2.2$ ó $4 = (1 + \sqrt{-3}).(1 - \sqrt{-3})$.

Claro...se debería probar que $(1+\sqrt{-3})$ y $(1-\sqrt{-3})$ son números primos en el anillo

---

[2] Demostración dada por el propio Fermat con su método del descenso infinito. Para detalles consultar Vargas REM Vol 2.2.

[3] Para una prueba actual referirse a Niven Zuckerman, pág.213.

$Z(\sqrt{-3})$. Para esto se comenzará por recordar algunas definiciones y propiedades de los números en el anillo $Z(\sqrt{m})$, con m $\in$ Z y libre de cuadrados[4], que se utilizarán para entender la necesidad de este planteo y su demostración.

Definición 1: Una **unidad** en $\mathbf{Z}(\sqrt{m})$ es un divisor de 1. En particular siempre 1 y -1 son unidades. Esto es, $\xi \in Z(\sqrt{m})$ es unidad si existe $\eta \in Z(\sqrt{m})$ de modo que $\xi \eta = 1$.

Definición 2: Para $b \in Z(\sqrt{m})$. Los números de la forma ξ. b con ξ unidad son los **asociados** al número b.

Definición 3: Un número $b \in Z(\sqrt{m})$ es **primo** si y sólo si es divisible por las unidades y sus asociados.

Definición 4: El **conjugado** de un número $\xi = a+b\sqrt{m}$, es $\xi' = a-b\sqrt{m}$

Definición 5: La **norma** $N\xi$ del número ξ es $\xi.\xi' = a^2 - m.b^2$

Propiedades: (i) La norma del producto de dos números es el producto de sus normas, o sea $N(a.b) = Na.Nb$

(ii) La norma de una unidad es 1, y todo número cuya norma es 1 es una unidad.

(iii) Un número cuya norma es un entero primo es primo.

---

[4]Un número entero es libre de cuadrados cuando en su factorización única en producto de primos, éstos aparecen con exponente igual a uno.

Ahora estamos en condiciones de probar que $1+\sqrt{-3}$ es primo, para lo cual es suficiente, razonando por el absurdo, plantear la siguiente suposición:

$1+\sqrt{-3} = (a+b\sqrt{-3}).(c+d\sqrt{-3})$, luego aplicando la norma a ambos miembros y por propiedad (i), se logra que: $4 = (a^2 + 3b^2).(c^2 + 3d^2)$ por lo que necesariamente $a^2 + 3b^2 = 2$, ya que ninguno de los dos factores es una unidad por propiedad (ii). Pero, 2 no puede ser de esta forma por ser a y b enteros, por lo tanto $1+\sqrt{-3}$ es primo.

Análogamente se demuestra que $1-\sqrt{-3}$ es primo lo que inevitablemente contradice la unicidad en la factorización, propiedad que Euler no consideró.

Sin embargo, en este caso, este error, es muy fácil de solucionar, porqué?... tal como lo propone Lamé (1795-1870), si tratamos de resolver la ecuación diofantina: $x^3 + y^3 = z^3$ utilizando una estrategia similar al caso $n=2$, se obtiene: $x^3 = z^3 - y^3$ de esto, $x^3 = (z-y)(z^2 + z.y + y^2)$, y ahora, factorizando el segundo factor mediante la introducción de las raíces cúbicas de la unidad[5] w y w^2 se logra:

$x^3 = (z-y)(z- w.y)(z-w^2.y)$, expresión que obviamente no pertenece a Z, sino a un nuevo conjunto que no sólo contiene a Z, sino a w y w^2, y que se denota $Z(w)$. Este sí es un dominio de factorización única, donde se puede demostrarla imposibilidad de solucionar: $x^3 + y^3 = z^3$. *(cf. Hardy-Wright)*

---

[5]Esta idea tuvo su origen en: Lagrange(1736-1813) quien marcó la posibilidad de introducir raíces n-esimas de la unidad en el tratamiento del problema de Fermat.

