Pro Mathematica Vol. XVI, Nos. 31-32, 2002

SOBRE LOS ENTEROS REPRESENTABLES COMO SUMA DE DOS CUBOS DE RACIONALES

Luis ***Gómez-Sánchez A.***

Abstract

A characterization of the natural numbers which are sum of two cubes of rationals is given. It is obtained into the realm of quadratic fields.

Universidad de Oriente, Venezuela.

1 Presentación

Se sabe que en la familia de las curvas de tercer grado, o cúbicas, en $\mathbb{Q}[X,Y]$, tanto las que tienen puntos racionales no triviales como las que carecen de ellos constituyen clases infinitas. Pero no se conoce hasta la fecha ningún criterio efectivo que permita asegurar que una cúbica posee un punto racional [2]. Así por ejemplo, no se sabe si la ecuación $X^3+Y^3=283$ en $\mathbb{Q}$ o, lo que es lo mismo, $X^3+Y^3=283Z^3$ en $\mathbb{Z}$, tiene o no solución distinta de la trivial $(1,-1,0)$. En la ocurrencia, el número 283 es el más pequeño primo congruente con 4 módulo 9 para el que no se sabe responder a esta cuestión. Para todos los primos de esta clase, menores que 283 se ha verificado que sí hay solución lo cual está acorde con una vieja conjetura de Sylvester, aún no demostrada. Esta sostiene que todo primo congruente con 4,7 u 8 módulo 9, es una suma de dos cubos de racionales. En cambio se tiene los dos siguientes resultados.

Teorema 1. *Sea p un número primo impar congruente con 2 ó 5 módulo 9. Entonces $X^3+Y^3=p$ no tiene soluciones racionales.*

Demostración: [4] (algo trabajosa pero elemental) □

Teorema 2. *(P. Satgé) Sea p un número primo impar congruente con 2 ó 5 módulo 9. Entonces, respectivamente, $X^3+Y^3=2p$ y $X^3+Y^3=2p^2$ tienen solución.*

Demostración: [6] (es muy técnica y quien no tenga un bagaje teórico suficiente sobre curvas elípticas, no podrá comprenderla) □

Entonces, por ejemplo, los números 22 y 1058 son suma de dos cubos de racionales, verificar lo cual podría ser "titánico"(o muy fácil, así es la teoría de números). Sin embargo, se demuestra que lo son de una infinidad de maneras distintas (ver más adelante). El teorema 2 es un resultado muy profundo, el primero que se conoce dando una clase infinita (en rigor, dos muy diferenciadas) de enteros sin factor cúbico, representables sobre $\mathbb{Q}$ por la forma cúbica $f(X,Y)=X^3+Y^3$. El próximo teorema caracteriza todos estos números pero los mismos en general están implícitos (como factor) dentro de la clase a que pertenecen

en $\mathbb{Q}^*$ módulo el subgrupo de los cubos, lo cual limita considerablemente su aplicabilidad.

Teorema 3. *Un número entero es una suma de dos cubos de racionales si y sólo si él es de la forma* $ab(a+b)r^3$ *donde* a *y* b *son enteros primos entre sí y* r *es un racional.*

Demostración: [3] □

Ejemplo 1. *El primo* $19 = 3^3 + (-2)^3$ *es obviamente representable. Entonces la ecuación* $19W^3 = XY(X+Y)Z^3$ *tiene soluciones enteras* X, Y, Z, W *con* $W \neq 0$. *Asimismo, substituyendo 19 por 283, debería haber soluciones enteras si se verificase para este último primo la conjetura de Sylvester citada.*

Ejemplo 2. *El número* $3 \times 8(3+8) = 24 \times 11 = 264$ *es entonces representable pero aquí lo que tiene valor teórico es el factor 33, desprovisto de factores cúbicos, y no el 264.*

La caracterización que damos en este artículo, se sitúa no en un grupo cociente sino en extensiones cuadráticas del campo de los racionales.

2 Ley de Grupo en las Curvas $X^3+Y^3 = AZ^3$

Un hecho fundamental sobre las cúbicas elípticas es la ley de grupo conmutativo que produce en las mismas el proceso llamado de "cuerdas y tangentes" según el cual 3 puntos de la cúbica tienen una suma cero si y sólo si los 3 puntos son colineales, es decir están en una misma recta. Notemos V_A la curva, donde A es un entero natural sin factores cúbicos.

Eligiendo como elemento neutro el punto $O = (1, -1, 0)$, (nótese que este punto pertenece trivialmente a toda curva V_A), si $M = (X_1, Y_1, Z_1)$, $N = (X_2, Y_2, Z_2)$ y $M + N = P$ con $P = (X_3, Y_3, Z_3)$ en la curva V_A, entonces el cálculo da para P un triplete de coordenadas homogéneas (es decir, a un factor constante de aproximación):

$$\text{Si } M \neq N \text{ se tiene} \begin{cases} X_3 &= X_1Z_1Y_2^2 - X_2Z_2Y_1^2 \\ Y_3 &= Y_1Z_1X_2^2 - Y_2Z_2X_1^2 \\ Z_3 &= X_1Y_1Z_2^2 - X_2Y_2Z_1^2 \end{cases}$$

$$\text{Si } M = N = (X, Y, Z) \text{ se tiene} \begin{cases} X_3 &= -Y(2X^3 + Y^3) \\ Y_3 &= X(X^3 + 2Y^3) \\ Z_3 &= Z(X^3 - Y^3) \end{cases}$$

Nota.- Estas fórmulas son en sí una manera analítica de definir la ley de grupo conmutativo en V_A, con $(1, -1, 0)$ como elemento neutro. Aparte de la asociatividad, un tanto engorrosa, todo lo demás se verifica con facilidad.

