Capítulo 5 Catetos

En lo sucesivo, dada una terna pitagórica (a, b, c) (ordenada o no), llamaremos *primer cateto* a a y *segundo cateto* a b. Además, tendremos en cuenta que, para cualquier $m \in \mathbb{N} - \{1, 2\}$, existe una correspondencia biunívoca entre las ternas pitagóricas no ordenadas con primer cateto igual a m y las ternas pitagóricas ordenadas con segundo cateto igual a m (y viceversa).

Para cualquier número natural mayor o igual que 3 existe, al menos, una terna pitagórica cuyo primer cateto es igual a dicho número. Además, para cualquier número natural mayor o igual que 3 y distinto de 4 existe, al menos, una terna pitagórica ordenada cuyo primer cateto es igual a dicho número.

Surge, de forma natural, contabilizar el número de ternas pitagóricas que tienen como primer cateto un cierto número natural m mayor o igual que 3. Para ello, hemos caracterizado las ternas pitagóricas en función de su primer cateto m y de los divisores de m^2, de forma que cada par de divisores gemelos $(d, \overline{d})$ de m^2 tal que $d < m$ y, tanto d como $\overline{d}$, tienen la misma paridad genera una terna pitagórica con primer cateto m, por lo que el número de ternas pitagóricas cuyo primer cateto es igual a m será igual al número de divisores de m^2 que son menores que m y tienen la misma paridad que su divisor gemelo. También se han caracterizado aquellas ternas pitagóricas con primer cateto igual a m que son ordenadas y se ha calculado cuántas de ellas pueden ser primitivas.

Otra cuestión que llama la atención es que, cuando m es un número natural impar, el número de ternas pitagóricas tales que su primer cateto es igual a m y su semiperímetro s es un número natural impar coincide con el número de divisores (necesariamente impares) de m^2 menores que m y tales que su divisor gemelo es congruente con m módulo 4, mientras que, cuando m es un número natural par, el número de ternas pitagóricas tales que su primer cateto es igual a m y su semiperímetro s es un número natural impar coincide con el número de divisores pares de m^2 menores que m y tales que su divisor gemelo no es congruente con m módulo 4.

Al comparar la relación de orden entre lados, inradio y exinradios, sorprende la relación entre el cateto menor a de una terna pitagórica ordenada con primer cateto

m y el segundo exinradio r_b de ésta, ya que, en algunos casos $a < r_b$, en otros casos se da la igualdad y en otros casos $a > r_b$, lo cual está determinado por el número de divisores de m^2 menores que $(\sqrt{2}-1)m$ con igual paridad que su divisor gemelo que se encuentran en los intervalos $\left(1, \frac{m}{3}\right)$ ó $\left(\frac{m}{3}, \sqrt{2}-1)m\right)$. Únicamente en las ternas pitagóricas proporcionales a la terna $(3, 4, 5)$ se da la igualdad entre el cateto menor y el segundo exinradio.

Teorema 5.1 (Parametrización de las ternas pitagóricas en función del primer cateto)**.** *Dado $m \in \mathbb{N} - \{1, 2\}$, cualquier terna pitagórica (a, b, c) con primer cateto igual a m es de la forma*

$$(a, b, c) = \left(m, \frac{\overline{d} - d}{2}, \frac{\overline{d} + d}{2}\right),$$

donde d y $\overline{d}$ son dos divisores de m^2 tales que $d \cdot \overline{d} = m^2$, siendo $d < m$ y verificando que, tanto d como $\overline{d}$, tienen la misma paridad.

Demostración. Si $m \in \mathbb{N} - \{1, 2\}$ es el primer cateto de una terna pitagórica (a, b, c), como

$$m^2 = a^2 = c^2 - b^2 = (c - b)(c + b),$$

entonces, $d = c - b$ y $\overline{d} = c + b$ son divisores (que denominaremos *divisores gemelos*) de m^2 verificando que

$$\begin{cases} c - b = d \\ c + b = \overline{d} \end{cases} \Rightarrow \begin{cases} b = \dfrac{\overline{d} - d}{2}, \\ c = \dfrac{\overline{d} + d}{2}, \end{cases}$$

por lo que

$$(a, b, c) = \left(m, \frac{\overline{d} - d}{2}, \frac{\overline{d} + d}{2}\right),$$

pero esta condición no es suficiente, ya que no garantiza que $\left(m, \frac{\overline{d}-d}{2}, \frac{\overline{d}+d}{2}\right) \in \mathbb{N}^3$. Para ello, debe ocurrir que $d < \overline{d}$ (es decir, que $d < m$) y que, tanto d como $\overline{d}$, tengan la misma paridad. □

