Triángulos Pitagóricos y Cajas Pitagóricas

J. O. Araujo, T. Bratten

Resumen
La presente nota trata sobre la resolución de la ecuación diofántica:

$$x_1^2 + \cdots + x_{n-1}^2 = x_n^2$$

Esto sería una generalización de las llamadas ternas pitagóricas cuando $n = 3$, y cajas pitagóricas cuando $n = 4$. Se presenta una expresión para obtener las soluciones haciendo uso de la parametrización de Cayley de matrices ortogonales a partir de matrices antisimétricas.

Ternas Pitagóricas

Una *terna pitagórica* es una solución de números enteros (x, y, z) de la ecuación de Pitágoras:

$$x^2 + y^2 = z^2 \tag{1}$$

Las ternas pitagóricas se asocian a triángulos rectángulos, conocidos como *triángulos pitagóricos,* donde las longitudes de sus lados se expresan con números enteros. Desde el enfoque geométrico, tiene sentido considerar ternas de números naturales, y naturalmente, desde el punto de vista algebraico se consideran las ternas de números enteros.

Una terna pitagórica (x, y, z) se dice *primitiva* si el máximo común divisor entre (x, y, z) es igual a 1.

Es claro que en una terna pitagórica primitiva (x, y, z), el máximo común divisor de los pares debe ser igual a 1, es decir $(x, y) = (y, z) = (z, x) = 1$ Además, es oportuno observar que el número z debe ser impar. Esto es inmediato si analiza las paridades de los términos de la identidad en (1).

Una manera elemental de generar ternas pitagóricas, resulta de observar que un cuadrado perfecto k^2 es la suma de los k primeros números impares, así:

$$1 = 1^2, 1 + 3 = 2^2, 1 + 3 + 5 = 3^2, 1 + 3 + 5 + 7 = 4^2 \ldots$$

Si tomamos la suma hasta un cuadrado perfecto, por ejemplo 9, obtenemos 5^2 dado que 9 es el quinto impar, entonces 5^2 se descompone como:

$$1 + 3 + 5 + 7 + 9 = 5^2$$
$$1 + 3 + 5 + 7 + 3^2 = 4^2 + 3^2 = 5^2$$

En general, si tomamos la suma:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

donde $2k - 1 = m^2$, entonces la identidad precedente puede ponerse como:

$$(k - 1)^2 + m^2 = k^2$$

Enteros de Gauss

El uso de los números complejos, más precisamente de los *enteros de Gauss*, brinda una posibilidad de parametrizar las ternas pitagóricas como mostraremos a continuación.

Notamos:

$$\mathbb{Z}[i] = \{m + ni \in \mathbb{C} : m, n \in \mathbb{Z}\}$$

El conjunto $\mathbb{Z}[i]$ es un subanillo del cuerpo de los número complejos $\mathbb{C}$, en particular es cerrado para la suma y el producto

Por otra parte, tenemos el conjunto de números complejos $\mathbb{Q}[i]$ dados por:

$$\mathbb{Q}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Q}\}$$

El conjunto $\mathbb{Q}[i]$ es un subcuerpo del cuerpo de los número complejos $\mathbb{C}$. Consideremos también la circunferencia racional S dada por:

$$S = \{z \in \mathbb{Q}[i] : |z| = 1\}$$

A partir de los enteros de Gauss, podemos establecer el conjunto de elementos en $\mathbb{Q}[i]$ que tienen módulo igual a 1, esto es, describir todos los elementos en S.

No es difícil ver que los números de la forma:

$$\frac{m + ni}{k + li} \text{ con } m + ni, k + li \in \mathbb{Z}[i]$$

representan todos los elementos en $\mathbb{Q}[i]$, y en particular, las fracciones con enteros de Gauss:

$$\frac{w}{\overline{w}} = \frac{m + ni}{m - ni}$$

representan elementos en S. En forma más general, los elementos S pueden ser obtenidos como las fracciones:

$$\frac{z}{w} \text{ con } z, w \in \mathbb{Z}[i] : |z| = |w| \neq 0$$

En este caso, partiendo de la identidad:

$$(\overline{z}+w)\,z-(z+\overline{w})\,w=|z|^2-|w|^2$$

si $\overline{z}+w\neq 0$, resulta:

$$\frac{z}{w}=\frac{z+\overline{w}}{\overline{\overline{z}+w}}=\frac{u}{\overline{u}}$$