Queda en evidencia un hecho de gran importancia: las fórmulas son racionales. Esto permite definir el grupo $V_A(K)$ que forma la cúbica V_A sobre cualquier campo K, finito o infinito (en $\mathbb{C}$ o en característica $p > 2$). Para A dado, nos interesa el grupo $V_A(\mathbb{Q})$ de la curva V_A sobre los racionales y usamos los grupos $V_A(\mathbb{Q}(\sqrt{m}))$ de V_A sobre ciertos campos cuadráticos $\mathbb{Q}(\sqrt{m})$.

El teorema 1, junto con el famoso teorema de la progresión aritmética de Dirichlet [1] nos asegura que en una infinidad de casos $V_A(\mathbb{Q}) = \{O\}$ donde $O = (1, -1, 0)$. Por otro lado se sabe que, salvo para los valores $A = 1$ y $A = 2$, (en los que $V_A(\mathbb{Q})$ es isomorfo respectivamente a $\frac{\mathbb{Z}}{3\mathbb{Z}}$ y $\frac{\mathbb{Z}}{2\mathbb{Z}}$), si $V_A(\mathbb{Q})$ no se reduce al grupo trivial $\{O\}$, es entonces infinito y sin torsión [3].

3 Los Grupos Cuadráticos $V_A(\mathbb{Q}(\sqrt{m}))$

Necesitamos de cierta terminología. Sea m un entero racional sin factores cuadrados y supongamos que existe un punto no racional

$M = (X, Y, Z)$ en $V_A(\mathbb{Q}(\sqrt{m}))$; se notará $\overline{M}$ al punto $(\overline{X}, \overline{Y}, \overline{Z})$ donde $\overline{X}$ designa la imagen del número cuadrático X por el único automorfismo no trivial del campo $\mathbb{Q}(\sqrt{m})$, es decir, si $X = a + b\sqrt{m}$, donde a y b son racionales, entonces $\overline{X} = a - b\sqrt{m}$. Como para todo Z no nulo en $\mathbb{Q}(\sqrt{m})$ se tiene $(X, Y, Z) = (X\overline{Z}, Y\overline{Z}, Z\overline{Z})$ (porque las coordenadas son homogéneas) y $Z\overline{Z}$ es racional, todo punto cuadrático sobre $\mathbb{Q}(\sqrt{m})$ es equivalente a un punto de la forma $(a_1 + b_1\sqrt{m}, a_2 + b_2\sqrt{m}, c)$ donde sin pérdida de generalidad, a_1, b_1, a_2, b_2 y c pueden considerarse enteros sin factor común. Diremos entonces que el punto cuadrático está bajo su forma reducida o es reducido. Los puntos de la forma $(a + b\sqrt{m}, a - b\sqrt{m}, c)$ serán dichos conjugados. Es fácil ver que si la forma reducida de un punto cuadrático M en $V_A(\mathbb{Q}(\sqrt{m}))$ no es conjugada entonces M no es equivalente a ningún punto conjugado de $V_A(\mathbb{Q}(\sqrt{m}))$.

Ejemplo 3. *El punto* $M = (4 + 2\sqrt{-11}, -1 + \sqrt{-11}, 6)$ *está en* V_2 *y un cálculo sencillo deja ver que* M *no puede ser equivalente a ningún punto conjugado de* V_2 *sobre* $\mathbb{Q}(\sqrt{-11})$.

Lema 1. *Sean una curva* V_A *definida sobre un campo cuadrático* $\mathbb{Q}(\sqrt{m})$ *y* M, N, R *puntos de esta curva.*

a) Si $M + N = R$ *entonces* $\overline{M} + \overline{N} = \overline{R}$

b) $M + \overline{M}$ *es racional, es decir* $M \in V_A(\mathbb{Q}(\sqrt{m}))$ *implica* $M + \overline{M} \in V_A(\mathbb{Q})$.

c) $M + \overline{M} = O$ *si y sólo si* M *es (equivalente a un punto) conjugado.*

Demostración: Sencilla, se deja como ejercicio. □

Lema 2. *Los grupos* $V_A(\mathbb{Q})$ *no tienen ningún punto de torsión de orden 2, salvo para el valor* $A = 2$.

