Ecuaciones diofánticas en enteros gaussianos

Diophantine equations on Gaussian integers

Javier Rodrigo Hitos y Mariló López González

Revista de Investigación

Volumen VII, Número 2, pp. 021–026, ISSN 2174-0410
Recepción: 1 Jun'17; Aceptación: 2 Sep'17

1 de octubre de 2017

Resumen

En este artículo se resuelven en los enteros gaussianos algunas ecuaciones diofánticas conocidas.

Palabras Clave: Teoría de números, ecuaciones diofánticas, enteros gaussianos.

Abstract

In this paper we search for solutions in Gaussian integers to some known Diophantine equations.

Keywords: Number theory, Diophantine equations, Gaussian integers.

1. Introducción

El estudio de las ecuaciones diofánticas es una de las ramas más fructíferas de la Teoría de números. Una ecuación diofántica es una ecuación con coeficientes enteros a la que se buscan soluciones enteras.

Una de las ecuaciones diofánticas más conocida es la ecuación de Fermat: $x^n + y^n = z^n$ (1). Fermat conjeturó que no existen soluciones enteras no triviales a su ecuación si el exponente n es mayor que 2 (para $n = 2$ existen infinitas soluciones enteras, las ternas pitagóricas), conjetura probada por Wiles en 1995 [1].

Se han realizado diversas generalizaciones a la ecuación (1), una de ellas consiste en añadir una variable a la derecha: $x^n + y^n = z^n + u^n$ (2), ecuación que da lugar a números que se pueden expresar como suma de dos potencias n-ésimas de dos formas distintas.

Para $n = 2, 3, 4$ existen soluciones paramétricas a la ecuación (2) que dan lugar a infinitas soluciones enteras de la misma (en el caso $n = 4$ no da lugar a todas las soluciones enteras), en cambio para $n=5$ no se conoce ninguna solución entera no trivial a la ecuación (2) y se conjetura que no hay ninguna [2] (un estudio del número de soluciones en media de la ecuación (2) para $n \geq 4$ se encuentra en [3]

Una generalización de la ecuación (2) es transformarla en sistema:

$$x_1^n + y_1^n = x_2^n + y_2^n = \ldots = x_k^n + y_k^n \text{ (3)}$$

Este sistema da lugar a números enteros que se pueden expresar como suma de dos potencias *n*-ésimas de *k* formas distintas. En el caso $n=4$, $k=3$ no se conocen soluciones enteras no triviales al sistema y se conjetura que no hay ninguna [4].

En este artículo hayamos soluciones a (2): $n=5$ y (3): $n=4$ en un contexto más débil, ya que son soluciones en enteros gaussianos y, en el caso del sistema, añadimos una variable más en cada ecuación: $x_1^4 + y_1^4 + z_1^4 = x_2^4 + y_2^4 + z_2^4 = \ldots = x_k^4 + y_k^4 + z_k^4$ (4).

Los enteros gaussianos son una extensión de los enteros introducida por Gauss como una herramienta para, entre otras cosas, resolver ciertas ecuaciones diofánticas mediante factorización gaussiana. Son los números de la forma $a+b\,i$ donde a,b son enteros, i es la unidad imaginaria. Al tener dos variables: parte real y parte imaginaria, es más factible que una ecuación ó sistema diofántico tenga soluciones en los enteros gaussianos.

Para resolver el sistema (4), resolveremos primero el siguiente sistema diofántico auxiliar:

$$x_1^4 + y_1^4 + z_1^4 = u^4, x_2^4 + y_2^4 + z_2^4 = u^4, \ldots, x_k^4 + y_k^4 + z_k^4 = u^4$$

El caso $k=1$de este sistema es la conocida como ecuación de Euler, que es otra generalización de la ecuación de Fermat de grado 3: Euler conjeturó que, al igual que es imposible expresar un cubo como suma de dos cubos, es imposible expresar una potencia cuarta como suma de tres potencias cuartas.

Elkies refutó esta conjetura en 1988 encontrando una solución entera no trivial a la ecuación de Euler y demostrando que había infinitas soluciones de este tipo [5].

La estructura del artículo es la siguiente: en la sección 2 damos una solución paramétrica en enteros gaussianos a la ecuación (2), en la sección 3 damos algunas soluciones en enteros gaussianos al sistema (4) y en la sección 4 comentamos futuras aplicaciones de los métodos utilizados en las secciones anteriores.