siendo $u=z+\overline{w}$. Por otra parte, si $\overline{z}+w=0$, la fracción puede representarse como:

$$\frac{z}{w}=\frac{z}{-\overline{z}}=\frac{iz}{\overline{iz}}$$

En consecuencia, todo elemento de S se obtiene como el cociente entre un entero de Gauss y su conjugado. En esta representación, cada entero de Gauss y un múltiplo entero de éste dan lugar al mismo elemento en S, por este motivo, en principio sólo habría que considerar los enteros dados por:

$$m+ni \text{ con } m,n\geq 0 \text{ y } n>0 \text{ si } m=0 \tag{2}$$

donde (m,n) es el máximo común divisor entre m y n.
En el sentido inverso, si $z,w\in\mathbb{Z}[i]$ representan el mismo elementos en S, se tiene:

$$\frac{z}{\overline{z}}=\frac{w}{\overline{w}}, \text{ o bien } z\overline{w}=\overline{z\overline{w}}$$

de donde $z\overline{w}=k\in\mathbb{Z}$ o sea $|w|^2\,z=kw$. Si ponemos $z=m+ni$ y $w=h+li$, con h y l coprimos, de la identidad precedente se tiene:

$$\begin{aligned}\left(h^2+l^2\right)m&=kh\\ \left(h^2+l^2\right)n&=kl\end{aligned} \tag{3}$$

dado que h^2+l^2 es coprimo con h y l, resulta que h es divisor de m y l es divisor de n. Poniendo $m=sh$ y $n=tl$ con $s,t\in\mathbb{Z}$, de las identidades en (3) surge:

$$\left(h^2+l^2\right)s=k=\left(h^2+l^2\right)t$$

luego, $s=t$ y $z=sw$.
Tenemos entonces que los enteros de Gauss en las condiciones de (2) dan una parametrización de la circunferencia racional S.
Sea $w=m+ni$ un entero de Gauss en las condiciones de (2), escribimos la fracción:

$$\frac{w}{\overline{w}}=\frac{m^2-n^2}{m^2+n^2}+\frac{2mn}{m^2+n^2}i$$

como se trata de un número complejo de módulo 1 se tiene:

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

o bien:

$$\left(m^2-n^2\right)^2+(2mn)^2=\left(m^2+n^2\right)^2$$

Resulta que $\left(m^2-n^2,2mn,m^2+n^2\right)$ es una terna pitagórica primitiva, puesto que $(m,n)=1$. De manera que encontramos asociada con elemento en S, una terna pitagórica primitiva.
Recíprocamente, dada una terna pitagórica primitiva (h,k,l) se tiene:

$$h^2+k^2=l^2$$

pero esto es que:

$$\frac{h}{l}+\frac{k}{l}i\in S$$

Esta correspondencia no es unívoca, basta ver que a (h,k,l) y $(-h,-k,-l)$ les corresponden el mismo elemento en S. Recíprocamente, si (h,k,l) y (x,y,z) son termas primitivas tales que:

$$\frac{h}{l}=\frac{x}{z},\ \frac{k}{l}=\frac{y}{z}$$

De la primer igualdad resulta que z divide a lx y l divide a hz, y puesto que $(x,z)=1=(h,l)$, se tiene que $z=\pm l$. Si $z=l$, $x=h$ y $y=k$, y si $z=-l$, entonces $x=-h$, $y=-k$. Se concluye que la correspondencia es dos a uno.
Podemos enunciar entonces el siguiente resultado:

Las ternas pitagóricas (x,y,z) con $z>0$ están en correspondencia biyectiva con los enteros de Gauss en las condiciones de (2).

$$m+ni\longleftrightarrow\left(m^2-n^2,2mn,m^2+n^2\right)$$

Cuaternas Pitagóricas
Las cuaternas pitagóricas son las soluciones enteras de la ecuación:

$$x^2+y^2+z^2=t^2 \tag{4}$$

Una cuaterna pitagórica (x,y,z,t) es *primitiva* si el máximo común divisor entre (x,y,z,t) es igual a 1.

