Ternas Pitagóricas

Alan Reyes-Figueroa
Teoría de Números

(Aula 06) 27.julio.2021

Como aplicación de las propiedades de divisibilidad, vamos a resolver algunas ecuciones diofantinas simples.

Teorema (Ecuación diofantina $x^2 - y^2 = n$)

Un número entero n corresponde a una diferencia de cuadrados perfectos si, y sólo si, n es impar, ó n es múltiplo de 4.

Prueba: ($\Rightarrow$) Suponga que $n = x^2 - y^2$, para $x, y \in \mathbb{Z}$. Entonces podemos escribir $n = x^2 - y^2 = (x+y)(x-y) = uv$, con $u = x+y$, $v = x-y$. Luego, $2x = u+v$, $2y = u - v \;\Rightarrow\; x = \frac{u+v}{2}$, $y = \frac{u-v}{2}$. En particular, u y v tienen la misma paridad (basta verificar los cuatro casos posibles).

- Si u y v son impares, entonces $n = uv$ es impar.
- Si u y v son pares, digamos $u = 2r$, $v = 2s$, entonces $n = uv = (2r)(2s) = 4rs$, y $4 \mid n$.

($\Leftarrow$) Analizamos cada caso por separado:

- Si n es impar, $n = 2k + 1 = (2k + 1)(1)$. Entonces $x = \frac{2k+1+1}{2} = k + 1$, $y = \frac{2k+1-1}{2} = k$ y podemos escribir $n = 2k + 1 = (k + 1)^2 - k^2$.
- Si $4 \mid n$, tenemos $n = 4k = (2k)(2)$. Entonces $x = \frac{2k+2}{2} = k + 1$, $y = \frac{2k-2}{2} = k - 1$ y podemos escribir $n = 4k = (k + 1)^2 - (k - 1)^2$. $\square$

Ejemplos:

- $31 = 31 \cdot 1 \;\Rightarrow\; 31 = 16^2 - 15^2$.
- $32 = 16 \cdot 2 \;\Rightarrow\; 32 = 9^2 - 7^2$.
- Observe también que $32 = 8 \cdot 4 \;\Rightarrow\; 32 = 6^2 - 2^2$.

Lo anterior muestra que la representación como diferencia de cuadrados no es única.

Ternas Pitagóricas

Mostramos ahora las soluciones a la ecuación del Último Teorema de Fermat en su caso más simple: $x^2 + y^2 = z^2$.

De entrada, observe que la ecuación $x^2 + y^2 = z^2$ admite soluciones **triviales** de la forma $(\pm x, 0, \pm x)$ y $(0, \pm y, \pm y)$, para cualesquiera $x, y \in \mathbb{Z}$.

Suponga que $x^2 + y^2 = z^2$, con $x, y, z > 0$. Sin pérdida de generalidad, podemos asumir que z, y, z son primos relativos entre sí, pues si $d = (x, y, z)$ entonces $x = dx'$, $y = dy'$, $z = dz'$, entonces

$$x^2+y^2 = z^2 \;\Rightarrow\; (dx')^2+(dy')^2 = (dz')^2 \;\Rightarrow\; d^2\big((x')^2+(y')^2\big) = d^2(z')^2 \;\Rightarrow\; (x')^2+(y')^2 = (z')^2.$$

En particular, x, y no pueden ser ambos pares, pues $2 \mid x$, $2 \mid y \;\Rightarrow\; 2 \mid z$.

Por otro lado, si x, y fuesen ambos impares, tendríamos $x = 2a + 1$, $y = 2b + 1$, luego

$$z^2 = x^2 + y^2 = (2a+1)^2 + (2b+1)^2 = 4a^2 + 4a + 1 + 4b^2 + 4b + 1 = 4(a^2 + b^2 + a + b) + 2.$$

Así, z^2 es de la forma $4k + 2 \;\Rightarrow\; z^2$ es par $\Rightarrow z$ es par y z^2 es de la forma $4k$ (absurdo).

En conclusión, x, y tienen paridad distinta.

