Ternas Pitagóricas

Alan Reyes-Figueroa
Teoría de Números

(Aula 08) 27.julio.2023

Como aplicación de las propiedades de divisibilidad, vamos a resolver algunas ecuaciones 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:

Algunas Ecuaciones Diofantinas

- 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 x, y, z son primos relativos entre sí, pues si $d = (x, y, z)$ entonces $x = dx'$, $y = dy'$, $z = dz'$, entonces

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

Llamamos a estas (x, y, z) con x, y, z coprimos dos a dos, **soluciones primitivas**.
Si (x, y, z) es una solución primitiva, entonces cualquier otra tripla de la forma $k \cdot (x, y, z)$, $k \in \mathbb{Z}$ es también solución.

Si (x, y, z) es una solución con entradas no negativas, entonces $(\pm x, \pm y, \pm z)$ son soluciones.
Basta entonces buscar soluciones no triviales, positivas, primitivas.

Construcción de Ternas Primitivas

Sea $(x, y, z) \in \mathbb{Z}^3$, una solución no trivial, positiva y primitiva. En particular, x, y no pueden ser ambos pares, pues $2 \mid x$, $2 \mid y \;\Rightarrow\; 2 \mid z$.

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 impar, y par. Luego z es impar. Como $y^2 = z^2 - x^2 = (z + x)(z - x)$, con $z + x$, $z - x$ son ambos pares. Luego,

$$\frac{z+x}{y} = \frac{y}{z-x} \in \mathbb{Q}. \qquad \text{Hacemos } \frac{y}{z-x} = \frac{u}{v}, \text{ para ciertos } u, v \in \mathbb{Z}^+,\ (u, v) = 1.$$

De ahí que

$$\frac{z}{y} - \frac{x}{y} = \frac{z-x}{y} = \frac{v}{u}, \qquad \frac{z}{y} + \frac{x}{y} = \frac{z+x}{y} = \frac{u}{v},$$

y

$$\frac{z}{y} = \frac{1}{2}\left(\frac{u}{v} + \frac{v}{u}\right) = \frac{u^2 + v^2}{2uv}, \qquad \frac{x}{y} = \frac{1}{2}\left(\frac{u}{v} - \frac{v}{u}\right) = \frac{u^2 - v^2}{2uv}.$$

Observe que u y v deben tener paridad distinta (¿Por qué?).

- Como $(u, v) = 1$ entonces u y v no son ambos pares.
- Si u y v son ambos impares, entonces u^2, v^2 son de la forma $4k + 1$. Luego, $u^2 - v^2$ es un múltiplo de 4.
  Pero $2uv$ no es múltiplo de 4, de forma que en la fracción $\frac{u^2-v^2}{2uv}$, el numerador es divisible por al menos la potencia 2^2, mientras que el denominador es divisible a lo sumo por 2, y así
  $$x = y \cdot \tfrac{u^2-v^2}{2uv} \text{ sería par.}$$
  Lo cual es un absurdo, pues asumimos que x es impar.

Esto muestra que u y v deben ser de paridad distinta.

Construcción de Ternas Primitivas

Entonces $u^2 - v^2$ y $u^2 + v^2$ son ambos impares, lo que muestra que las fracciones

$$\frac{z}{y} = \frac{1}{2}\Big(\frac{u}{v} + \frac{v}{u}\Big) = \frac{u^2+v^2}{2uv}, \qquad \frac{x}{y} = \frac{1}{2}\Big(\frac{u}{v} - \frac{v}{u}\Big) = \frac{u^2-v^2}{2uv}.$$

ya están reducidas. Así, obtenemos la parametrización

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

con $u > v$ enteros positivos, $(u, v) = 1$ y u, v de paridad distinta.

En particular
$$x^2 + y^2 = (u^2 - v^2)^2 + 4u^2v^2 = (u^4 - 2u^2v^2 + v^4) + 4u^2v^2 = u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2 = z^2.$$

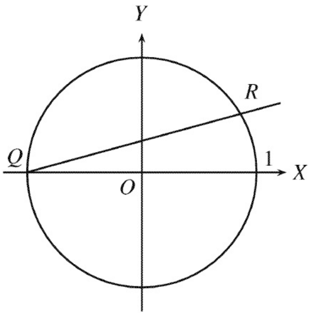
Ejemplos:

u	v	x	y	z
1	2	3	4	5
2	3	5	12	13
3	4	7	24	25
1	4	15	8	17
2	5	21	20	29

Ternas pitagóricas primitivas.

El método de Diofanto

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.

El método de Diofanto

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

$$Y = t\Big(\frac{1-t^2}{1+t^2} + 1\Big) = \frac{2t}{1+t^2}.$$

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

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

El método de Diofanto

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

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

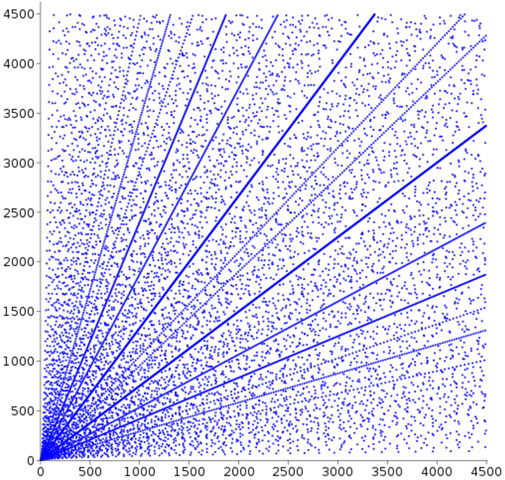
y recuperamos las mismas ecuaciones paramétricas anteriores.

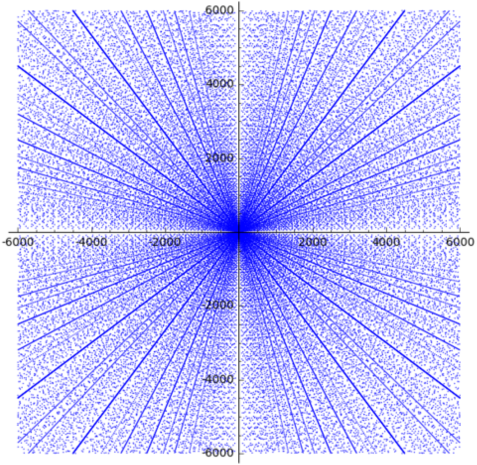
$$\boxed{y = 2uv, \qquad x = v^2 - u^2, \qquad z = v^2 + u^2.}$$

y el punto racional

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

Ternas Pitagóricas





Ternas Pitagóricas