Ecuación de Pell

Ian Castellanos

Historia

- Poema del ganado del rey Sol escrito por Arquímedes, enviado a Eratóstenes.
- 1653 d.C.- Desafío de Fermat: demostrar que $x^2 - dy^2 = 1, d > 1$ tiene un número infinito de soluciones.
- Wallis y Brouncker proponen un conjunto de métodos de solución, pero no llegan a demostrar la conjetura. Los métodos están relacionados a fracciones continuas de $\sqrt{d}$
- 1768 d.C.- Lagrange demuestra que los métodos de Wallis y Brouncker siempre tienen solución.

Casos triviales de la ecuación de Pell

- $\forall d \in \mathbb{Z}, x^2 - dy^2 = 1\ se\ satisface\ de\ manera\ trivial\ con\ x = \pm 1\ \&\ y = 0$
- $Si\ d < -1 \Rightarrow x^2 - dy^2 \geq 1\ [excepto\ en\ el\ caso\ x = y = 0]$
- $d = -1 \Rightarrow x = 0, y = \pm 1$
- $d = n^2 \Rightarrow x^2 - dy^2 = 1 \Rightarrow (x + ny)(x - ny) = 1$

$$\Leftrightarrow x + ny = x - ny = \pm 1 \Rightarrow x = \frac{(x + ny)(x - ny)}{2} = \pm 1$$

$$\&\ la\ ecuación\ no\ tiene\ soluciones\ aparte\ de\ la\ trivial:$$

$$x = \pm 1, y = 0.$$

$$Porque: (x + ny) + (x - ny) = 2 \Rightarrow 2x = 2 \Rightarrow x = 1$$

Casos triviales de la ecuación de Pell

- De lo anterior se tiene que el caso considerado en adelante es aquel en que $d \in \mathbb{Z} \ni d \neq n^2$ $(d\ es\ irracional)$, con el fin de tener más soluciones además de la trivial.
- Además, se restringen las soluciones de $x^2 - dy^2 = 1$ a soluciones positivas $x, y > 0$ puesto que, cuando $y > 0$ se tienen conjuntos de cuatro combinaciones: $\pm x, \pm y$.
- De esta manera se buscan solo las positivas porque al conocer estas se conoce el resto.

Teoremas asociados

- **Teorema 1**: p, q *solución postitiva de* $x^2 - dy^2 = 1$

$\Rightarrow \frac{p}{q}$ *es un convergente de la expansión de fracciones continuas de* $\sqrt{d}$

Demostración:Quitar essta demostración

$p, q > 0$, *por hipótesis se tiene* $p^2 - dq^2 = 1$

$$\Rightarrow (p - q\sqrt{d})(p + q\sqrt{d}) = 1$$

Sea $p > q$

$$\Rightarrow \frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})}$$

$$\Rightarrow 0 < \frac{p}{q} - \sqrt{d} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{2q^2\sqrt{d}} = \frac{1}{2q^2}$$

Teoremas asociados

- $Se\ considera\ el\ teorema: x\ irracional\ arbitrario. Si\ \frac{a}{b} \in \mathbb{Q}, b \geq 1\ \&\ (a,b) = 1\ satisface: \left|x - \frac{a}{b}\right| < \frac{1}{2b^2} \Rightarrow$ $\frac{a}{b} es\ un\ convergente\ \frac{p_n}{q_n}\ de\ la\ expansión\ de\ x$

$\Rightarrow Por\ teorema\ anterior, \frac{p}{q} es\ un\ convergente\ de\ \sqrt{d}$

Q.E.D

Importante: En general, la recíproca del teorema anterior es falsa.