2. La ecuación de grado 5

Para resolver la ecuación (2) para $n=5$, realizamos el siguiente cambio de variable: $x=a\,t+c$, $y=b\,t+d$, $z=b\,t+c$, $u=a\,t+d$. Nótese que los coeficientes de t y los términos independientes forman dos soluciones triviales de (2): (a,b,b,a), (c,d,c,d). Esto hace que al sustituir en (2) y pasar todo a un lado obtengamos un polinomio en t de grado 4 sin término independiente, que tiene la raíz trivial 0 y otra raíz racional: $t=\dfrac{-c-d}{a+b}$ que da lugar a una solución trivial de (2), ya que es de la forma $(x,-x,z,-z)$. El polinomio en t de grado 2 restante tiene como discriminante:

$$(ac+bc+ad+bd)^2 - 4(a^2+b^2)(c^2+d^2) \text{ (5)}$$

Buscamos c para que la expresión de (5) se anule y así las raíces restantes no tengan radicales, lo que da lugar a una nueva ecuación, en c, de grado 2 de discriminante:

$$-a^4d^2 + 2a^3bd^2 - 2a^2b^2d^2 + 2ab^3d^2 - b^4d^2 (6)$$

Observamos que para $d = b$, (6) se transforma en $-2(a-b)^2b^2(a^2+b^2)$.

Entonces si buscamos una solución a la ecuación diofántica de grado 2: $a^2 + b^2 = 2u^2$ (7), tenemos que, para dicha solución, el discriminante es de la forma $-v^2$ con $v \in N$, lo que da lugar a soluciones complejas con coeficientes racionales a la ecuación en c y consecuentemente a raíces complejas con coeficientes racionales del polinomio inicial de grado 2 en t. Sustituyendo en el cambio de variable estos valores hallados, quitando denominadores y factores comunes (puesto que la ecuación (2) es homogénea) y desarrollando en los complejos, obtendremos una solución en enteros gaussianos de (2).

Una solución paramétrica de (7) es $a = -m^2 - 2mn + n^2 + 4mo - 2o^2$, $\mathrm{b} = m^2 - 2mn - n^2 + 4no - 2o^2$, con $m, n, o \in Z$ que lleva a la siguiente solución paramétrica en enteros gaussianos de (2) utilizando el procedimiento expuesto:

$$\{x = m^2 - mn - mo + no + i(-mn - n^2 + mo + 3no - 2o^2),$$
$$y = mn - n^2 - mo + no + i(m^2 + mn - 3mo - no + 2o^2),$$
$$z = m^2 + mn - 3mo - no + 2o^2 + i(mn - n^2 - mo + no),$$
$$u = -mn - n^2 + mo + 3no - 2o^2 + i(m^2 - mn - mo + no)\}$$

Tenemos por tanto el siguiente resultado:

Teorema 1. Existen enteros gaussianos que se pueden expresar como suma de dos potencias quintas de enteros gaussianos de 2 formas distintas.

Observaciones:

1) Las soluciones de (2) cumplen que $z = i\,\bar{y}$, $u = i\,\bar{x}$, donde la barra es conjugación, por lo que el entero gaussiano que puede expresarse como suma de dos potencias quintas de dos formas distintas tiene igual la parte entera que la imaginaria, ya que si lo llamamos $a + b\,i$, cumple que $a + b\,i = z^5 + u^5 = i\left(\bar{x}^5 + \bar{y}^5\right) = i\,(a - b\,i) \Rightarrow a = b$.

Entonces si renombramos $x \to x + y\,i$, $y \to z + u\,i$, tenemos que hemos encontrado incidentalmente una solución paramétrica a la siguiente ecuación diofántica de grado 5:

$$\begin{aligned} &\mathrm{Re}\left((x+y\,i)^5 + (z+u\,i)^5\right) - \mathrm{Im}\left((x+y\,i)^5 + (z+u\,i)^5\right) = \\ &= x^5 - y^5 + z^5 - u^5 + 5\,x\,y^4 + 5\,z\,u^4 - 5\,x^4\,y - 5\,z^4\,u + 10\,x^2\,y^3 + 10\,z^2\,u^3 - 10\,x^3\,y^2 - 10\,z^3\,u^2 = 0 \end{aligned} \quad (8)$$

La solución paramétrica es:

$$\{x = m^2 - mn - mo + no, y = -mn - n^2 + mo + 3no - 2o^2,$$
$$z = mn - n^2 - mo + no, u = m^2 + mn - 3mo - no + 2o^2\}$$

Donde $m, n, o \in Z$

2) La solución de (8) parametriza también la siguiente variedad de dimensión 2 contenida en (8): $\{x - y + z - u = 0, x(y+z) - (y-z)z = 0\}$, lo que nos indica que se puede obtener la siguiente solución más sencilla (dos parámetros) de (8):

$\{x = (p - q)q, y = p(p + q), z = q(p + q), u = p(q - p)\}$, que con la observación 1) da la siguiente solución más sencilla de (2):

$$\{x = (p - q)q + ip(p + q), y = q(p + q) + ip(q - p), z = p(q - p) + iq(p + q),$$

