Ecuaciones Diofantinas

Alan Reyes-Figueroa

Teoría de Números (Aula 26a) 12.octubre.2023

Estudiamos algunas ecuaciones diofantinas.

Ternas Pitagóricas:

Las triplas de números no negativos (x, y, z) que satisfacen la ecuación $x^2 + y^2 = z^2$, se llaman **triplas** o **ternas pitagóricas**.

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 $x, y, z > 0$. 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

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

Una terna pitagórica cuyos términos son primos relativos entre sí se llama una **terna pitagórica primitiva**. Nos limitamos a buscar ternas primitivas.

Observe que x, y no pueden ser ambos pares, pues si $2 \mid x$, $2 \mid y \;\Rightarrow\; 2 \mid z$.

Ternas Pitagóricas

Por otro lado, recordemos que módulo 4, todo par $a \in \mathbb{Z}$ satisface $a^2 \equiv 0 \mod 4$, mientras que todo impar satisface $a^2 \equiv 1 \pmod 4$. Así, los cuadrados son congruentes a 0 ó $1 \pmod 4$.

Si x, y fuesen ambos impares, tendríamos $z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$, lo cual es imposible. Entonces uno es par, el otro impar. Sin pérdida vamos a suponer x impar, y par $\Rightarrow$ 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.

Ternas Pitagóricas

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.

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

Esto muestra la

Proposición

Las ternas pitagóricas primitivas (x, y, z) son de la forma -0.2cm

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

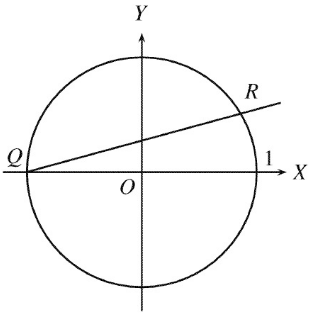
Ternas Pitagóricas

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
1	11	11	60	61
3	5	15	8	17
3	7	21	20	29
3	11	33	56	65
5	7	35	12	37
5	9	45	28	53
5	11	55	48	73
7	9	63	16	65
7	11	77	36	85

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

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

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.

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

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

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

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

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, y el punto racional

$$\boxed{y = uv, \qquad x = \tfrac{v^2-u^2}{2}, \qquad z = \tfrac{v^2+u^2}{2}.} \qquad \boxed{R = \big(\tfrac{x}{z}, \tfrac{y}{z}\big).}$$

Teorema

Los puntos racionales sobre la circunferencia S^1 son todos puntos de la forma

$$(x, y) = (-1, 0) \qquad y \qquad (x, y) = \Big(\tfrac{1-t^2}{1+t^2}, \tfrac{2t}{1+t^2}\Big), \quad \textit{con } t \in \mathbb{Q}. \quad \square$$

Sumas de Cuadrados:

Vamos a probar un resultado debido a Legendre que proporciona un criterio para determinar cuándo una ecuación del tipo $ax^2 + by^2 + cz^2 = 0$ posee solución no nula, y que da una generalización natural de las ternas pitagóricas.

Teorema (Legendre)

Sean $a, b, c \in \mathbb{Z}$ enteros libres de cuadrados, primos relativos entre sí, dos a dos, y no todos del mismo signo. La ecuación $ax^2 + by^2 + cz^2 = 0$ posee solución no trivial $(x, y, z) \neq (0, 0, 0)$., con $x, y, z \in \mathbb{Z}$ si, y sólo si, $-bc$ es un cuadrado módulo a, $-ca$ es cuadrado módulo b, y $-ab$ es cuadrado módulo c.

Prueba: $(\Rightarrow)$ Mostramos que $-bc$ es un cuadrado módulo a. De hecho, x, y y z son primos relativos dos a dos, pues si $d \mid x$, $d \mid y$, entonces $d^2 \mid x^2$, $d^2 \mid y^2 \;\Rightarrow\; d^2 \mid ax^2 + by^2 = -cz^2$ y como c es libre de cuadrados, $\;d^2 \mid cz^2 \;\Rightarrow\; d \mid z$. Al igual que en el caso de las ternas pitagóricas

Sumas de Cuadrados

Podemos escribir entonces $x = dx', y = dy', z = dz'$, con $z', y', z' \in \mathbb{Z}$, y tenemos que

$$\begin{aligned} ax^2 + by^2 + cz^2 = 0 \quad &\Longrightarrow \quad a(dx')^2 + b(dy')^2 + c(dz')^2 = 0 \\ &\Longrightarrow \quad a(x')^2 + b(y')^2 + c(z')^2 = 0, \end{aligned}$$

y podemos limitarnos a buscar soluciones primitivas (x, y, z).