- El teorema siguiente brinda información del tamaño de los valores de $\mathrm{k} = p_n^2 - dq_n^2$

Teoremas asociados

- **Teorema 2:** $\frac{p}{q} es\ convergente\ de\ la\ expansión\ de\ \sqrt{d} \Rightarrow$

$x = p, y = q\ es\ una\ solución\ de\ las\ ecuaciones$:

$$x^2 - dy^2 = k, |k| < 1 + 2\sqrt{d}.$$

Demostración:(quitar esta demostración)

$Sea \frac{p}{q}\ un\ convergente\ de\ \sqrt{d}$

$\Rightarrow dado\ que\ por\ corolario \frac{p_n}{q_n}\ es\ el\ n\ ésimo\ convergente\ del\ irracional\ \sqrt{d}$

$\Rightarrow \left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}(I)$

$\Rightarrow \left|p - q\sqrt{d}\right| < \frac{1}{q}$

$\Rightarrow \left|p + q\sqrt{d}\right| = \left|\left(p - q\sqrt{d}\right) + 2q\sqrt{d}\right| \leq \left|p - q\sqrt{d}\right| + \left|2q\sqrt{d}\right| < \frac{1}{q} + 2q\sqrt{d} \leq \left(1 + 2\sqrt{d}\right)q\ (II)$

$\Rightarrow Se\ combinan\ las\ ecuaciones\ (I)\ \&\ (II)\ como\ sigue$:

$|p^2 - dq^2| = \left|p - q\sqrt{d}\right|\left|p + q\sqrt{d}\right| \leq \frac{1}{q}\left(1 + 2\sqrt{d}\right)q = 1 + 2\sqrt{d}$

Q.E.D.

Ejemplo 1

$Sea\ d = 7, con\ expansión\ en\ fracciones\ continuas\ de\ \sqrt{7}$

$= [2; \overline{1,1,1,4}]\ cuyos\ primero\ convergentes\ son: \frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3} \ldots$

$\Rightarrow p_n^2 - 7q_n^2$

$\Rightarrow El\ teorema\ 2\ estipula\ que\ x = p_n\ \&\ y = q_n$

$Las\ posibles\ respuestas\ son\ entonces, con\ 1 + 2\sqrt{7} \approx 6.2915$

- $2^2 - 7(1)^2 = -3$
- $3^2 - 7(1)^2 = 2$
- $5^2 - 7(2)^2 = -3$
- $8^2 - 7(3)^2 = 1$

$\therefore el\ único\ convergente\ que\ cumple\ con\ x^2 - 7y^2 = 1\ es\ x = 8\ \&\ y = 3$

La estructura de la expansión en fracciones continuas de $\sqrt{d}$

$Sea\ d \in \mathbb{Z}^+ \ni d\ no\ es\ un\ cuadrado\ perfecto, se\ tiene\ que$
$la\ expansión\ en\ fracciones\ continuas\ del\ mismo\ tiene\ la\ forma$

$$\sqrt{d} = [a_0; \overline{a_1, a_2, a_3, \dots, a_3, a_2, a_1, 2a_0}], a_1 = \lfloor \sqrt{d} \rfloor$$

$Por\ teorema\ 1, se\ tiene\ que\ x^2 - dy^2 = 1\ tiene\ solución$
$\Rightarrow tiene\ soluciones\ positivas\ x = p_k\ \&\ y = q_k$
$\ni \frac{p_k}{q_k}\ convergente\ de\ \sqrt{d}$

La estructura de la expansión en fracciones continuas de $\sqrt{d}$

Asimismo se tiene que el período n de la expansión de $\sqrt{d}$ *provee información necesaria para mostrar que* $x^2 - dy^2 = 1$ *tiene solución en* $\mathbb{Z}$.

Estas soluciones son en realidad infinitas y obtenidas de $\frac{p_k}{q_k}$.