$u = p(p + q) + i(p - q)q\}$, con $p, q \in Z$

Ejemplo

Para valores pequeños de los parámetros en la primera solución: $m=1$, $n=2$, $o=3$, obtenemos la siguiente solución primitiva (sin factores comunes) de (2):

$\{x = 2 - 3i, y = 1 + 6i, z = 6 + i, u = -3 + 2i\}$. Esto da el siguiente entero gaussiano expresable como suma de dos potencias quintas de dos formas distintas:

$$6243 + 6243i = (2 - 3i)^5 + (1 + 6i)^5 = (6 + i)^5 + (-3 + 2i)^5$$

Tenemos entonces la siguiente solución de (8): $\{x = 2, y = -3, z = 1, u = 6\}$, es decir:

$$6243 = Re((2 - 3i)^5 + (1 + 6i)^5) = Im((2 - 3i)^5 + (1 + 6i)^5)$$

3. El sistema de grado 4

Para resolver el sistema auxiliar (ver la introducción), necesitamos el siguiente lema demostrado en [6] y [7] utilizando técnicas similares a las mostradas en la sección 2.

Lema 1

Si (e, f, g, h) es solución de la ecuación diofántica $ix^4 + jy^4 + kz^4 + lu^4 = 0$ (9), entonces también lo es:

$$\{x = e(4e^2f^6g^2h^2j\sqrt{ijkl}(-g^4k + h^4l) + f^4j(g^4k - h^4l)^2(g^4k + h^4l) + g^4h^4kl(g^4k + h^4l)^2 + f^8j^2(g^8k^2 - 6g^4h^4kl + h^8l^2)),$$

$$y = f\left(4e^6f^2g^2h^2i\sqrt{ijkl}(g^4k - h^4l) - 3g^4h^4kl(g^4k + h^4l)^2 + f^4j(g^4k + h^4l)(g^8k^2 - 10g^4h^4kl + h^8l^2) + f^8j^2(g^8k^2 - 6g^4h^4kl + h^8l^2)\right),$$

$$z = g\left(-8e^2f^6g^2h^6jl\sqrt{ijkl} - 4e^2f^2g^2h^6l\sqrt{ijkl}(g^4k + h^4l) + g^4h^4kl(g^4k + h^4l)^2 + f^8j^2(g^8k^2 + 6g^4h^4kl - 3h^8l^2) + f^4j(g^4k + h^4l)(g^8k^2 + 6g^4h^4kl - 3h^8l^2)\right),$$

$$u = h(8e^2f^6g^6h^2jk\sqrt{ijkl} + 4e^2f^2g^6h^2k\sqrt{ijkl}(g^4k + h^4l) + g^4h^4kl(g^4k + h^4l)^2 - f^4j(g^4k + h^4l)(3g^8k^2 - 6g^4h^4kl - h^8l^2) + f^8j^2(-3g^8k^2 + 6g^4h^4kl + h^8l^2))\}$$

Observación: Entonces si los coeficientes enteros i, j, k, l cumplen que $ijkl = -v^2$ con $v \in N$, la solución del lema 1 da soluciones en enteros gaussianos a (9) (si $ijkl$ es un cuadrado perfecto, las soluciones serían enteras).

Vemos ya el procedimiento. Partimos de la solución más pequeña a la ecuación de Euler, encontrada por Roger Frye en 1988 [8]: $95800^4 + 217519^4 + 414560^4 = 422481^4$. Observamos que si multiplicamos a los dos lados por p^4 se sigue cumpliendo la igualdad:

$p^4\, 95800^4 + p^4\, 217519^4 + p^4\, 414560^4 = p^4\, 422481^4$, lo que da la solución:

$$x_1 = p\,95800, y_1 = p\,217519, z_1 = p\,414560, u = p\,422481.$$

Buscamos ahora x_2, y_2, z_2 tales que:

$$x_2^4 + y_2^4 + z_2^4 = p^4\, 422481^4 \Leftrightarrow x_2^4 + y_2^4 + z_2^4 + \left(-422481^4\right)p^4 = 0 \text{ (10).}$$

Pero esta es una ecuación del tipo (9) con $i = j = k = 1,\ l = -422481^4$, que cumplen la condición $i\,j\,k\,l = -v^2$, luego iterando con la solución:

