DIFERENCIAS DE CUADRADOS

ANTONIO M. OLLER MARCÉN

1. Introducción

Un problema clásico de la teoría de números, y que aún hoy se sigue presentando en cualquier curso elemental sobre la materia, es el de estudiar la posibilidad de descomponer un entero como suma de dos cuadrados. Esta cuestión, que parece remontarse a Diofanto, atrajo la atención de múltiples matemáticos a lo largo de la historia. El primero en dar las indicaciones para una resolución del problema fue Fermat aunque, como otras muchas veces, no llegó a concretar sus ideas por escrito. El primero en probar el resultado fue Lagrange, y su demostración fue posteriormente simplificada por Euler.

Puede probarse que un entero n es suma de dos cuadrados si y sólo si todos los factores primos de n de la forma $4m+3$ aparecen con exponente par en la descomposición de n como producto de potencias de primos. En [2] (Capítulo 20) se dan hasta cuatro demostraciones de este resultado. De hecho puede obtenerse una fórmula que proporciona el número de soluciones para cada n dado (ver por ejemplo [1] Capítulo 2, §4, Teorema 3).

En este pequeño artículo estudiaremos una cuestión similar: la de enteros representables, no como suma, sino como diferencia de dos cuadrados. En la segunda sección damos la caracterización de tales enteros, en la tercera se estudian algunas descomposiciones concretas. En la siguiente se presentan fórmulas explícitas que proporcionen el número de representaciones distintas y se dan aplicaciones a ciertos casos particulares. La quinta y sexta secciones son de carácter mucho más geométrico y relacionan la posibilidad de representar un entero como diferencia de cuadrados de dos formas distintas con las ternas pitagóricas y con los triángulos rectángulos de lados y alturas enteras. Finalmente la última sección es una curiosidad sobre una cierta regularidad en las representaciones de ciertos enteros como diferencia de cuadrados. Los resultados principales de las secciones 2 y 4 pueden encontrarse, aunque enunciados de una manera ligeramente distinta, en [3] (Capítulo 6, §2).

2. Caracterización de los números que son diferencia de cuadrados

Por su sencillez comenzaremos presentando directamente la caracterización de aquellos enteros representables como diferencia de cuadrados.

Proposición 1. *Un entero puede ser representado como diferencia de cuadrados si y sólo si es impar o múltiplo de* 4.

Demostración: Supongamos que un entero n es diferencia de cuadrados. En tal caso $n = x^2 - y^2 = (x+y)(x-y)$ y se concluye que n posee una factorización tal que ambos factores son de igual paridad. Si dichos factores son impares el número n es impar y si ambos son pares n es múltiplo de 4.

Recíprocamente, si n es impar o múltiplo de 4, está claro que existe una factorización de tipo $n = ab$ con a y b de igual paridad. Si tomamos $x = \frac{a+b}{2}$ e $y = \frac{a-b}{2}$ se tiene que $n = x^2 - y^2$. □

Como consecuencia de la proposición anterior obtenemos que todo primo impar es representable como diferencia de cuadrados; contrariamente a lo que sucede en el caso de la suma de dos cuadrados, donde debe exigirse que $p \equiv 1 \pmod 4$. No obstante podríamos haber observado esto inicialmente y haber razonado a partir de allí haciendo uso de las identidades:

$$(a^2 - b^2)(c^2 - d^2) = (ac + bd)^2 - (ad + bc)^2 = (ac - bd)^2 - (ad - bc)^2$$

Es interesante observar que si $n = 4$ la única forma de representarlo como diferencia de cuadrados es como $4 = 2^2 - 0^2$ (diremos que esta es la *representación trivial* de 4 como diferencia de cuadrados, notar que sólo los cuadrados perfectos admiten representación trivial). De hecho el 1 y el 4 son los únicos enteros que sólo admiten la representación trivial, por ello podemos dar la siguiente versión geométrica de nuestro resultado anterior

Corolario 1. *Si $n > 2$ es un entero cualquiera, entonces siempre existe un triángulo rectángulo de lados enteros tal que n es la medida de uno de sus catetos.*

Observar que, sin embargo, el resultado anterior es falso para el caso de la hipotenusa. Es decir, existen (infinitos) enteros tales que no son la hipotenusa de ningún triángulo rectángulo de lados enteros. Por ejemplo no existen triángulos rectángulos de lados enteros cuya hipotenusa valga 7, esto se debe a que la única forma de representar 49 como suma de cuadrados es $49 = 7^2 + 0^2$.