Se tiene que $\sqrt{d} = [a_0; a_1, a_2, \dots]$ *se obtienen al definir*:

$$x_0 = \sqrt{d} \ \ \& \ \ x_{k+1} = \frac{1}{x_k - [x_k]}, \qquad k \in \mathbb{N}$$

La estructura de la expansión en fracciones continuas de $\sqrt{d}$

El propósito de los siguientes teoremas es el de establecer que:

Si n es la longitud del período para $\sqrt{d}$

$\Rightarrow \frac{p_{kn-1}}{q_{kn-1}}\ satisface\colon\ p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn}$

Lema 1

$$Sea\ \sqrt{d} = [a_0; a_1, a_2, \dots]\ se\ consideran\ s_0 = 0, t_0 = 1,$$

$$s_{k+1} = a_k t_k - s_k, \qquad t_{k+1} = \frac{d - s_{k+1}^2}{t_k}, \qquad k \in \mathbb{N}$$

$Entonces\ se\ cumple\ lo\ siguiente$:

$a)\ \ s_k, t_k \in \mathbb{Z}, t_k \neq 0$

$b)\ \ t_k | (d - s_k^2)$

$c)\ \ x_k = \frac{s_k + \sqrt{d}}{t_k},\ \ k \geq 0$

- Este lema se demuestra por inducción.

Teorema 3

$\frac{p_k}{q_k}$ $convergentes\ de\ la\ expansión\ de\ \sqrt{d}$

$\Rightarrow p_k^2 - dq_k^2 = (-1)^{(k+1)} t_{k+1}, \qquad t_{k+1} > 0, \qquad k = 0,1,2,3, \ldots$

Demostración: (quitar demostración)

$Para\ \sqrt{d} = [a_0; a_1, \ldots, a_k, x_{k+1}] se\ sabe\ que\ \sqrt{d} = \frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}}$

$Se\ sustituye\ x_{k+1} = \frac{s_{k+1} + \sqrt{d}}{t_{k+1}}\ en\ la\ expresión\ anterior$:

$$\sqrt{d} = \frac{\frac{s_{k+1} + \sqrt{d}}{t_{k+1}} * p_k + p_{k-1}}{\frac{s_{k+1} + \sqrt{d}}{t_{k+1}} * q_k + q_{k-1}}$$

$Se\ simplifica\ entonces\ en$:

$\sqrt{d}(s_{k+1}q_k + t_{k+1}q_{k-1} - p_k) = s_{k+1}p_k + t_{k+1}p_{k-1} - dq_k$

$Se\ tiene\ que\ la\ parte\ derecha\ es\ racional\ y\ \sqrt{d}\ es\ irracional$

$por\ lo\ que\ se\ tiene\ que$:

$s_{k+1}q_k + t_{k+1}q_{k-1} = p_k\ \&\ s_{k+1}p_k + t_{k+1}p_{k+1} = dq_k$

$\Rightarrow p_k(s_{k+1}q_k + t_{k+1}q_{k-1}) = p_k p_k\ \&\ -q_k(s_{k+1}p_k + t_{k+1}p_{k+1}) = dq_k(-q_k)$

$\Rightarrow p_k(s_{k+1}q_k + t_{k+1}q_{k-1}) + (-q_k)(s_{k+1}p_k + t_{k+1}p_{k+1}) = \mathrm{p}_\mathrm{k}^2 - dq_k^2$

$= t_{k+1}(p_k q_{k-1} - p_{k-1}q_k)$

$Por\ teorema\ (15.3\ en\ Burton),\qquad p_k q_{k-1} - p_{k-1}q_k = (-1)^{k-1} = (-1)^{k+1}$

$\Rightarrow p_k^2 - dq_k^2 = (-1)^{k+1}t_{k+1}$

$Por\ propiedades\ de\ convergentes\ se\ tiene\ C_{2k} < \sqrt{d} < C_{2k+1},\qquad k \geq 0$

$Dado\ que\ C_k = \dfrac{p_k}{q_k}$

- $p_k^2 - dq_k^2 > 0, k\ impar$
- $p_k^2 - dq_k^2 < 0, k\ par$

Se tiene $\frac{p_k^2 - dq_k^2}{p_{k-1}^2 - dq_{k-1}^2} = -\frac{t_{k+1}}{t_k},\ k \geq 1$

$$\Rightarrow \frac{p_k^2 - dq_k^2}{p_{k-1}^2 - dq_{k-1}^2} < 0 \ \& \ 0 < -\frac{t_{k+1}}{t_k}$$