Corolario 5.1.1. *Sea $(a_0, b_0, c_0) \in \mathcal{T}_p$ una terna pitagórica primitiva:*

1. *La sucesión de ternas pitagóricas definida recurrentemente por*

$$\forall n \in \mathbb{N} : (a_n, b_n, c_n) = \left(c_{n-1}, \frac{c_{n-1}^2 - 1}{2}, \frac{c_{n-1}^2 + 1}{2}\right),$$

   verifica que:

   a) *Está bien definida.*
   b) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada.*
   c) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva.*
   d) *Para cualquier $n \in \mathbb{N}$, (a_n, b_n, c_n) es la terna pitagórica de hipotenusa máxima que se puede construir con primer cateto igual a c_{n-1} .*

2. *La sucesión de ternas pitagóricas definida recurrentemente por*

$$\forall n \in \mathbb{N} : (a_n, b_n, c_n) = \left(a_{n-1} + b_{n-1}, \frac{(a_{n-1} + b_{n-1})^2 - 1}{2}, \frac{(a_{n-1} + b_{n-1})^2 + 1}{2}\right),$$

verifica que:

   a) *Está bien definida.*
   b) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada.*
   c) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva.*
   d) *Para cualquier $n \in \mathbb{N}$, (a_n, b_n, c_n) es la terna pitagórica de hipotenusa máxima que se puede construir con primer cateto igual a $a_{n-1} + b_{n-1}$.*

3. *Si b_0 es par, la sucesión de ternas pitagóricas definida recurrentemente por*

$$\forall n \in \mathbb{N} : (a_n, b_n, c_n) = \left(b_{n-1} + c_{n-1}, \frac{(b_{n-1} + c_{n-1})^2 - 1}{2}, \frac{(b_{n-1} + c_{n-1})^2 + 1}{2}\right),$$

verifica que:

   a) *Está bien definida.*
   b) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada.*
   c) *Para cualquier $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva.*
   d) *Para cualquier $n \in \mathbb{N}$, (a_n, b_n, c_n) es la terna pitagórica de hipotenusa máxima que se puede construir con primer cateto igual a $b_{n-1} + c_{n-1}$.*

Demostración.

1. La sucesión de ternas pitagóricas definida recurrentemente por

$$\forall n \in \mathbb{N} : (a_n, b_n, c_n) = \left(c_{n-1}, \frac{c_{n-1}^2 - 1}{2}, \frac{c_{n-1}^2 + 1}{2}\right),$$

verifica que:

   a) Como la terna pitagórica (a_0, b_0, c_0) es primitiva, entonces, c_0 es impar, lo cual implica que todos los divisores de c_0^2 tienen la misma paridad que los correspondientes divisores gemelos, por lo que, en particular, $(1, c_0^2)$ es un par de divisores válidos de c_0^2, garantizando este hecho que

$$(a_1, b_1, c_1) = \left(c_0, \frac{c_0^2 - 1}{2}, \frac{c_0^2 + 1}{2}\right)$$

   es una terna pitagórica. Además, como $a_1 = c_0$ es impar, entonces, c_1 es impar, por lo que bastaría con repetir indefinidamente el razonamiento anterior.

b) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada si y sólo si

$$c_{n-1} = a_n < b_n = \frac{c_{n-1}^2 - 1}{2},$$

lo cual es cierto si y sólo si $c_{n-1} > 1 + \sqrt{2}$. Por tanto, para todo $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada, ya que, según el sexto apartado de las propiedades 1.1 (pág. 17), la hipotenusa de cualquier terna pitagórica es mayor o igual que $5 > 1 + \sqrt{2}$.

c) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva, ya que

$$\forall\, n \in \mathbb{N} : c_n = \frac{c_{n-1}^2 + 1}{2} = \frac{c_{n-1}^2 - 1}{2} + 1 = b_n + 1,$$

y cualesquiera dos números naturales consecutivos son primos entre sí.

d) Es consecuencia directa del teorema 5.1 y del lema 1.3 (pág. 45).