3. Algunos casos particulares

Esta sección estará dedicada a presentar algunos resultados particulares sobre representaciones concretas de un entero como diferencia de cuadrados. Esto servirá, en parte, como introducción a la sección siguiente. Como hemos visto que un entero podía descomponerse como diferencia de cuadrados si y sólo si es impar o múltiplo de 4, parece bastante claro que en lo sucesivo vayamos distinguiendo ambos casos.

Para los enteros impares existe una representación como diferencia de cuadrados que, además, cumple una propiedad interesante.

Proposición 2. *Si $n \geq 1$ es un entero impar, existen x e y enteros tales que $x^2 - y^2 = n$ y además $x + y = n$.*

Demostración: Basta escribir $n = 2b + 1$ con $b \geq 0$ y observar que se cumple que $(b + 1)^2 - b^2 = n$. □

En el caso de los múltiplos de 4 tenemos un resultado similar.

Proposición 3. *Si $n \geq 4$ es un múltiplo de 4, existen x e y enteros tales que $x^2 - y^2 = n$ y además $x + y = \frac{n}{2}$.*

Demostración: Ponemos $n = 2 \cdot 2b$ con $b \geq 1$. Entonces basta con observar que $(b + 1)^2 - (b - 1)^2 = n$. □

De hecho estos resultados se pueden expresar de una forma algo más general:

Proposición 4. *Dado $n \geq 1$ impar y $k > 0$ cualquiera, entonces para todo natural $1 \leq h \leq k$ existen enteros x e y tales que $x^2 - y^2 = n^k$ y que $x + y = n^h$.*

Demostración: Es suficiente con comprobar que para todo $1 \leq h \leq k$ se tiene que:

$$\left(\frac{n^h + n^{k-h}}{2}\right)^2 - \left(\frac{n^h - n^{k-h}}{2}\right)^2 = n^k$$

□

Proposición 5. *Dado $n \geq 4$ múltiplo de 4 y $k > 0$ cualquiera, entonces para todo $1 \leq h \leq k$ existen enteros x e y tales que $x^2 - y^2 = n^k$ y además $x + y = \frac{n^k}{2^h}$.*

Demostración: Ponemos $n = 2 \cdot 2b$ y para cada $1 \leq h \leq k$ se tiene que:

$$\left(\frac{2^{2k-h}b^k + 2^h}{2}\right)^2 - \left(\frac{2^{2k-h}b^k - 2^h}{2}\right)^2 = n^k$$

□

Obsérvese que en las proposiciones precedentes se admiten valores negativos para y. Más adelante, sin embargo, cuando tratemos aspectos geométricos nos veremos obligados a rechazar tal posibilidad.

4. Contando diferencias de cuadrados

En las secciones anteriores hemos caracterizado los enteros representables como diferencia de cuadrados. Además hemos dado algunos ejemplos que nos daban distintas representaciones en algunos casos particulares. En esta sección pretendemos contar de manera exacta las distintas maneras de representar un entero dado como diferencia de cuadrados.

Como se desprende del razonamiento seguido en la demostración de la Proposición 1 existe una fuerte relación entre el número de divisores de un entero y la manera de representarlo como diferencia de cuadrados. De hecho, para cada posible factorización del entero en factores de igual paridad, obtenemos una descomposición del mismo como diferencia de cuadrados.