Demostración: Sea $P = (a, b, c)$, con $abc \neq 0$, en $V_A(\mathbb{Q})$, tal que $2P = O$. La ley de grupo en V_A da entonces $a(a^3 + 2b^3) = b(2a^3 + b^3)$ y $c(a^3 - b^3) = 0$ de donde $a = b$ porque $a^2 + ab + b^2$ no puede anularse. Por lo tanto

$2a^3 = Ac^3$ y entonces $A = 2$. Se verifica por otro lado que en V_2 se tiene $(1,1,1) + (1,1,1) = (1,-1,0)$, es decir $2(1,1,1) = O$ □

Proposición 1. *Toda curva V_A tiene puntos conjugados.*

Demostración: En efecto $(a + b\sqrt{M})^3 + (a - b\sqrt{M})^3 = Ac^3$ equivale a $M = \frac{Ac^3 - 2a^3}{6ab^2}$ y para valores enteros arbitrarios no nulos de a, b, c, en general M no es un cuadrado. Entonces V_A tiene un punto cuadrático conjugado sobre $\mathbb{Q}(\sqrt{m})$ donde m es el producto de los factores primos cuyo exponente es impar en la descomposición en factores primos del entero $6a(Ac^3 - 2a^3)$. □

Nota: Se demuestra que si la curva V_A tiene un punto conjugado sobre $\mathbb{Q}(\sqrt{m})$, entonces, salvo cuando $(A, m) \neq (2, -3)$, tiene una infinidad sobre $\mathbb{Q}(\sqrt{m})$ (ver[3]). El problema de saber si V_A no tiene puntos cuadráticos sobre $\mathbb{Q}(\sqrt{m})$ para un m dado, es sumamente difícil (ver[5]).

Ejemplo 4. *La cúbica de Fermat $X^3 + Y^3 = Z^3$ no tiene puntos racionales no triviales pero sí tiene una infinidad de puntos enteros cuadráticos. Uno de éstos es $(243 + 7295\sqrt{29}, 243 - 7295\sqrt{29}, 13104)$ de donde se deduce una infinidad sobre $\mathbb{Q}(\sqrt{29})$.*

4 La Caracterización

Para todo A, la curva V_A tiene 3 puntos al infinito $V_A \cap H_\infty = \{(1,-1,0), (1,-\rho,0), (1,-\overline{\rho},0)\}$ donde ρ es raíz cúbica no real de la unidad. Esto muestra 2 puntos cuadráticos no conjugados que existen en toda ocasión. Son la única excepción (¡trivial!) cuando el único punto racional de V_A es $(1,-1,0)$, es decir, cuando A no es suma de dos cubos de racionales.

Teorema. *Sea la curva V_A definida por $X^3 + Y^3 = AZ^3$ donde A es un entero natural sin factores cúbicos. Entonces $V_A(\mathbb{Q}) = \{O\}$ si y sólo si todo punto cuadrático de V_A sobre $\mathbb{Q}(\sqrt{m})$ con $m \neq -3$ es (equivalente a un punto) conjugado.*

Demostración: Si todos los puntos cuadráticos reducidos son conjugados, entonces $A \neq 2$ por el ejemplo 3. Supongamos que existe un punto racional R en V_A y sea M un punto cuadrático de V_A sobre $\mathbb{Q}(\sqrt{m})$; la suma $S = M + R$ es un punto cuadrático sobre $\mathbb{Q}(\sqrt{m})$ y podemos suponer que es conjugado. Por el lema 1, $S + \overline{S} = O$, es decir $M + R + \overline{M} + \overline{R} = M + \overline{M} + R + \overline{R} = 2R = O$. Entonces, por el lema 2, $R = O$.

Recíprocamente, supóngase que el único punto racional de V_A es $(1, -1, 0)$ y sea M un punto cuadrático de V_A. Por el lema 1, $M + \overline{M}$ es un punto racional de V_A y $M + \overline{M} = O$ por lo cual M es (equivalente a) un punto conjugado de V_A. □

Corolario 1. *Sea $A > 2$ un entero natural sin factores cúbicos. Entonces A es representable como suma de dos cubos de racionales si y sólo si la curva V_A tiene un punto cuadrático (cuyo reducido es) no conjugado sobre algún campo $\mathbb{Q}(\sqrt{m})$ con $m \neq -3$.*

Demostración: Obvia. □

Referencias

[1] APOSTOL, T. M. (1980). *Introducción a la Teoría Analítica de Números.* Reverté S.A., Barcelona.

[2] CASSELS, J.W.S. (1983). *Mordell's finite basis revisited.* Math., Proc. Cambridge Philosophy Society, 100, p.31-41.

[3] GÓMEZ SÁNCHEZ, L. (1993). *Invitación al estudio de la aritmética de curvas elípticas.* VI Escuela Venezolana de Matemáticas, Centro de Estudios Avanzados, IVIC, Caracas.

[4] MORDELL, L. J. (1969). *Diophantine Equations.* Academic Press, New York.

[5] RIBENBOIM, P. (1979). *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York.

[6] SATGÉ PH. (1987). *Quelques résultats sur les entiers qui sont somme des cubes de deux rationnels.* Société Mathématique de France, Asterisque 147-148, p. 335-341.

Luis Gómez-Sánchez
Universidad de Oriente, Venezuela
lagomez@amauta.rcp.net.pe