Analizando la ecuación en (4), módulo 4, se podrá ver que t debe ser impar, y sólo uno de los números x, y, z es impar.
Estas cuaternas se asocian con cajas, es decir paralelepípedos rectos, tales que las medidas de sus aristas y de la diagonal interior estén dadas, todas ellas, por números enteros.
Una generación simple de cuaternas pitagóricas puede obtenerse como en el caso de las ternas, por ejemplo:

$$\begin{aligned} 1+3+5 &= 3^2 \\ 1+3+5+7+3^2 &= 5^2 = 4^2+3^2 \\ 1+3+\cdots+23+5^2 &= 13^2 = 12^2+5^2 \\ 13^2 &= 12^2+4^2+3^2 \end{aligned}$$

Es decir, si k es un número natural impar mayor que 1, se tiene

$$\begin{aligned} 1+3+\cdots+(2k-1) &= k^2 \\ 1+3+\cdots+\left(k^2-2\right)+k^2 &= \left(\frac{k^2+1}{2}\right)^2 = \left(\frac{k^2-1}{2}\right)^2 + k^2 \\ 1+3+\cdots+\left(\frac{k^2+1}{2}\right)^2 &= \left(\frac{\left(\frac{k^2+1}{2}\right)^2+1}{2}\right)^2 \\ &= \left(\frac{\left(\frac{k^2+1}{2}\right)^2-1}{2}\right)^2 + \left(\frac{k^2+1}{2}\right)^2 \end{aligned}$$

de donde surge la identidad:

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

Resulta claro que este proceso puede continuarse par obtener *n-uplas pitagóricas*, es decir soluciones enteras de la ecuación:

$$x_1^2 + x_2^2 + \cdots + x_{n-1}^2 = x_n^2 \tag{5}$$

Estas n-uplas también pueden asociarse a cajas en dimensión n, es decir paralelepípedos rectos tales que las medidas de sus aristas y la diagonal mayor estén dadas por números enteros.

Es razonable pensar que, como el caso de los enteros de Gauss, los cuaterniones de Hamilton puedan contribuir a la generación de 5-uplas pitagóricas Estos cuaterniones, que podrían llamarse enteros de Hamilton, son los cuaterniones con coeficientes enteros:

$$\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$$

Para mayores detalles sobre los números cuaterniónicos puede consultarse por ejemplo [4].
Si $w \neq 0$ está en $\mathcal{H}$, el cociente entre w y su conjugado $\overline{w}$ es un cuaternión de módulo 1, esto es:

$$\left|\frac{a + bi + cj + dk}{a - bi - cj - dk}\right| = \left|\frac{\alpha + \beta i + \gamma j + \delta k}{a^2 + b^2 + c^2 + d^2}\right| = 1$$

donde

$$\alpha = a^2 - b^2 - c^2 - d^2,\ \beta = 2ab,\ \gamma = 2ac,\ \delta = 2ad$$

luego

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \left(a^2 + b^2 + c^2 + d^2\right)^2$$

entonces la 5-upla pitagórica asociada con el cuaternión $a + bi + cj + dk$ es:

$$a^2 - b^2 - c^2 - d^2, 2ab, 2ac, 2ad, a^2 + b^2 + c^2 + d^2 \tag{6}$$

como veremos más adelante, las 5-uplas de este tipo no agotarían las 5-uplas pitagóricas.
Pero también los cuaterniones pueden contribuir a la generación de cuaternas pitagóricas. Por ejemplo, los cuaterniones de la forma:

$$wiw^{-1} : w \in \mathcal{H}$$

Dado que $\left|wiw^{-1}\right| = 1$, en forma análoga al trabajo con números complejos, las componentes de este cuaternión podrán asociarse con una cuaterna pitagórica. Si $w = a + bi + cj + dk$ entonces:

$$wiw^{-1} = \frac{a^2 + b^2 - c^2 - d^2}{a^2 + b^2 + c^2 + d^2}i + 2\frac{ad + bc}{a^2 + b^2 + c^2 + d^2}j - 2\frac{ac - bd}{a^2 + b^2 + c^2 + d^2}k \tag{7}$$

En este caso la cuaterna pitagórica asociada con w es:

$$\left(a^2+b^2-c^2-d^2, 2\left(ad+bc\right), -2\left(ac-bd\right), a^2+b^2+c^2+d^2\right) \tag{8}$$