Antes de comenzar veremos la definición de una importante función aritmética. Denotaremos por $\tau : \mathbb{Z} \longrightarrow \mathbb{N}$ a la función que asigna a cada entero n el número de sus divisores. La propiedad más importante de esta función es que es *multiplicativa*; esto quiere decir que si m y n son enteros coprimos entonces $\tau(mn) = \tau(m)\tau(n)$. Gracias a esta última propiedad podemos dar una expresión para $\tau(n)$ si se conoce una descomposición de n es factores primos. De hecho si $n = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$ entonces $\tau(n) = (e_1+1)(e_2+1)\dots(e_r+1)$. Algunas propiedades que se deducen fácilmente de lo anterior:

- $\tau(n) = 2$ si y sólo si n es primo.
- $\tau(n)$ es impar si y sólo si n es un cuadrado perfecto.

De manera similar denotaremos por $\iota : \mathbb{Z} \longrightarrow \mathbb{N}$ a la función aritmética que asigna a cada entero n el número de sus divisores impares. Es obvio que ι es también una función multiplicativa, que n es impar si y sólo si $\tau(n) = \iota(n)$ y que tenemos para ι una expresión similar a la de τ en función de los exponentes de los primos en una factorización de n. De hecho, si $n = 2^e p_2^{e_2}\dots p_r^{e_r}$, entonces $\iota(n) = \tau\left(\frac{n}{2^e}\right) = \tau(p_2^{e_2}\dots p_r^{e_r})$.

Con estas consideraciones ya podemos presentar los dos resultados principales de esta sección.

Proposición 6. *Sea n es un entero impar. Si n no es un cuadrado perfecto, puede representarse como diferencia de cuadrados de $\frac{\tau(n)}{2}$ formas distintas. Si n es cuadrado perfecto, entonces el número de representaciones diferentes es $\frac{\tau(n)+1}{2}$.*

Demostración: Como hemos indicado antes, para cada factorización de n obtenemos una representación distinta como diferencia de dos cuadrados. Para cada divisor poseemos una factorización, pero cada de una de ellas aparece dos veces (siempre que n no sea un cuadrado, en cuyo caso una de las factorizaciones no está repetida). De esta observación se deduce trivialmente el resultado. □

Proposición 7. *Sea n es un entero múltiplo de 4. Si n no es un cuadrado perfecto, puede representarse como diferencia de cuadrados de $\frac{\tau(n)}{2} - \iota(n)$ formas distintas. Si n es un cuadrado perfecto, entonces el número de representaciones diferentes es $\frac{\tau(n)+1}{2} - \iota(n)$.*

Demostración: De manera análoga al caso anterior, si n no es un cuadrado perfecto, podemos factorizarlo de $\tau(n)$ formas. Cada una de ellas aparece repetida dos veces, por lo que tenemos $\tau(n)$ factorizaciones diferentes. Sin embargo, hemos de excluir aquellas que estén formadas por factores de distinta paridad. Por el hecho de ser n múltiplo de 4 se tiene que cada divisor impar induce una de estas factorizaciones no deseadas. De estas consideraciones se sigue el resultado. Para el caso en que n sea un cuadrado perfecto sólo hay que tener en cuenta el hecho de que una de las factorizaciones no está repetida. □

Nota. En los resultados anteriores se han considerado únicamente soluciones con $x, y \geq 0$, pero es claro que si (x, y) es una solución también lo son $(\pm x, \pm y)$. Nosotros descartaremos en lo que sigue estas soluciones por no considerarlas esencialmente distintas.

Anteriormente se ha mencionado que si $n = 4$ el único modo (salvo el signo) de representarlo como diferencia de cuadrados era el trivial $4 = 2^2 - 0^2$ y que los únicos casos en los que esto sucedía eran $n = 1$ y $n = 4$. Sin embargo sí hay más enteros que admiten una única representación como diferencia de cuadrados. El resultado siguiente los caracteriza:

Corolario 2. *Sea n un entero positivo. Entonces n se representa como diferencia de cuadrados de manera única si y sólo si $n = 1$, 4, 8, p ó $4p$ siendo p un primo impar.*

Demostración: Si n es de una de las formas del enunciado basta obtener todos sus divisores y aplicar las proposiciones anteriores para ver que existe una única representación como diferencia de cuadrados.

