Pro Mathematica Vol. XIII, Nos. 25-26, 1999

REPRESENTACIÓN DE NÚMEROS POR FORMAS CÚBICAS

Luis ***Gómez Sánchez A.***

Abstract

An old conjecture still unproved says that on $\mathbb{Z}$ every number is a sum of four cubes. We show here that this is so on $\mathbb{Q}$.

1. Introducción

Un célebre teorema de la Teoría de Números – el mismo que da lugar a sendos dificilísimos problemas para cada exponente r – establece que para todo entero $r > 1$, existe un entero s tal que la forma

$$(x_1, x_2, \cdots, x_s) \mapsto x_1^r + x_2^r + \cdots + x_s^r$$

(a la aproximación del signo en cada sumando), representa todo entero natural. En otros términos, todo número natural es igual a una suma algebraica, de un cierto número s de potencias r-ésimas perfectas, donde r es arbitrario y s depende de r [2].

✏ *Profesor jubilado de la Escuela de Ciencias, Departamento de Matemáticas, Universidad de Oriente, Venezuela.*

El problema inmediato que se deriva de este hermoso resultado, conjeturado por Waring en 1770 y demostrado por Hilbert en 1909, es el siguiente: Dado r, ¿cuál es el mínimo valor apropiado de s ?

El estado actual del problema en $\mathbb{Z}$ es el que exponemos a continuación (al menos hasta no hace mucho y aclaramos que en $\mathbb{Z}$ porque el problema análogo se investiga en cuerpos arbitrarios, en particular cuerpos finitos y p-ádicos).

$$r = 2$$

Para $r = 2$ el valor requerido de s es 4, lo que constituye el famoso teorema de los cuatro cuadrados de Lagrange (todo entero no negativo es una suma de 4 cuadrados). Se descarta $s = 2$ por el teorema siguiente:

Teorema.- Sea n un entero natural y $n = \prod p_i^{n_i}$ su descomposición en factores primos. El entero n es una suma de dos cuadrados si y sólo si para cada uno de sus factores primos p_i que sean congruentes con -1, módulo 4, el exponente n_i es par [3].

Así, por ejemplo, si $n = 7N$ donde N no tiene factores primos de la forma $4m - 1$, entonces n no es suma de dos cuadrados pero $7n$ sí lo es.

Tampoco $s = 3$ sirve por el

Teorema.- Para que un entero positivo n sea suma de tres cuadrados, es necesario y suficiente que él no sea de la forma $4^a(8b - 1)$ donde a y b son enteros no negativos [4].

Así por ejemplo, los números n no múltiplos de 4, son una suma de tres cuadrados sí y sólo si $n \equiv 1, 2, 3, 5, 6 \pmod 8$ por lo cual la forma $f(x, y, z) = x^2 + y^2 + z^2$ no es sobreyectiva en $\mathbb{N}$. En cambio la forma $f(x, y, z, w) = x^2 + y^2 + z^2 + w^2$ sí representa todo entero no negativo por el mencionado teorema de Lagrange.

$$r = 3$$

Una antigua conjetura, aún no demostrada, sostiene que para los cubos ($r = 3$) el valor requerido de s es también 4, como en el caso de los

cuadrados ($r = 2$). Aquí demostramos que $s = 4$ vale efectivamente si se considera valores racionales, es decir demostramos que para todo entero n, existen 4 racionales a, b, c, d tal que $n = a^3 + b^3 + c^3 + d^3$. El resultado no es muy importante ya que considera las variables dentro de un conjunto de mayor "*operatividad*", en el cuerpo $\mathbb{Q}$ y no en el anillo $\mathbb{Z}$. No obstante, creemos que dicho resultado no carece de cierto interés.

Aclaremos que esta conjetura (en $\mathbb{Z}$, no lo olvidemos) es bastante plausible y ha sido parcialmente demostrada. Se sabe que es válida para todos los números que no son congruentes con ± 4 módulo 9; es decir, para su total demostración bastaría con limitarse a los enteros de la forma $9m \pm 4$ lo cual ha sido verificado para aquéllos menores que 1000 [2]. También se ha demostrado que en este caso, no es posible explicitar soluciones por polinomios lineales, tal como sucede por ejemplo con la identidad

$$18m + 8 = (m-5)^3 + (-m+14)^3 + (3m-30)^3 + (-3m+29)^3$$

la cual, obviamente, responde por la afirmativa a la conjetura para cierta clase de números.