Para establecer un paralelismo con el caso de las ternas pitagóricas, sería en principio razonable saber si podemos identificar los números wiw^{-1} $(w \in \mathcal{H})$, con los puntos de la esfera racional de radio 1 en el espacio $\mathbb{R}^3$. En tal sentido, identificamos cada *cuaternión puro*, es decir un cuaternión w tal que $\overline{w} = -w$, con el punto de $\mathbb{R}^3$ dado por sus coordenadas:

$$xi + yj + zk \longleftrightarrow (x, y, z) \tag{9}$$

Observemos que para cuaterniones puros de módulo 1 se cumple :

$$w^2 = -w\overline{w} = -\left|w\right|^2 = -1$$

Si w es un cuaternión puro con $|w| = 1$ y $w \neq -i$, se tiene:

$$\begin{aligned}
\left(w+i\right) i \left(w+i\right)^{-1} &= \frac{-1}{\left|w+i\right|^2}\left(w+i\right) i \left(w+i\right) \\
&= \frac{w}{\left|w+i\right|^2} w \left(w+i\right) i \left(w+i\right) \\
&= \frac{w}{\left|w+i\right|^2}\left(-1+wi\right)\left(iw-1\right) \\
&= \frac{w}{\left|w+i\right|^2}\left(wi-1\right)\overline{\left(wi-1\right)} \\
&= \frac{\left|\left(w+i\right) i\right|^2}{\left|w+i\right|^2} w = w
\end{aligned} \tag{10}$$

Por otra parte, si $w = -i$:

$$kik^{-1} = -jk = -i$$

Resulta entonces que todo cuaternión puro de módulo 1 puede ser expresado en la forma wiw^{-1}. De esta manera, buscamos parametrizar las esfera racional como se hizo en el caso de las ternas pitagóricas. De acuerdo con la expresión en (7) y la identificación en (9), la correspondencia

$$wiw^{-1} \to \left(\frac{a^2+b^2-c^2-d^2}{a^2+b^2+c^2+d^2}, 2\frac{ad+bc}{a^2+b^2+c^2+d^2}, -2\frac{ac-bd}{a^2+b^2+c^2+d^2}\right) \tag{11}$$

cubre la esfera unitaria en el espacio $\mathbb{R}^3$. De las identidades en (9) resulta:

$$(w+i)\,i\,(w+i)^{-1} = w$$

de modo que si w tiene coordenadas racionales, puede ser obtenido a partir de cuaterniones con coordenadas enteras. En efecto, si $k \in \mathbb{Z}$ es tal que $u = k\,(w+i)$ es un cuaternión con coordenadas enteras, entonces:

$$uiu^{-1} = w$$

Tenemos entonces que la expresión en (11) con a, b, c, d números enteros haría lugar a una parametrización de la esfera unitaria racional y en especial, de las cuaternas pitagóricas primitivas. En efecto, bajo ciertas condiciones sobre los parámetros a, b, c, d, Spira en [5] muestra que la expresión en (9) da una parametrización de las cuaternas pitagóricas.
El paso siguiente es será mostrar que parametrizaciones similares podrían obtenerse para n-uplas pitagóricas, para tal fin, trataremos con matrices o transformaciones ortogonales. Es oportuno destacar que la transformaciones $r\,(z) = wzw^{-1}$ en los cuaterniones puros, se identifican con las rotaciones en $\mathbb{R}^3$, de modo que la parametrización de las cuaternas surge de la acción de las rotaciones, dadas por matrices racionales, en el vector $(1, 0, 0)$ el que se identifica con i según (9).

Observación: Antes de considerar el caso de las n-uplas pitagóricas, hacemos una conexión con la *ecuación de Pell* siguiendo la exposición dada en [2] sobre cajas pitagóricas con una cara cuadrada como base. Esto es cuaternas pitagóricas del tipo (x, x, y, t). En este caso la ecuación puede ponerse como:

$$y^2 = t^2 - 2x^2$$

Esta ecuación es una ecuación de Pell, es decir, ecuaciones del tipo $y^2 = t^2 - kx^2$ dode k es un entero que no es un cuadrado perfecto. Si $y = 1$, hay infinitas soluciones, o sea que hay infinitas cajas pitagóricas que tienen como base un cuadrado de lado igual a 1. En general, la ecuación de Pell tiene solución si, y sólo si, $y = \pm 1$ o es producto de números primos de la forma $8k \pm 1$, ver [1].

