M. Mercedes Sánchez Benito

Notas históricas relacionadas con la descomposición de un número como suma de dos cuadrados.

La Aritmética de Diofanto es una colección de 189 problemas, cada uno de ellos admite una o más soluciones en números racionales; en ocasiones, la solución incluye la condición que tienen que cumplir los datos para que el problema tenga solución y aparece por primera vez un resultado general: **ningún número primo de la forma *4n+3* puede escribirse como suma de dos cuadrados**.

Vamos a documentar esta afirmación.

En el libro II de la Aritmética encontramos el siguiente problema:

II-8: Descomponer un cuadrado dado en dos cuadrados

Es decir, dado a, encontrar x, y tales que $x^2 + y^2 = a^2$

Solución de Diofanto

Supongamos que queremos descomponer 16 como suma de dos cuadrados. Sea $x = \alpha$, entonces $y = m\alpha - 4$, m es un entero positivo arbitrario y 4 es la raíz de 16; en particular $m = 2$, por lo tanto $y = 2\alpha - 4$. Entonces se debe verificar que $16 = \alpha^2 + (2\alpha - 4)^2$, de aquí obtenemos que $\alpha = \frac{16}{5}$, con lo que

$$16 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2$$

En el *Codex Matritensis 48*, que es el más antiguo de los textos griegos de Diofanto, una segunda mano escribió esta nota:

“Que tu alma, Diofanto, sea con Satanás por la dificultad de los otros teoremas y sobre todo por la de éste”.

Bachet de Mézirac obtiene la solución general; si $a > 0$, $m > n$,

$$x = \frac{2mna}{m^2 + n^2} \qquad y = \frac{(m^2 - n^2)a}{m^2 + n^2}$$

y la presenta así: Para descomponer a^2 en suma de dos cuadrados, se descompone $a = u + v$ siendo $u = m^2\lambda$ y $v = n^2\lambda$, $m \neq n$ siempre posible en números racionales; entonces los números

$x=|u-v|$ e $y=2\sqrt{uv}$ son los números que verifican dicha descomposición. Por ejemplo, de $7=1\cdot\frac{7}{5}+4\cdot\frac{7}{5}$ resulta:

$$7^2=\left(\frac{21}{5}\right)^2+\left(\frac{28}{5}\right)^2$$

Así podemos tener todas las descomposiciones posibles de un cuadrado entero en suma de dos cuadrados enteros.

Es decir, para a, x, y enteros positivos, se tiene:

$a^2=x^2+y^2 \Leftrightarrow a=u+v$, $x=|u-v|$, $y=2\sqrt{uv}$, donde $u=m^2\lambda$, $v=n^2\lambda$, m, n, λ también enteros positivos.

Por ejemplo, $65=1+64=13+52=16+49=20+45$

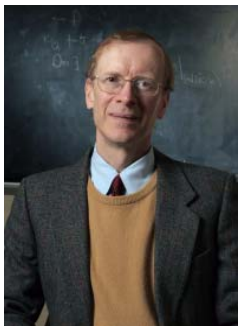
A partir de aquí se encuentran las cuatro descomposiciones en suma de dos cuadrados:

$$65^2=63^2+16^2=39^2+52^2=33^2+56^2=25^2+60^2.$$

Fermat escribió al lado de este problema el comentario más famoso de la historia de las matemáticas:

Por el contrario, no se puede dividir un cubo en dos cubos, ni un bicuadrado en dos bicuadrados, ni en general una potencia superior al cuadrado, hasta el infinito, en dos potencias del mismo grado: he encontrado una demostración verdaderamente admirable de esta afirmación. La exigüidad del margen no podría contenerla.

Esta cuestión, conocida como "el último teorema de Fermat", ha mantenido en vilo a los matemáticos durante más de tres siglos, hasta que en 1995 **Andrew Wiles** encontró una demostración.



Es bien conocido que la ecuación $x^2+y^2=z^2$ tiene soluciones enteras:

$x=2\lambda pq$, $y=\lambda(p^2-q^2)$, $z=\lambda(p^2+q^2)$ donde λ es un entero arbitrario y p, q $(p>q)$ son enteros positivos primos entre si y de distinta paridad, las llamadas ternas pitagóricas. En particular, no para cualquier z admite soluciones enteras positivas.

En este mismo libro, Diofanto plantea el siguiente problema: dado un número que es suma de dos cuadrados, descomponerlo en otros dos cuadrados. Es decir, si $a = b^2 + c^2$, encontrar x, y tales que $a = x^2 + y^2$

Solución de Diofanto

Sea $a = 13 = 4 + 9$, pongamos que $x = \alpha + 2$ y que $y = m\alpha - 3$ con m arbitrario, por ejemplo $y = 2\alpha - 3$, entonces:

$x^2 + y^2 = 5\alpha^2 + 13 - 8\alpha = 13$, de donde $\alpha = \frac{8}{5}$ y por lo tanto $x = \frac{18}{5}$, $y = \frac{1}{5}$; y obviamente $\frac{324}{25} + \frac{1}{25} = \frac{325}{25} = 13$

Hay que esperar hasta **Euler** para encontrar el siguiente análisis :

Si se buscan x, y racionales tales que $x^2 + y^2 = a^2 + b^2$, póngase, con n, m racionales arbitrarios, $x = b + n\alpha$, $y = c - m\alpha$ lo que proporciona la siguiente igualdad: $(n^2 + m^2)\alpha^2 = 2(mc - nb)\alpha$, resultando $\alpha = \frac{2(mc - nb)}{n^2 + m^2}$

Vieta resuelve este problema del siguiente modo: Basta construir dos triángulos rectángulos semejantes, de lados racionales, de hipotenusas b y c, a saber (x_1, y_1, b) y (x_2, y_2, c). Entonces $x_1 + y_2$ e $y_1 - x_2$, o bien $x_1 - y_2$ e $y_1 + x_2$ son la solución.