Ahora, como $by^2 + cz^2 \equiv 0 \pmod{a}$, se sigue que $b^2y^2 \equiv -bcz^2 \pmod{a}$. Observe que z debe ser primo relativo con a, pues si p es un primo tal que $p \mid a$ y $p \mid z$, entonces $p \mid by^2$, y como $(a, b) = 1$, entonces $p \mid y$. Esto contradice el hecho que y y z son primos relativos entre sí. Portanto, $(a, z) = 1$. Luego, z es invertible módulo a y $(byz^{-1})^2 \equiv -bc \pmod{a}$. Esto muestra que $-bc$ es residuo cuadrático módulo a.
Por la simetría de la ecuación, también se prueba que $-ca$ es cuadrado módulo b, y que $-ab$ es cuadrado módulo c.

($\Leftarrow$) Vamos a suponer, sin pérdida de generalidad, que $a < 0$, $b < 0$ y $c > 0$.
Por hipótesis, existe $u \in \mathbb{Z}$ tal que $-bc \equiv u^2 \pmod{a}$. Entonces, módulo a

Sumas de Cuadrados

$$\begin{aligned} ax^2+by^2+cz^2 &\equiv by^2+cz^2 \equiv b^{-1}(b^2y^2+bcz^2) \equiv b^{-1}(b^2y^2-u^2z^2) \\ &\equiv b^{-1}(by-uz)(by+uz) \equiv (y-b^{-1}uz)(by+uz) \\ &\equiv L_1(x,y,z)\,M_1(x,y,z) \pmod{a}, \end{aligned}$$

donde $L_1(x,y,z)=d_1x+e_1y+f_1z$, y $M_1(x,y,z)=g_1x+h_1y+i_1z$ son funciones lineales, con $d_1=g_1=0$, $e_1=1$, $f_1=-b^{-1}u$, $h_1=b$ e $i_1=u$.

Similarmente,

$$\begin{aligned} ax^2+by^2+cz^2 &\equiv L_2(x,y,z)\,M_2(x,y,z) \pmod{b}, \\ ax^2+by^2+cz^2 &\equiv L_3(x,y,z)\,M_3(x,y,z) \pmod{c}, \end{aligned}$$

con $L_k(x,y,z)=d_kx+e_ky+f_kz$, y $M_k(x,y,z)=g_kx+h_ky+i_kz$, para $k=2,3$. Como a,b,c son primos relativos entre sí, por el Teorema Chino podemos hallar dos formas lineales $L(x,y,z)=dx+ey+fz$, y $M(x,y,z)=gx+hy+iz$, tales que

$$\begin{aligned} &L\equiv L_1 \pmod{a}, && L\equiv L_2 \pmod{b}, && L\equiv L_3 \pmod{c}, \\ &M\equiv M_1 \pmod{a}, && M\equiv M_2 \pmod{b}, && M\equiv M_3 \pmod{c}. \end{aligned}$$

Sumas de Cuadrados

Luego,
$$ax^2 + by^2 + cz^2 \equiv L(x,y,z)\,M(x,y,z) \pmod{abc}.$$

Consideramos ahora todas las triplas $(x,y,z) \in \mathbb{Z}^3$, con $0 \le x \le \sqrt{|bc|}$, $0 \le y \le \sqrt{|ca|}$, $0 \le z \le \sqrt{|ab|}$.
Tenemos en total $(\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ca|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > abc$ de estas triplas.

Por el Principio de Dirichlet (principio de las casillas), existen dos triplas distintas de entre estas, (x_1, y_1, z_1) y (x_2, y_2, z_2), con $L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}$
$\iff L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0 \pmod{abc}$.

Haciendo $\tilde{x} = x_1 - x_2$, $\tilde{y} = y_1 - y_2$, $\tilde{z} = z_1 - z_2$, tenemos
$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x},\tilde{y},\tilde{z})\,M(\tilde{x},\tilde{y},\tilde{z}) \pmod{abc}.$$

Note que $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0)$. Además, $|\tilde{x}| < \sqrt{|bc|}$, $|\tilde{y}| < \sqrt{|ca|}$ y $|\tilde{z}| < \sqrt{|ab|}$.
De hecho, como a, b, c son coprimos dos a dos y libres de cuadrados, no puede ocurrir la igualdad.

Sumas de Cuadrados

Por otro lado, como $a, b, < 0$ y $c > 0$, tenemos

$$-2abc = a|bc| + b|ca| < a\tilde{x}^2 + b\tilde{y}^2 a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < |ab|c = abc.$$

Como $abc \mid a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, entonces tenemos $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$, lo que resuelve el problema, o tenemos $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$.
En este último caso tenemos

$$\begin{aligned} 0 &= (a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 + abc)(\tilde{z}^2 + ab), \\ &= a(\tilde{x}\tilde{z} + b\tilde{y})^2 + b(\tilde{z}\tilde{y} - a\tilde{x})^2 + c(\tilde{z}^2 + ab)^2. \end{aligned}$$

Lo que nos da la solución $(\tilde{x}\tilde{z} + b\tilde{y}, \tilde{z}\tilde{y} - a\tilde{x}, \tilde{z}^2 + ab)$. $\square$