Las n-uplas Pitagóricas
Cada n-upla pitagórica $(x_1, \ldots, x_{n-1}, x_n)$ se asocia con el punto

$$\left(\frac{x_1}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right)$$

en la esfera racional unitaria, es decir, con los puntos de coordenadas racionales de norma o longitud igual a 1. Si nos limitamos a las n-uplas pitagóricas primitivas, esto es, como el máximo común divisor de sus elementos igual a 1, esta correspondencia es dos a uno. En efecto, notemos primero que si $(x_1, \ldots, x_{n-1}, x_n)$ es primitiva, de la igualdad:

$$x_1^2 + \cdots + x_{n-1}^2 = x_n^2$$

se sigue que el máximo común divisor de $x_1, \ldots, x_{n-1}$ es 1, luego existen enteros $z_1, \ldots, z_{n-1}$ tales que:

$$x_1 z_1 + \cdots + x_{n-1} z_{n-1} = 1$$

Supongamos que $(y_1, \ldots, y_{n-1}, y_n)$ es una n-upla pitagórica tal que:

$$\left(\frac{x_1}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right) = \left(\frac{y_1}{y_n}, \ldots, \frac{y_{n-1}}{y_n}\right)$$

esto es:

$$y_n \left(x_1, \ldots, x_{n-1}\right) = x_n \left(y_1, \ldots, y_{n-1}\right)$$

haciendo el producto escalar miembro a miembro por $(z_1, \ldots, z_{n-1})$ resulta:

$$y_n = x_n \left(y_1 z_1 + \cdots + y_{n-1} z_{n-1}\right)$$

luego x_n divide a y_n y se tiene la igualdad:

$$\left(y_1, \ldots, y_{n-1}\right) = \frac{y_n}{x_n} \left(x_1, \ldots, x_{n-1}\right)$$

Si además $(y_1, \ldots, y_{n-1})$ es primitiva, por el mismo argumento, y_n divide a x_n, es decir $y_n = \pm x_n$ y en consecuencia:

$$\left(y_1, \ldots, y_{n-1}, y_n\right) = \pm \left(x_1, \ldots, x_{n-1}, x_n\right)$$

A partir de este hecho, resultará interesante obtener expresiones que representen los puntos de la esfera racional unitaria. Para este fin, se considerará a continuación la generación de matrices ortogonales con coeficientes racionales y la acción de éstas sobre una esfera racional.

Reflexiones

En el espacio euclídeo $\mathbb{R}^n$ con producto interno usual $\langle\ ,\rangle$, se puede considerar el *grupo ortogonal* $O_n(\mathbb{R})$, dado por el conjunto de las *transformaciones ortogonales*, es decir, las transformaciones lineales de $\mathbb{R}^n$ que conservan las distancias, o equivalentemente, las transformaciones lineales que preservan el producto interno o la longitud. De modo que, si indicamos los endomorfismos de $\mathbb{R}^n$ con $End(\mathbb{R}^n)$ se tiene;

$$\begin{aligned} O(V) &= \{\sigma \in End(\mathbb{R}^n) : \langle \sigma(v), \sigma(w)\rangle = \langle v, w\rangle, \forall v, w \in \mathbb{R}^n\} \\ &= \{\sigma \in End(\mathbb{R}^n) : \|\sigma(v)\| = \|v\|, \forall v \in \mathbb{R}^n\} \end{aligned}$$

Las matrices asociadas a transformaciones ortogonales en una base ortonormal, son *matrices ortogonales*, es decir matrices que satisfacen las identidad:

$$^tA = A^{-1}$$

La reflexión ortogonal es una transformación ortogonal, asociada a un vector no nulo α que viene definida por la fórmula:

$$r_\alpha(v) = v - 2\frac{\langle v, \alpha\rangle}{\langle \alpha, \alpha\rangle}\alpha \tag{12}$$

Para establecer que r_α es una transformación ortogonal, es suficiente mostrar que:

$$\|r_\alpha(v)\| = \|v\| \qquad \forall v \in V$$

Si se tiene en cuenta los vectores ortogonales $p = v - \frac{\langle v,\alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha$ y $q = -\frac{\langle v,\alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha$, resulta:

$$r_\alpha(v) = p + q \quad \text{y} \quad v = p - q$$

luego:

$$\|r_\alpha(v)\|^2 = \|p\|^2 + \|q\|^2 = \|v\|^2$$

En el plano $\mathbb{R}^2$, la reflexión asociada con α, es la simetría respecto de la recta perpendicular a α que pasa por el origen. En el espacio $\mathbb{R}^3$, es la simetría respesto del plano perpendicular a α que pasa por el origen.
Es conocido que las reflexiones generan el grupo ortogonal, en realidad, no es difícil mostrar que cada transformación ortogonal en $\mathbb{R}^n$ se descompone como composición de a lo sumo n reflexiones.