Recíprocamente, supongamos que n admite una única representación como diferencia de cuadrados y analicemos los distintos casos:

- Si n es impar no cuadrado perfecto, entonces debe ser $\frac{\tau(n)}{2} = 1$, luego $\tau(n) = 2$ y como se indicó tras la definición de la función τ, n debe ser primo.
- Si n es impar cuadrado perfecto se sigue análogamente que $\tau(n) = 1$, luego que $n = 1$.
- Si n es múltiplo de 4 no cuadrado perfecto debe ser $\frac{\tau(n)}{2} - \iota(n) = 1$. Si ponemos $n = 2^a b$ con b impar se tiene que que $\tau(n) = (a + 1)\tau(b)$ y que $\iota(n) = \iota(b) = \tau(b)$. Sustituyendo en lo anterior se sigue que $a = 3$ y $b = 1$ (y por tanto que n=8) o bien que $a = 2$ y que b es primo.
- Finalmente, si n es múltiplo de 4 y cuadrado perfecto, se tiene por hipótesis que $\frac{\tau(n)+1}{2} - \iota(n) = 1$. Poniendo $n = 2^{2a} b^2$ con $b > 1$ impar y razonando como en caso anterior se llega a que $a = 1 = b$ y por lo tanto que $n = 4$.

□

Siguiendo esta misma idea podemos caracterizar los enteros que pueden descomponerse como diferencia de cuadrados de exactamente dos formas distintas. Así, lo que se tiene es:

Corolario 3. *Dado un entero n, éste puede representarse como diferencia de cuadrados exactamente de dos maneras si y sólo si $n = 16$, 32, $8p$, p^2, $4p^2$, p^3, $4p^3$, pq ó $4pq$ con p y q primos impares.*

Demostración: Es completamente análoga a la del corolario anterior. □

Nota. Está claro que empleando las mismas técnicas que en los dos corolarios anteriores pueden caracterizarse los enteros representables como diferencia de cuadrados de exactamente k formas para cada k dado.

Además, podemos refinar el corolario anterior para caracterizar aquellos enteros que admiten una única representación no trivial como diferencia de cuadrados. Obtenemos así la siguiente proposición.

Proposición 8. *Dado un entero n, éste puede representarse de una única manera no trivial como diferencia de cuadrados si y sólo si $n = 8$, 16, p, $4p$, p^2 ó $4p^2$ con p un primo impar.*

Demostración: Es una consecuencia directa de los corolarios anteriores y de la observación de que un cuadrado perfecto siempre admite la representación trivial como diferencia de cuadrados. □

Finalmente podemos reinterpretar el resultado anterior en términos más geométricos:

Corolario 4. *Si $n = 4$, p ó $2p$ con p un primo impar, entonces existe un único triángulo rectángulo de manera que uno de sus catetos mide n.*

Como ejemplo de aplicación del corolario anterior podemos presentar el siguiente resultado:

Proposición 9. *Dado p un primo impar, existe un único triángulo de lados enteros de manera que una de sus alturas mida p. Además este triángulo es isósceles y p es la medida de la altura sobre el lado desigual.*

Demostración: Consideremos un triángulo como el mostrado en la Figura 1 en el que $a, b, c = c_1 + c_2 \in \mathbb{Z}$. En primer lugar observamos que, al ser p una altura se cumple que $c_1^2 = a^2 - p^2 \in \mathbb{Z}$. Por otro lado se tiene que $\dfrac{c_1}{a} = \cos\alpha$ y por el Teorema del Coseno se tiene $\cos\alpha = \dfrac{a^2 + c^2 - b^2}{2ac} \in \mathbb{Q}$. Así pues $c_1 \in \mathbb{Q}$ y debe cumplirse que $c_1 \in \mathbb{Z}$. De igual modo se tiene que $c_2 \in \mathbb{Z}$. Es decir, tenemos que p es el cateto de

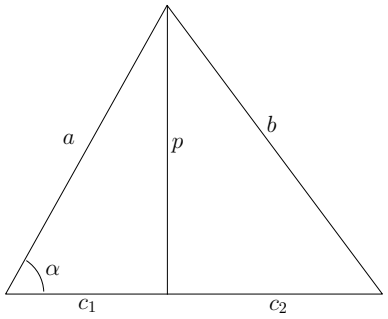

FIGURA 1. Triángulo de lados enteros y altura un primo p.