El programa 5.2 (pág. 330), introduciendo un valor $m \in \mathbb{N}$, nos muestra los m primeros términos de esta sucesión de ternas pitagóricas.

2. La sucesión de ternas pitagóricas definida recurrentemente por

$$\forall\, n \in \mathbb{N} : (a_n, b_n, c_n) = \left(a_{n-1} + b_{n-1}, \frac{(a_{n-1} + b_{n-1})^2 - 1}{2}, \frac{(a_{n-1} + b_{n-1})^2 + 1}{2}\right),$$

verifica que:

a) Como la terna pitagórica (a_0, b_0, c_0) es primitiva, entonces, $a_0 + b_0$ es impar, lo cual implica que todos los divisores de $(a_0 + b_0)^2$ tienen la misma paridad que los correspondientes divisores gemelos, por lo que, en particular, $\big(1, (a_0 + b_0)^2\big)$ es un par de divisores válidos de $(a_0 + b_0)^2$, garantizando este hecho que:

$$(a_1, b_1, c_1) = \left(a_0 + b_0, \frac{(a_0 + b_0)^2 - 1}{2}, \frac{(a_0 + b_0)^2 + 1}{2}\right)$$

es una terna pitagórica. Además, como $a_1 = a_0 + b_0$ es impar, entonces,

$$(a_0 + b_0)^2 \equiv 1 (\text{mód}\, 4) \Rightarrow (a_0 + b_0)^2 - 1 \equiv 0 (\text{mód}\, 4),$$

por lo que

$$b_1 = \frac{(a_0 + b_0)^2 - 1}{2} \equiv 0 (\text{mód}\, 2),$$

siendo $a_1 + b_1$ impar y, por tanto, bastaría con repetir indefinidamente el razonamiento anterior.

b) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada si y sólo si

$$a_{n-1} + b_{n-1} = a_n < b_n = \frac{(a_{n-1} + b_{n-1})^2 - 1}{2},$$

lo cual es cierto si y sólo si $a_{n-1} + b_{n-1} > 1 + \sqrt{2}$. Por tanto, para todo $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada, ya que, según el sexto apartado de las propiedades 1.1 (pág. 17), la suma de los catetos de cualquier terna pitagórica es mayor o igual que $7 > 1 + \sqrt{2}$.

c) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva, ya que

$$\forall\, n \in \mathbb{N} : c_n = \frac{(a_{n-1} + b_{n-1})^2 + 1}{2} = \frac{(a_{n-1} + b_{n-1})^2 - 1}{2} + 1 = b_n + 1,$$

y cualesquiera dos números naturales consecutivos son primos entre sí.

d) Es consecuencia directa del teorema 5.1 y del lema 1.3 (pág. 45).

El programa 5.3 (pág. 331), introduciendo un valor $m \in \mathbb{N}$, nos muestra los m primeros términos de esta sucesión de ternas pitagóricas.

3. La sucesión de ternas pitagóricas definida recurrentemente por

$$\forall\, n \in \mathbb{N} : (a_n, b_n, c_n) = \left(b_{n-1} + c_{n-1}, \frac{(b_{n-1} + c_{n-1})^2 - 1}{2}, \frac{(b_{n-1} + c_{n-1})^2 + 1}{2}\right),$$

verifica que:

a) Como la terna pitagórica (a_0, b_0, c_0) es primitiva y b_0 es par, entonces, $b_0 + c_0$ es impar, lo cual implica que todos los divisores de $(b_0 + c_0)^2$ tienen la misma paridad que los correspondientes divisores gemelos, por lo que, en particular, $\big(1, (b_0 + c_0)^2\big)$ es un par de divisores válidos de $(b_0 + c_0)^2$, garantizando este hecho que

$$(a_1, b_1, c_1) = \left(b_0 + c_0, \frac{(b_0 + c_0)^2 - 1}{2}, \frac{(b_0 + c_0)^2 + 1}{2}\right)$$