Proposición 1. Sean u y v en $\mathbb{R}^n$ vectores con la misma longitud. Entonces, si $\alpha = u - v$, la reflexión r_α intercambia los vectores u y v.

Demostración: Sea $\beta = u + v$, como u y v tienen la misma longitud, α y β son vectores ortogonales, luego por la expresión en (12) resulta:

$$r_\alpha(\beta) = \beta \quad \text{y} \quad r_\alpha(\alpha) = -\alpha$$

de modo que:

$$r_\alpha(u) = r_\alpha\left(\frac{\alpha+\beta}{2}\right) = \frac{-\alpha+\beta}{2} = v$$

La identidad $r_\alpha(v) = u$, sigue del hecho $r_\alpha \circ r_\alpha = id_{\mathbb{R}^n}$, el cuál se puede establecer sin mayor dificultad desde la definición de r_α en (12).

Nota: Esta proposición garantiza que dos puntos en una esfera, con centro en el origen, pueden ser conectados mediante una transformación ortogonal. Dicho de otro modo, pensando en coordenadas cartesianas, si $(x_1, \ldots, x_n)$ y $(y_1, \ldots, y_n)$ en $\mathbb{R}^n$ tienen la misma norma, entonces existe una matriz ortogonal $O \in \mathbb{R}^{n\times n}$ tal que:

$$O\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

El resultado se mantiene para esferas racionales, es decir; si $(x_1, \ldots, x_n)$ y $(y_1, \ldots, y_n)$ en $\mathbb{Q}^n$ tienen la misma norma, entonces existe una matriz ortogonal $A \in \mathbb{Q}^{n\times n}$ que transforma uno en otro. Esto se debe al hecho que la matriz de la reflexión r_α asociada a la base canónica tiene entradas racionales, para $\alpha = (x_1 - y_1, \ldots, x_n - y_n)$.
Por ejemplo, si se consideran los puntos $(1, 2, 3)$ y $(3, 1, 2)$, será $\alpha = (-2, 1, 1)$ y la matriz de r_α asociada a la base canónica es:

$$\begin{bmatrix} -\frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

Del análisis precedente podemos concluir que los puntos en la esfera racional unitaria pueden ser representados como:

$$O\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} : O \in O_n(\mathbb{Q}) \tag{13}$$

aquí $O_n(\mathbb{Q})$ denota el grupo de las matrices ortogonales con coeficientes racionales.

Parametrización de Cayley
Un importante conjunto de matrices ortogonales pueden ser parametrizadas por matrices antisimétricas mediante la expresión dada en (14) debida a Cayley.

Proposición 2: Sea A una matriz real antisimétrica de orden n. El único posible valor propio real de A es 0.
Demostración: De la ecuación:

$$Ax = \lambda x \qquad x \in \mathbb{R}^n, \lambda \in \mathbb{R}$$

multiplicano ambos miembros por ${}^t x$, el traspuesto de x, se tiene:

$${}^t xAx = \lambda {}^t xx = \lambda \|x\|^2$$

pero por ser A antisimétrica ${}^t xAx = 0$ y en consecuencia.$\lambda = 0$ si $x \neq 0$.
Sea O la matriz dada por:

$$O = (A+I)(A-I)^{-1} = (A-I)^{-1}(A+I) \tag{14}$$

donde I es la matriz identidad.
Hay un par de acotaciones que hacer respecto de la definición de O. En primer lugar, la matriz $A - I$ es inversible, ya que en caso contrario su determinante sería igual a 0 y 1 un valor propio de A, pero en virtud de la proposición 2, esto no es posible . En segundo lugar, las matrices $A+I$ y $(A-I)^{-1}$ conmutan debido a que $A + I$ y $A - I$ claramente conmutan y no es difícil ver que si una matriz conmuta con otra, también conmuta con la inversa.
Usando propiedades de la traspuesta de una matriz, en especial que conmuta con la inversión, se tiene:

$$\begin{aligned} {}^t O &= {}^t\left((A+I)(A-I)^{-1}\right) \\ &= {}^t\left((A-I)^{-1}\right)^t (A+I) \\ &= (-A-I)^{-1}(-A+I) \\ &= (A+I)^{-1}(A-I) = O^{-1} \end{aligned} \tag{15}$$