V-9: Descomponer la unidad en dos partes de modo que al añadir a cada una de ellas un mismo número dado se forme un cuadrado

Es decir, dado a, encontrar x, y tales que

$$x + y = 1, \quad x + a = \square, \quad y + a = \square$$

Es necesario que el número dado a no sea impar, y que $2a + 1$ no sea divisible por un número primo de la forma $4n - 1$.

(condiciones necesarias para que $2a+1$ sea la suma de dos cuadrados. Si $2a+1$ es la suma de dos cuadrados, uno debe ser par y otro impar, y esta suma es congruente con 1 módulo 4, luego $2a+1$ debe ser congruente con 1 módulo 4, y por lo tanto a debe ser par. Y como consecuencia si tenemos un número de la forma $4a+3$, nunca podremos descomponerlo como suma de dos cuadrados)

$$x+y=1,\quad x+a=\square,\quad y+a=\blacksquare$$

Solución de Diofanto

Sea $a=6$. Hay que descomponer el número $2a+1=13$ en dos cuadrados mayores que 6, o bien en dos cuadrados cuya diferencia sea menor que 1. Busquemos en primer lugar una fracción cuadrática como $\frac{1}{4\alpha^2}$ que añadida a $\frac{13}{2}$, la mitad de 13, forme un cuadrado. Debe verificarse que $26\alpha^2+1$ sea un cuadrado. Identificando $26\alpha^2+1\equiv(5\alpha+1)^2$ resulta $\alpha=10$ y $\frac{13}{2}+\frac{1}{400}=\left(\frac{51}{20}\right)^2$

Ahora vamos a descomponer 13 en suma de dos cuadrados de este modo:

Como $13=2^2+3^2$ consideramos $\frac{51}{20}=2+\frac{11}{20}$ y $\frac{51}{20}=3-\frac{9}{20}$

Identifiquemos

Un cuadrado = $(2+11\beta)^2$ y el otro cuadrado = $(3-9\beta)^2$, entonces:

$$13=(2+11\beta)^2+(3-9\beta)^2=202\beta^2-10\beta+13,$$

de donde se tiene que $\beta=\frac{5}{501}$ y consecuentemente $x=\frac{4843}{10201}$, $y=\frac{5358}{10201}$

- Bachet prueba que si $2a+1$ es suma de dos cuadrados, entonces a es par. Y afirma lo siguiente: “pensé que Diofanto quería decir que $2a+1$, (a par) fuera un número primo, ya que los primos de la forma $4n+1$ como 5, 13, 17, 29, 41, etc se componen de dos cuadrados. Pero tampoco se sostiene esta lectura: quedarían excluidos los a tales que $2a+1$ fuera un cuadrado, muy aptos para resolver el problema como en II-8; y por otro lado los a como 22, 58, 62 e infinitos otros, tales que $2a+1$ se descompone en suma de dos cuadrados aun teniendo varios divisores primos: $45=36+9$, $117=81+36$, $125=100+25$. Acójase la condición en la forma que le hemos dado hasta que alguien restituya el pensamiento de Diofanto a partir de un códice mejor restaurado”

Observaciones de Fermat

- En la primera observación da una respuesta rápida a la duda de Bachet sobre si un número como 21, que no es ni cuadrado ni suma de dos cuadrados enteros, podría ser suma de dos números racionales: El número 21 no se puede descomponer en suma de dos cuadrados fraccionarios. Lo puedo demostrar muy fácilmente; con mayor generalidad, ningún número divisible por 3 pero no por 9 puede ser suma de dos cuadrados, ni enteros ni fraccionarios.
  La primera demostración de que si un número no es suma de dos cuadrados enteros, tampoco es suma de dos cuadrados racionales, asunto infructuosamente tratado por Fermat y por Euler parece ser que la dio L. Aubry en 1912
- En la segunda, en relación con el tratamiento aproximativo que da Bachet a la segunda condición del problema sobre el número dado a, Fermat reescribe una condición necesaria para que un número entero sea representable como suma de dos cuadrados que ya había comunicado a Roberval en 1640:
  Es necesario que el número dado a no sea impar, y que $2a+1$, después de dividirle por el mayor cuadrado que contenga como factor, no se pueda dividir por un número primo de la forma $4n-1$.

La condición de Fermat también es suficiente. La demostración de la suficiencia, que es la parte más dfícil, se reduce a probar que todo primo de la forma $4n+1$ es suma de dos cuadrados. Fermat anunciaba ya este resultado, añadiendo además que en este caso la representación es única, en una carta de 1640 a Mersenne. Pero no dejó escrita la demostración. El primero en hacerlo fue Euler. La demostración de Euler se sirve de una técnica indirecto de descenso, es muy “fermatiana”.