O sea se ha subsanado el error de Euler, pues $Z \subset Z(\sqrt{-3}) \subset Z(w)$ y se conserva el procedimiento primitivo que tal como se anticipara es la idea directriz de esta forma de abordaje al problema: **"Encontrar un conjunto que contenga a *Z*, que conserve sus propiedades,en el cual la ecuación planteada no tenga solución, por lo que obviamente no tendrá solución en *Z*".**

Situados en este punto, cuál será la continuación natural de tal investigación? Sin duda generalizar la introducción de raíces n-ésimas de la unidad en la solución de:

$x^n + y^n = z^n$. *Escribamos*

$z^n = x^n + y^n = x^n - (-y)^n = (x+y)(x+\omega.y).....(x+\omega^{n-1}.y)$, con n impar. O sea, este problema es estudiado en el conjunto:

$Z(\omega_n) = \{a_0 + a_1\omega^1 + ...+ a_{n-1}\omega^{n-1} \ , \ a_i \in Z\}$ denominado: **Anillo de enteros ciclotómicos de grado n.** Se trata de hacer en este anillo una aritmética similar a la construida en *Z*.

Fue el mismo Lamé quien en 1847 presentó una demostración de la conjetura de Fermat, basándose en las ideas precedentemente expuestas, pero fue Liouville [1809-1882] quien en la misma exposición oral Lamé rebatió su argumento indicando la necesidad de demostrar la unicidad en la factorización de los números pertenecientes a $Z(\omega_n)$. Es de destacar que la demostración de un toerema de unicidad en el anillo mencionado, no es evidente ni siquiera verdadero para todo n.

En efecto, recién en 1976 se ha podido demostrar que sólo para $n=3,5,7,11,13,17,19$ $Z(\omega_n)$ es dominio de factorización única. c.f Unique factorization in cyclotomic fields, Jour. f. Reine u. Angew. Math 286-287 (1976).

Conociendo ya este avance en la resolución del problema se percibe claramente que la investigación se ha centrado en tratar de preservar la unicidad que nos brinda el Teorema Fundamental de la Aritmética en nuevos conjuntos de números.

Esta es la concepción que guió el trabajo de Kummer [1810-1893], quien al tratar de remediar esta situación trabaja despegado de las raíces de la unidad y construye una nueva clase de números que los llama números ideales . Las ideas de Kummer constituyen la génesis de la actual Teoría algebraica de números. cf. Dieudonné.

Por último cabe reafirmar que con éste análisis se pretende generar formas de pensamiento matemático, mostrando una sucesión de dificultades que permitieron la construcción de conceptos fundamentales, hecho que favorece reconocer el real funcionamiento de esta ciencia. En este caso particular se dimensiona, tal como lo señala Gentile, una de las ideas mas fecundas en toda la historia del desarrollo del Algebra y la Aritmética: **extender el ámbito natural de aplicación de un concepto y resolver allí el problema propuesto.**

Finalmente, puntualizamos que Wiles ha resuelto el problema de Fermat en el año 1993. Su solución se encuentra publicada en la bibliografía indicada sobre Wiles. Un bosquejo de la demostración se encuentra en http://www.ams.org.

Bibliografía

GENTILE, Enzo - Aritmética Elemental en la Formación Matemática- O.M.A. (1991).

KLINE, Morris- Mathematical Thought fron Ancient to Modern Times. OXFORD UNIVERSITY PRESS.

NIVEN Y ZUCKERMAN- An Introduction to The Theory of Numbers- JOHN WILEY Y SONS INC.

HARDY- WRIGHT - Introduction to Number Theory.

WILES A. Modular Elliptic curves and Fermat's Last Theorem. Annals of Math. Vol 141, No 3, 1995 443-551.

DIEUDONNE . Abregu des histoires des Mathematiques. 2 Vol.

Departamento de Matemática. Facultad de Ciencias Exactas-Fco.Qca y Naturales.

Universidad Nacional de Río Cuarto (U.N.R.C.).