Es oportuno notar que O no tiene a 1 como valor propio, es decir $\det(O-I) \neq 0$. En efecto:

$$\begin{aligned} O - I &= (A+I)(A-I)^{-1} - I \\ &= (A + I - (A-I))(A-I)^{-1} \\ &= 2(A-I)^{-1} \end{aligned}$$

En el sentido inverso, si partimos de una matriz ortogonal O tal que 1 no es valor propio de O, entonces la matriz:

$$A = (O+I)(O-I)^{-1} = (O-I)^{-1}(O-I)$$

es antisimétrica Esta afirmación se comprueba en forma análoga a lo hecho en (15).
Las propociones dadas a continuación muestran que esta parametrización cubre una parte importante del grupo ortogonal. Estos resultados pueden verse en [3].
Usaremos $\mathcal{D}_n$ para denotar el conjunto de todas las matrices diagonales de orden n que tienen ± 1 en la diagonal principal. Notar que $\mathcal{D}_n$ tiene 2^n elementos los cuales son matrices ortogonales.

Proposición 3. Dada una matriz B de orden n existe una matriz $D \in \mathcal{D}_n$ tal que $B - D$ es inversible.
Demostración: Se hará por inducción en el orden n de la matrices. Si $n = 1$, es claro. Si $n > 1$, descomponemos B en bloques

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \\ b_{n1} & & \end{bmatrix}$$

donde $C = [b_{ij}]_{2 \leq i,j \leq n}$. Por la hipótesis inductiva, existe una matriz $D' \in \mathcal{D}_{n-1}$ tal que $C - D'$ es inversible. Si consideramos las matrices en $\mathcal{D}_n$ dadas por:

$$D_{\pm} = \begin{bmatrix} \pm 1 & \cdots & 0 \\ \vdots & & \\ 0 & & \end{bmatrix}$$

se tiene:

$$B - D_{\pm} = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \\ b_{n1} & & C \end{bmatrix} - \begin{bmatrix} \pm 1 & \cdots & 0 \\ \vdots & & \\ 0 & & D \end{bmatrix}$$
$$= \begin{bmatrix} b_{11} \pm 1 & \cdots & b_{1n} \\ \vdots & & \\ b_{n1} & & C - D \end{bmatrix}$$

luego, por propiedades del determinante, es:

$$\det(B - D_{\pm}) = \det \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \\ b_{n1} & & C - D \end{bmatrix} \pm \det \begin{bmatrix} 1 & \cdots & b_{1n} \\ \vdots & & \\ 0 & & C - D \end{bmatrix}$$

como el segundo término es igual a $\det(C - D) \neq 0$, la suma y la resta en el segundo miembro toman valores distintos, entonces al menos uno de ellos es distinto de 0, es decir uno de los valores $\det(B - D_+)$ o $\det(B - D_-)$ es distinto de cero.
La siguiente proposición se enuncia conservando las notaciones precedentes

Proposición 4. Sea O una matriz ortogonal. Existe $D \in \mathcal{D}$ tal que OD no tiene a 1 como valor propio.
Demostración: Teniendo en cuenta que $D^2 = D$, cualquiera sea $D \in \mathcal{D}$, podemos poner:

$$\begin{aligned} \det(OD - I) &= \det((O - D)D) \\ &= \det(O - D) \det D = \pm \det(O - D) \end{aligned}$$

en consecuencia, bastará elegir D de modo que $O - D$ sea inversible.
Esta última proposición muestra que la parametrización de las matrices ortogonales por las matrices simétricas alcanzan al menos una de las 2^n matrices de la forma OD con $D \in \mathcal{D}_n$. Por ejemplo, si $O = I$, $-I$ es la única matriz en $\mathcal{D}_n$ alcanzada por esta parametrización.