los triángulos rectángulos de lados enteros (a, p, c_1) y (b, p, c_2). Sin embargo hemos visto que p sólo puede tenerse como cateto de un único triángulo rectángulo. De aquí se deduce que $a = b$ y que $c_1 = c_2$ y por tanto el resultado. □

5. Diferencias de cuadrados y ternas pitagóricas

Comenzaremos recordando que una terna pitagórica es un triple de enteros (x, y, z) tales que $x^2 + y^2 = z^2$. Es decir, tales que el triángulo de lados x, y y z es rectángulo. Una terna pitagórica se dice primitiva si x, y y z son coprimos. Denotaremos mediante $\mathcal{T}$ el conjunto de todas las ternas pitagóricas primitivas; es decir:

$$\mathcal{T} = \{(x, y, z) \in (\mathbb{Z})^3 \mid x^2 + y^2 = z^2,\ \text{m.c.d.}(x, y, z) = 1\}.$$

Ya hemos demostrado que todo entero $n > 2$ puede verse como el cateto de un triángulo rectángulo de lados enteros y que además esto puede hacerse en general de más de una manera. Supongamos que tenemos pues dos de tales triángulos. Entonces podemos pegarlos por su lado común para obtener un nuevo triángulo cuya altura será el entero n de partida (ver Figura 2). En tal caso tenemos que $a^2 - b^2 = n^2 = c^2 - d^2$, en particular, estaremos interesados en la situación en la que el nuevo triángulo es también rectángulo; es decir, cuando $a^2 + c^2 = (b + d)^2$. Observar que entonces los triángulos de partida eran semejantes y que el triángulo rectángulo obtenido tiene lados y alturas enteros. En lo que sigue denotaremos la situación recién descrita mediante una 5-tupla de enteros (a, b, n, c, d) y llamaremos $\mathcal{Q}$ al siguiente conjunto:

$$\mathcal{Q} = \{(a, b, n, c, d) \in (\mathbb{Z})^5 \mid a^2 - b^2 = n^2 = c^2 - d^2,\ a^2 + c^2 = (b+d)^2,\ \text{m.c.d}(b, d) = 1\}.$$

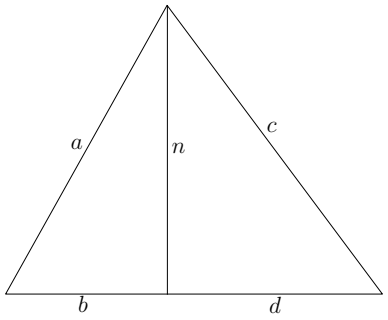

FIGURA 2. Un entero n como cateto de dos triángulos rectángulos distintos.

Tomemos $(x, y, z) \in \mathcal{T}$ y llamemos $b = x^2$ y $d = y^2$. Es fácil ver que $b^2 + bd = x^4 + x^2y^2 = x^2z^2$ y que $d^2 + bd = y^4 + x^2y^2 = y^2z^2$ son ambos, pues, cuadrados perfectos. Pongamos $a = \sqrt{b^2 + bd} = xz$ y $c = \sqrt{d^2 + bd} = yz$. Con esta notación se tiene que $a^2 - b^2 = b^2 + bd - b^2 = bd = d^2 + bd - d^2 = c^2 - d^2$, de modo que poniendo $n = xy$ tenemos una 5-tupla $(a, b, n, c, d) = (xz, x^2, xy, yz, y^2)$ con b y d coprimos, lo que nos da una representación de $n = xy$ como el cateto de dos triángulos rectángulos distintos y semejantes (ver Figura 3).

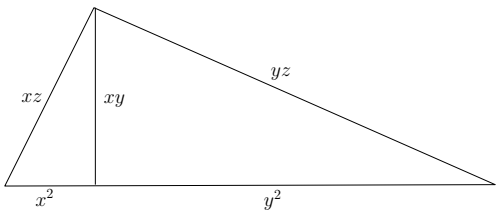

FIGURA 3. Las dos representaciones semejantes de xy dadas por la terna pitagórica (x, y, z).