Sea entonces x par, y impar. Luego z es impar. Como $x^2 = z^2 - y^2 = (z+y)(z-y)$, y los términos $z+y$, $z-y$ son ambos pares, podemos escribir

$$x = 2a, \quad z+y = 2b, \quad z-y = 2c, \qquad \text{para ciertos } a, b, c \in \mathbb{Z}.$$

Observe en particular que $z = b + c$, $y = b - c$.

De ahí que $4a^2 = (2a)^2 = x^2 = (z+y)(z-y) = (2b)(2c) = 4bc \;\Rightarrow\; a^2 = bc$. Afirmamos que $(b, c) = 1$. Caso contrario, si p es un primo tal que $p \mid b$ y $p \mid c$, entonces $p \mid b + c = z$ y $p \mid b - c = y$, lo que implica que $p \mid z^2 - y^2 = x^2 \;\Rightarrow\; p \mid x$, y así $(x, y, z) \geq p$, contrario al supuesto inicial.

Sea $a = p_1^{k_1} \cdots p_r^{k_r}$ la factoración en primos de a. Entonces $a^2 = p_1^{2k_1} \cdots p_r^{2k_r}$ y todos estos primos dividen al producto bc. Siendo $(b, c) = 1$, entonces necesariamente estos primos se particionan en dos grupos: (los que dividen a b y los que dividen a c), y obtenemos $b = p_1^{2k_1} \cdots p_m^{2k_m}$ y $c = p_{m+1}^{2k_{m+1}} \cdots p_r^{2k_r}$. Portanto, b y c son cuadrados perfectos.

Ternas Pitagóricas

Entonces $b = v^2$, $c = u^2$. Ambos u, v son impares y $(u, v) = 1$, con $u < v$. Luego $z + y = v^2$, $z - y = u^2$, y $x^2 = u^2v^2$. Así, obtenemos la parametrización

$$\boxed{x = uv, \qquad y = \frac{v^2 - u^2}{2}, \qquad z = \frac{v^2 + u^2}{2}.}$$

En particular

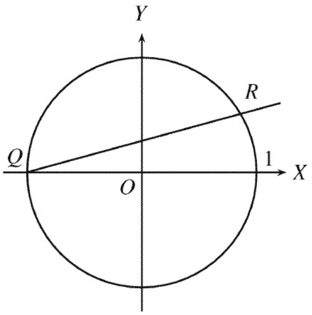
$$x^2 + y^2 = u^2v^2 + \left(\frac{v^2 - u^2}{2}\right)^2 = u^2v^2 + \frac{v^4 - 2u^2v^2 + u^4}{4} = \frac{v^4 + 2u^2v^2 + u^4}{4} = \left(\frac{v^2 + u^2}{2}\right)^2 = z^2.$$

Ejemplos:

u	v	x	y	z
1	3	3	4	5
1	5	5	12	13
1	7	7	24	25
1	9	9	40	41
3	5	15	8	17
3	7	21	20	29
5	7	35	12	37
5	9	45	28	53

Ternas pitagóricas primitivas.

Puntos Racionales sobre el Círculo: *Método de las cuerdas* de DIOFANTO.



Una solución entera (a, b, c) de la ecuación $x^2 + y^2 = z^2$ implica que

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Entonces $X = \frac{a}{c}$, $Y = \frac{b}{c}$ es una solución racional de la ecuación $X^2 + Y^2 = 1$. En otras palabras, $(X, Y) \in \mathbb{Q}^2$ es un punto racional sobre el círculo $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

Cualquier múltiplo de la tripla (ma, mb, mc) corresponde al mismo punto racional (X, Y), de modo que podemos restringirnos a buscar soluciones primitivas. DIOFANTO encontró las soluciones racionales de $X^2 + Y^2 = 1$ mediante un método algebraico, cuya geometría se ilustra en la Figura. Sean $Q = (-1, 0)$, R un punto racional sobre S^1, y ℓ la recta de Q a R.