Nota: Según la parametrización de Cayley en (14), matrices antisimétricas racionales, se corresponden con matrices con matrices ortogonales racionales y

recíprocamente. Ahora, teniendo en cuenta la proposición 4, los elementos en $O_n(\mathbb{Q})$ pueden ser representados como:

$$D(A+I)(A-I)^{-1} : D \in \mathcal{D}_n,\ A \in \mathbb{Q}^{n\times n},\ {}^tA = -A \tag{16}$$

La condición $A \in \mathbb{Q}^{n\times n}$ puede ser modificada. Sea $d \in \mathbb{Z}$ tal que $dA \in \mathbb{Z}^{n\times n}$, entonces:

$$(A+I)(A-I)^{-1} = (dA+dI)(dA-dI)^{-1}$$

es decir (16) puede reformularse como:

$$D(B+dI)(B-dI)^{-1} : D \in \mathcal{D}_n,\ B \in \mathbb{Z}^{n\times n},\ {}^tB = -B,\ d \in \mathbb{Z} \tag{17}$$

Por ejemplo, para $n = 3$, (17) resulta:

$$\begin{bmatrix} \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \end{bmatrix} \begin{bmatrix} d & a & b \\ -a & d & c \\ -b & -c & d \end{bmatrix} \begin{bmatrix} -d & a & b \\ -a & -d & c \\ -b & -c & -d \end{bmatrix}^{-1}$$

donde $a, b, c, d \in \mathbb{Z}$, o bien:

$$\begin{bmatrix} \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \end{bmatrix} \begin{bmatrix} \frac{a^2+b^2-c^2-d^2}{a^2+b^2+c^2+d^2} & -2\frac{ad-bc}{a^2+b^2+c^2+d^2} & -2\frac{ac+bd}{a^2+b^2+c^2+d^2} \\ 2\frac{ad+bc}{a^2+b^2+c^2+d^2} & \frac{a^2-b^2+c^2-d^2}{a^2+b^2+c^2+d^2} & 2\frac{ab-cd}{a^2+b^2+c^2+d^2} \\ -2\frac{ac-bd}{a^2+b^2+c^2+d^2} & 2\frac{ab+cd}{a^2+b^2+c^2+d^2} & -\frac{a^2-b^2-c^2+d^2}{a^2+b^2+c^2+d^2} \end{bmatrix}$$

y según (13), una expresión para los puntos de la esfera racional unitaria estará dada por:

$$\left(\pm\frac{a^2+b^2-c^2-d^2}{a^2+b^2+c^2+d^2}, \pm2\frac{ad+bc}{a^2+b^2+c^2+d^2}, \pm2\frac{ac-bd}{a^2+b^2+c^2+d^2}\right)$$

que es prácticamente la obtenida a partir de los cuaterniones.
Para $n = 4$, salvo signos, se obtienen las 5-uplas dadas por:

$$\begin{aligned} x_1 &= a^2g^2 + a^2h^2 - 2abfg + 2acdg + b^2f^2 + b^2h^2 \\ &\quad -2bcdf + c^2d^2 + c^2h^2 - d^2h^2 - f^2h^2 - g^2h^2 - h^4 \\ x_2 &= 2ah^3 + 2bdh^2 + 2ag^2h + 2cfh^2 + 2cdgh - 2bfgh \\ x_3 &= 2bh^3 - 2adh^2 + 2bf^2h + 2cgh^2 - 2cdfh - 2afgh \\ x_4 &= 2ch^3 - 2afh^2 + 2cd^2h - 2bgh^2 + 2adgh - 2bdfh \\ x_5 &= a^2g^2 + a^2h^2 - 2abfg + 2acdg + b^2f^2 + b^2h^2 \\ &\quad -2bcdf + c^2d^2 + c^2h^2 + d^2h^2 + f^2h^2 + g^2h^2 + h^4 \end{aligned}$$

Seguramente más soluciones que las obtenidas en (6) usando los cuaterniones.

Referencias

[1] Adler A., Coury J., *The Theory of Numbers.* A Text and Source Book of Problems (1995).

[2] Beauregard, R.A. and Suryanarayan E. R., *Pythagorean boxes*, Math. Magazine 74 (2001), 222–227.

[3] Liebeck; H., Osborne, A., *The Generation of All Rational Orthogonal Matrices.* The American Mathematical Monthly, Vol. 98, No. 2. (Feb., 1991), pp. 131-133.

[4] Kuipers, J. B. *Quaternios and Rotations Sequences.* Geometry, Intregrability and Quantization. September 1-10, 1999. Varma, Bulgaria. Disponible en http://www.emis.de/proceedings/Varna/vol1/GEOM09.pdf

[5] Spira, R. *The diophantine equation* $x^2+y^2+z^2 = m^2$, Amer. Math. Monthly 69 (1962), 360–365.

Facultad de Ciencias Exactas - UNCPBA