Se sabe por otro lado que en el caso de cubos que estamos viendo, los valores $s = 2$ y $s = 3$ no sirven pero no se conocen hasta la fecha caracterizaciones en $\mathbb{Z}$ similares a las dadas para los cuadrados. El tópico es en verdad difícil ya que involucra curvas elípticas (para $s = 2$) y superficies cúbicas (para $s = 3$), temas ambos muy complejos.

$r \geq 4$

El problema crece mucho en dificultad. Hasta donde sabemos, se ha llegado a demostrar que, para $r = 4$, se debe tener s igual a 9 ó 10 pero no se ha podido establecer cuál de estos dos valores es el definitivo. Tampoco se sabe caracterizar los números en relación a $s < 9$.

En cambio para $r > 4$, según T.M. Apóstol en su "*Introducción a la Teoría Analítica de Números*", se sabe hallar en la actualidad los valores correspondientes de s.

2. El Resultado en $\mathbb{Q}$

Demostramos ahora el siguiente

Teorema.- En $\mathbb{Q}$, todo elemento es suma de cuatro cubos no nulos.

Utilizamos primero una caracterización de una suma binomial.

Lema.- Se tiene la equivalencia

$$a+b=c \Leftrightarrow (9ab^2+(b-a)^3)^3+(9a^2b-(b-a)^3)^3=27abc(a^2+ab+b^2)^3.$$

Demostración: Basta con efectuar los cálculos. Una prueba más ilustrativa se puede ver en [1].

Volviendo a la conjetura presentada, hemos dicho qué $s = 2$ no sirve para los cubos y en efecto se sabe que hay una infinidad de enteros que no son una suma de dos cubos no nulos de racionales, por ejemplo $n = 1$ lo cual constituye el último Teorema de Fermat para el exponente 3. El lema dado establece una infinidad de números representables sobre $\mathbb{Q}$ por la forma cúbica $f(x, y)=x^3+y^3$, a saber, aquellos de la forma $ab(a + b)$. De esto se deduce sin dificultad que si se consideran las expresiones siguientes:

$$A_1=a^5+10a^4-8a^3+16a^2+64a-32$$
$$A_2=a^5-10a^4-8a^3-16a^2+64a+32$$
$$A_3=-a^5+8a^4+8a^3-16a^2+80a+32$$
$$A_4=-a^5-8a^4+8a^3+16a^2+80a-32,$$

se tiene entonces la igualdad

$$a(6a^4+24a^2+96)^3=A_1^3+A_2^3+A_3^3+A_4^3.$$

Es claro que el factor de a nunca se anula para a racional. Asimismo, los A_i se descomponen en factores no lineales irreducibles. Esto demuestra el teorema (necesariamente sobre $\mathbb{Q}$) el cual, por otro lado, podría ser verificado directamente en vista de la formulación explícita lograda.

Observación:

Habida cuenta del teorema demostrado, se puede demostrar con teoría elemental de curvas elípticas, que esta representación cúbica sobre $\mathbb{Q}$ es entonces posible de una infinidad de maneras distintas. Precisando, si $F(x, y, z, w) = x^3 + y^3 + z^3 + w^3$ entonces, para todo racional a la imagen inversa $F^{-1}(\{a\})$ es un conjunto infinito.

3. Bibliografía

[1] Gómez Sánchez, L. "*Invitación al estudio de la Aritmética de curvas elípticas*". VI Escuela Venezolana de Matemáticas, Centro de Estudios avanzados, IVIC, Caracas, 1993.

[2] Mordell, L. J. "*Diophantine Equations*". Academic Press, New York, 1969.

[3] Samuel, P. "*Théorie Algébrique des Nombres*". Hermann, Paris, 1971.

[4] Serre, J. P. "*Cours d'arithmétique*". Presses Universitaires de France, Paris, 1971.

Luis Gómez Sánchez
Departamento de Matemáticas,
Universidad de Oriente, Venezuela.
lgomez@sucre.udo.edu.ve
lagomez@pucp.edu.pe