Ternas Pitagóricas

ℓ es una recta con pendiente racional, porque las coordenadas de R y Q son racionales. Si la pendiente es t, la ecuación de esta línea es

$$Y = t(X+1).$$

Recíprocamente, cualquier recta de esta forma, con pendiente racional t, se encuentra con el círculo S^1 en un punto racional $R \in \mathbb{Q}^2$. Esto se puede ver calculando las coordenadas de R: sustituyendo $Y = t(X+1)$ en $X^2 + Y^2 = 1$, lo que resulta

$$X^2 + t^2(X+1)^2 = 1, \qquad \Rightarrow \qquad (1+t^2)X^2 + 2t^2X + t^2 - 1 = 0.$$

de donde obtenemos las soluciones $X = -1$ y $X = \frac{1-t^2}{1+t^2}$.

La solución $X = -1$ corresponde al punto Q, entonces la coordenada X en R es $\frac{1-t^2}{1+t^2}$, y por tanto la coordenada Y es

$$Y = t\big(\tfrac{1-t^2}{1+t^2} + 1\big) = \tfrac{2t}{1+t^2}.$$

Así, un punto racional arbitrario en el círculo unitario S^1 tiene coordenadas

$$R = \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big), \qquad \text{con } t \in \mathbb{Q}.$$

Ternas Pitagóricas

Ahora podemos recuperar las fórmulas pitagóricas de Euclides.

Sea $t \in \mathbb{Q}$ un racional arbitrario, $t = \frac{u}{v}$ donde $u, v \in \mathbb{Z}$. El punto racional R se convierte en

$$R = \Big(\frac{1 - u^2/v^2}{1 + u^2/v^2}, \frac{2u/v}{1 + u^2/v^2}\Big) = \Big(\frac{v^2 - u^2}{v^2 + u^2}, \frac{2uv}{v^2 + u^2}\Big) = \Big(\frac{\frac{v^2-u^2}{2}}{\frac{v^2+u^2}{2}}, \frac{uv}{\frac{v^2+u^2}{2}}\Big), \qquad \text{con } u, v \in \mathbb{Z},$$

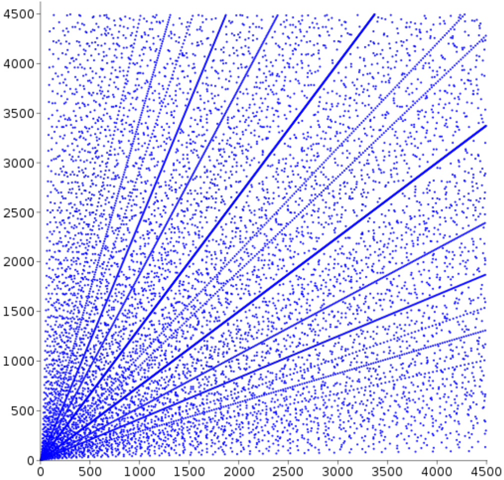
y recuperamos las mismas ecuaciones paramétricas anteriores.

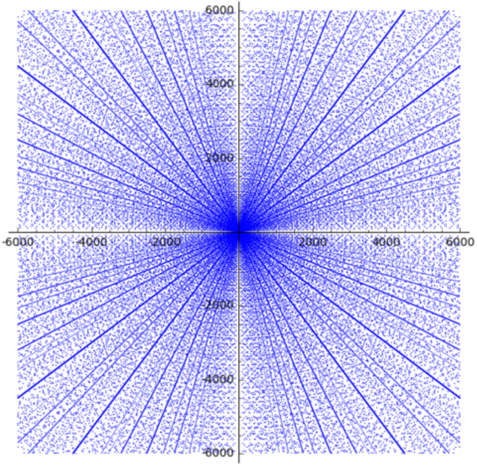
$$\boxed{y = uv, \qquad x = \frac{v^2-u^2}{2}, \qquad z = \frac{v^2+u^2}{2}.}$$

y el punto racional

$$\boxed{R = \big(\tfrac{x}{z}, \tfrac{y}{z}\big).}$$

Ternas Pitagóricas





Ternas Pitagóricas