Recíprocamente, supongamos que $(a, b, n, c, d) \in \mathcal{Q}$. Por semejanza de triángulos se tiene que $bd = n^2$ y se sigue que, siendo b y d coprimos, $b = x^2$ y $d = y^2$. Ahora, se tiene $a^2 = n^2 + b^2 = b(d + b)$ con lo que b divide a a^2 y consecuentemente x divide a a. De manera idéntica se prueba que y divide a c. Más aún, se tiene que $\dfrac{a^2}{b} = d + b = \dfrac{c^2}{d}$ y así $\dfrac{a}{x} = \dfrac{b}{y}$. Finalmente, de todas las consideraciones anteriores se sigue que $\left(x, y, \dfrac{a}{x}\right) \in \mathcal{T}$ es una terna pitagórica primitiva.

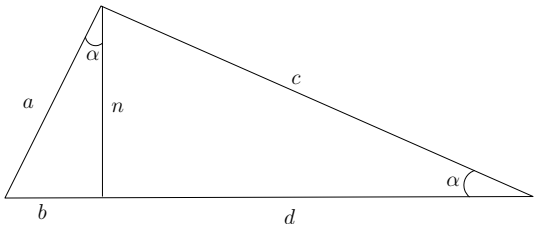

FIGURA 4. Un entero n como cateto de dos triángulos rectángulos distintos y semejantes.

En vista de todo lo anterior podemos presentar el resultado principal de esta sección.

Proposición 10. *$\mathcal{T}$ y $\mathcal{Q}$ son biyectivos.*

Demostración: Acabamos de construir aplicaciones $\varphi : \mathcal{T} \longrightarrow \mathcal{Q}$ y $\psi : \mathcal{Q} \longrightarrow \mathcal{T}$ dadas por $\varphi(x, y, z) = (xz, x^2, xy, yz, y^2)$ y $\psi(a, b, n, c, d) = \left(\sqrt{b}, \sqrt{d}, \dfrac{a}{\sqrt{b}}\right)$. Ya hemos visto que están bien definidas por lo que basta ver que son inversas una de la otra; pero esto es una comprobación trivial. □

6. Triángulos rectángulos con lados y alturas enteros

En la sección anterior hemos hecho notar que un elemento $(a, b, n, c, d) \in \mathcal{Q}$ puede verse como un triángulo rectángulo cuyos lados y alturas son números enteros (a, c y $b + d$ son los lados y n la altura sobre la hipotenusa). Comenzaremos esta sección viendo todo triángulo rectángulo cuyos lados y alturas sean números enteros es de esta forma.

Proposición 11. *En un triángulo rectángulo cuyos lados y alturas son números enteros, la altura sobre la hipotenusa divide a la misma en dos segmentos cuyas longitudes son también números enteros.*

Demostración: Emplearemos la notación de la Figura 5. Por hipótesis d, e, h y $f+g$ son números enteros, nuestro objetivo es probar que f y g también lo son.

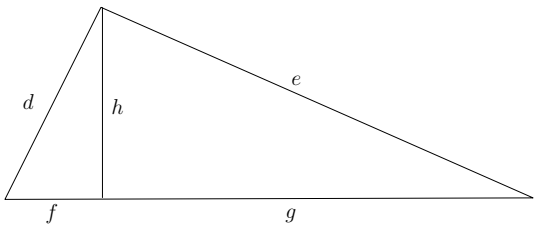

FIGURA 5. Un entero n como cateto de dos triángulos rectángulos distintos y semejantes.