es una terna pitagórica. Además, como $a_1 = b_0 + c_0$ es impar, entonces,

$$(b_0 + c_0)^2 \equiv 1 (\text{mód } 4),$$

por lo que

$$\begin{cases} (b_0 + c_0)^2 - 1 \equiv 0 (\text{mód } 4) \Rightarrow b_1 = \dfrac{(b_0 + c_0)^2 - 1}{2} \equiv 0 (\text{mód } 2), \\ (b_0 + c_0)^2 + 1 \equiv 2 (\text{mód } 4) \Rightarrow c_1 = \dfrac{(b_0 + c_0)^2 + 1}{2} \equiv 1 (\text{mód } 2), \end{cases}$$

resultando que $b_1 + c_1$ es impar y, por tanto, bastaría con repetir indefinidamente el razonamiento anterior.

b) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada si y sólo si

$$b_{n-1} + c_{n-1} = a_n < b_n = \frac{(b_{n-1} + c_{n-1})^2 - 1}{2},$$

lo cual es cierto si y sólo si $b_{n-1} + c_{n-1} > 1 + \sqrt{2}$. Por tanto, para todo $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es ordenada, ya que, según el sexto apartado de las propiedades 1.1 (pág. 17), la suma de un cateto y la hipotenusa de cualquier terna pitagórica es mayor o igual que $8 > 1 + \sqrt{2}$.

c) Para cada $n \in \mathbb{N}$, la terna pitagórica (a_n, b_n, c_n) es primitiva, ya que

$$\forall\, n \in \mathbb{N} : c_n = \frac{(b_{n-1} + c_{n-1})^2 + 1}{2} = \frac{(b_{n-1} + c_{n-1})^2 - 1}{2} + 1 = b_n + 1,$$

y cualesquiera dos números naturales consecutivos son primos entre sí.

d) Es consecuencia directa del teorema 5.1 y del lema 1.3 (pág. 45).

El programa 5.4 (pág. 331), introduciendo un valor $m \in \mathbb{N}$, nos muestra los m primeros términos de esta sucesión de ternas pitagóricas.

□

Ejemplo 5.1. Tomando $(a_0, b_0, c_0) = (3, 4, 5) \in \mathcal{T}_p$, los primeros términos de las sucesiones consideradas en el corolario 5.1.1 son:

1. $(3, 4, 5), (5, 12, 13), (13, 84, 85), (85, 3612, 3613), (3613, 6526884, 6526885), \ldots$
2. $(3, 4, 5), (7, 24, 25), (31, 480, 481), (511, 130560, 130561), \ldots$
3. $(3, 4, 5), (9, 40, 41), (81, 3280, 3281), (6561, 21523360, 21523361), \ldots$

Pueden consultarse los programas 5.2, 5.3 y 5.4 (pág. 330) para comprobar los resultados obtenidos.

Corolario 5.1.2. *Dado un número natural impar p que no es múltiplo de 3, para cualquier $n \in \mathbb{N}$, se verifica que*

$$p^{2n} - 1 \equiv 0 (\text{mód } 24).$$

Demostración. Vamos a distinguir dos casos:

Teorema chino del resto

El teorema chino del resto es un resultado sobre congruencias en teoría de números y sus generalizaciones en álgebra abstracta. Apareció publicado por primera vez en el siglo III en una obra con los trabajos del matemático chino Sun Tzu.

Supongamos que $n_1, n_2, \ldots, n_k$ son enteros positivos coprimos dos a dos. Entonces, para números enteros dados $a_1, a_2, \ldots, a_k$, existe un número entero x que resuelve el siguiente sistema de congruencias simultáneas

$$\left.\begin{array}{c} x \equiv a_1 (\text{mód } n_1) \\ x \equiv a_2 (\text{mód } n_2) \\ \vdots \\ x \equiv a_k (\text{mód } n_k) \end{array}\right\}$$

Todas las soluciones de x de dicho sistema son congruentes módulo el producto $N = n_1 n_2 \cdots n_k$.

De manera más general, las congruencias simultáneas pueden ser resueltas si los n_i son coprimos a pares. Existe una solución x si y solo si $a_i \equiv a_j \big(\text{mód } \operatorname{mcd}(n_i, n_j)\big)$, para todo i y j. Todas las soluciones x son, en dicho caso, congruentes módulo el mínimo común múltiplo de los n_i.