$e = 95800,\ f = 217519,\ g = 414560,\ h = 1$, llegamos a una solución en enteros gaussianos de la ecuación por el lema 1 y su observación. Quitando los factores comunes de las componentes de la solución y multiplicando por el conjugado de la cuarta componente de la solución para que p sea entero (se puede porque la ecuación (10) es homogénea), llegamos a la siguiente solución de (10):

$$\{x2 = -2326746014065867069523285098922572139856788163057190335890658594 00 - 544274656369015465903981796172592217073718058241135926657539200 00i,$$

$$y2 = 160715108449256615936096471585923721160932470224641226789547723839 + 133334060596430610523805040969864244087461173066138974162944000000i,$$

$$z2 = 353747746544407098790044432971214401466700318746100833334646331360 - 185889664785802851899294266493199271430764318412331226436482560 00i,$$

$$p = 8365892513642210861853807592644146186114619725320935054792 81\}$$

Sustituyendo el valor de p obtenido en x_1, y_1, z_1, u, completamos la solución del sistema auxiliar, lo que lleva a una solución del sistema (4) para $k = 2$.

Esto da un entero (una potencia cuarta) que se puede expresar como suma de tres potencias cuartas de enteros gaussianos de dos formas distintas (una de ellas con enteros).

Observación: Se puede iterar el procedimiento partiendo esta vez de la solución x_2, y_2, z_2, u (si partimos de x_1, y_1, z_1, u obtenemos $p = 1$ y la solución sería la misma) para encontrar una solución del sistema (4) para $k = 3$. El nuevo p con el que multiplicamos las soluciones anteriores sería:

$$p = 810241954754962931444186919515309607152424292755115316715919909575522747547649529426004692$$
$$316963634413675833173194195280765398600290260705568806350726731081534826031362234310140026 1$$
$$815450721951415557896312277117042798643685884426094944756468775815484757584877926219088184$$
$$273254924436123837280292632104511005226431127566362035014305632623611863690551292329761405 6$$
$$706013601132136192325817554107649461607976846963613837759077363246666207625968409603949421 9$$
$$802699327335417714063188059467346078141521832377691123971413812947557737101584430337 69$$

Hemos obtenido por tanto el siguiente resultado:

Teorema 2. Existe un entero que se puede expresar como suma de tres potencias cuartas de enteros gaussianos de tres formas distintas

4. Líneas futuras de investigación

La continuación natural a este trabajo sería encontrar soluciones no trivialesen enteros a la ecuación (2) para $n=5$ y al sistema (3) para $n=4$. Sin embargo estas líneas de trabajo son demasiado ambiciosas, ya que, como se comentó en la introducción, son problemas abiertos para los que además se sabe que no hay soluciones pequeñas, como se ha comprobado computacionalmente [8].

Una línea futura de investigación más asequible sería encontrar soluciones a (3) en enteros gaussianos y, en el caso de la ecuación (8) para la que sí se han encontrado soluciones enteras, ver si la solución paramétrica hallada es completa o si, por el contrario, existen soluciones extra a dicha ecuación.

Referencias

[1] WILES, A. *Modular Elliptic-Curves and Fermat's Last Theorem*. Ann. Math.141, 443-551, 1995.

[2] HARDY, G. H. AND WRIGHT, E. M. *An Introduction to the Theory of Numbers*, 5th ed. Oxford, England: Clarendon Press, 1979.

[3] BROWNING, HEATH-BROWN, *Plane curves in boxes and equal sums of two powers*, Math. Zeit. 251, 233–247, 2005.

[4] DICKSON, L.E.*Theory of Numbers*, Vol II. AMA Chelsea Publishing, USA, 1992.

[5] ELKIES, N.*On* $A^4 + B^4 + C^4 = D^4$. Mathematics of Computation. 51 (184): 825–835, 1988.

[6] LOGAN,A., MCKINNON, D., VANLUIJK, R. *Density of Rational Pointson Diagonal Quartic Surfaces*. Algebra NumberTheory, 4(1):1–20, 2010

[7] RODRIGO, J. *Utilización del programa Mathematica para la resolución de ecuaciones diofánticas de cuarto grado,* Actas del 3cm (Tercer congreso de Mathematica en España): 477, 2009.

[8] GUY, R. K. *Sums of LikePowers. Euler's Conjecture*, in Unsolved Problems in Number Theory, 2nd ed.New York: Springer-Verlag, pp. 139-144, 1994.

Agradecimientos

This work has been partially supported by FEDER and the State Research Agency (AEI) of the Spanish Ministry of Economy and Competition under grant TIN2016-76843-C4-2-R (AEI/FEDER, UE).

Sobre los autores:

Nombre: Javier Rodrigo
Correo Electrónico: jrodrigo@comillas.edu
Institución: Universidad Pontificia Comillas, España.

Nombre: Mª Dolores López
Correo Electrónico: marilo.lopez@upm.es
Institución: Universidad Politécnica de Madrid, España.