Tenemos que $f^2 = d^2 - h^2 \in \mathbb{Z}$, $g^2 = e^2 - h^2 \in \mathbb{Z}$ y $fg = h^2 \in \mathbb{Z}$. Como consecuencia se sigue que $g^2 - f^2 \in \mathbb{Z}$ y así $g - f = \dfrac{g^2 - f^2}{g + f} \in \mathbb{Q}$. Por otra parte $(g - f)^2 = g^2 + f^2 - 2fg \in \mathbb{Z}$ y por tanto resulta que $g - f \in \mathbb{Z}$. Finalmente $2f = (g + f) - (g - f) \in \mathbb{Z}$ y del mismo modo $2g \in \mathbb{Z}$; por tanto $f, g \in \mathbb{Q}$. Pero como $f^2, g^2 \in \mathbb{Z}$ se tiene que $f, g \in \mathbb{Z}$ como se quería. □

Una vez visto esto y con ayuda de la sección anterior podemos ya parametrizar todos los triángulos rectángulos de lados y alturas enteros.

Teorema 1. *Un triángulo rectángulo de lados (h,k,l) tiene lados y alturas enteros si y sólo si existen enteros coprimos p y q (con $p>q$ y uno de ellos par) tales que:*

$$h = p^4 - q^4.$$
$$k = 2pq(p^2+q^2).$$
$$l = (p^2+q^2)^2.$$

En este caso, además, la altura sobre la hipotenusa tiene longitud $2pq(p^2-q^2)$.

Demostración: Consideremos un triángulo rectángulo de lados enteros (h,k,l) y tal que su altura sobre la hipotenusa es un número entero n. entonces por la proposición anterior sabemos que existen enteros a y b con $a+b=l$ tales que $(h,a,n,k,b)\in\mathcal{Q}$. Por otro lado, según se vio en la sección anterior, existe una única terna $(x,y,z)\in\mathcal{T}$ de modo que $h=xz$, $k=yz$, $a=x^2$, $b=y^2$ y $n=xy$. Si recordamos que la parametrización usual de las ternas pitagóricas dice que existen p y q en las condiciones del enunciado cumpliendo:

$$x = p^2 - q^2.$$
$$y = 2pq.$$
$$z = p^2 + q^2.$$

basta sustituir en las anteriores expresiones para obtener el resultado. □

7. Una curiosidad: los múltiplos de 25

En la cuarta sección hemos probado que un número de la forma p^2, siendo p un primo impar puede representarse de una única forma no trivial como diferencia de cuadrados. En particular se tiene que $25 = 13^2 - 12^2$. En esta última sección, que no es más que una mera curiosidad,veremos cómo estos valores (13 y 12) aparecen persistentemente en las representaciones como diferencia de cuadrados de ciertos múltiplos de 25. Por ejemplo, se tiene que:

$$25 = 13^2 - 12^2 \qquad 625 = 313^2 - 312^2$$
$$225 = 113^2 - 112^2 \qquad 7225 = 3613^2 - 3612^2$$

Proposición 12. *Si n es un entero impar, entonces el número $25n^2$ admite una representación como diferencia de cuadrados, pongamos $25n^2 = x^2 - y^2$, tal que $x = 100a+13$ e $y = 100b+12$; es decir, tal que x termina en 13 e y lo hace en 12.*

Demostración: Podemos representar $25n^2$ como diferencia de cuadrados, al menos, de este modo:

$$25n^2 = \left(\frac{25n^2+1}{2}\right)^2 - \left(\frac{25n^2-1}{2}\right)^2$$

Ahora, es fácil ver que para todo n impar $\frac{25n^2+1}{2} \equiv 13 \pmod{100}$ puesto que si ponemos $n=2n'+1$ resulta que $\frac{25n^2+1}{2} = \frac{100n'^2+100n'+26}{2} = 100\frac{n'(n'+1)}{2} + 13$. Ver que $\frac{25n^2-1}{2} \equiv 12 \pmod{100}$ es análogo y concluye la prueba. □

Referencias

[1] **Grosswald, E.** *Representation of integers as sums of squares*, Springer-Verlag, New York 1985.

[2] **Hardy, G.H., Wright, E.M.** *An introduction to the theory of numbers*, Clarendon Press, Oxford 1992.

[3] **Mollin, R.A.** *Fundamental number theory with applications*, CRC Press, 1997.

Departamento de Matemáticas, Universidad de Zaragoza, C/Pedro Cerbuna 12, 50009 Zaragoza (España)

E-mail address: oller@unizar.es