$Se\ tiene\ entonces\ t_1 = d - a_0^2 > 0$
$\Rightarrow t_{k+1} > 0$

Q.E.D

Corolario:

$Si\ n\ es\ la\ longitud\ del\ período\ de\ la\ expansión\ de\ \sqrt{d}, entonces$
$t_j = 1 \Leftrightarrow n|j$

Ejemplo 2

$Sea\ \sqrt{15} = [3; \overline{1, 6}] \Rightarrow n = 2$

Se tienen los primeros cuatro convergentes:

$$C_1 = \frac{3}{1}, \qquad C_2 = \frac{4}{1}, \qquad C_3 = \frac{27}{7}, \qquad C_4 = \frac{31}{8}$$

Por teorema 2:

$$3^2 - 15 * 1^2 = 27^2 - 15 * 7^2 = -6$$
$$4^2 - 15 * 1^2 = 31^2 - 15 * 8^2 = 1$$

Por corolario $2|2\ \ \&\ \ 2|4$

$$\Rightarrow t_1 = t_3 = 6, \qquad t_2 = t_4 = 1$$

Teorema 4

$Sea\ \frac{p_k}{q_k}\ convergentes\ de\ la\ expansión\ \sqrt{d}\ y\ sea\ n\ la\ longitud\ de\ la\ expansión.$

- $Si\ n\ es\ par \Rightarrow todas\ las\ soluciones\ positivas\ de\ x^2 - dy^2 = 1\ son:$

$$x = p_{kn-1}\ \&\ y = q_{kn-1}, \qquad k = 1,2,3, \ldots$$

- $Si\ n\ es\ impar \Rightarrow todas\ las\ soluciones\ positivas\ de\ x^2 - dy^2 = 1\ son:$

$$x = p_{2kn-1}\ \&\ y = q_{2kn-1}, \qquad k = 1,2,3, \ldots$$

Demostración: (este si se va a demostrar)

$Por\ teorema, se\ tiene\ que\ toda\ solución\ x_0 = p_j, yo = q_j$
$para\ algún\ convergente\ \frac{p_j}{p_j}\ de\ \sqrt{d}.$
$Por\ teorema\ anterior\ p_j^2 - dq_j^2 = (-1)^{j+1} t_{j+1}$
$\Rightarrow j+1\ es\ par\ \&\ t_{j+1} = 1\ con\ el\ fin\ que\ quede\ la\ forma\ de\ e.Pell$
$\Rightarrow n|(j+1)\ por\ corolario$
$\Rightarrow j+1 = nk, para\ algún\ k$
$Si\ n\ es\ impar \Rightarrow k\ es\ par.$
$Si\ n\ es\ par \Rightarrow cualquier\ valor\ de\ k\ basta\ para\ resolverlo.$

Q.E.D.

Ejemplo 3

$$Sea\ x^2 - 7y^2 = 1, \qquad \sqrt{7} = [2; \overline{1,1,1,4}]$$

$\Rightarrow los\ primeros\ 10\ convergentes\ son$:

$$\frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{18}{5}, \frac{119}{33}, \frac{137}{38}, \frac{256}{71}, \frac{393}{109}, \frac{649}{180}$$

$$\Rightarrow x = p_{10k-1} \quad y = q_{10k-1}, \qquad k = 1,2,3, \ldots$$

$$x = p_9 = 649, \quad y = q_9 = 180$$

La solución fundamental

$Es\ la\ menor\ solución\ positiva\ x_0, y_0 \ni x_0 < x' \& y_0 < y' \forall x', y'$

- $Por\ teorema\ 3, se\ tiene\ que\ x^2 - dy^2 = 1$
  $tiene\ soluciones\ en\ n\ o\ 2n\ pasos.$
- Con este concepto se busca generar de manera más rápida las soluciones de la ecuación de Pell.
- Los siguientes teoremas buscan un proceso sencillo para el cálculo de las soluciones a partir de la solución fundamental.

Teorema 5

$Sea\ x_1, y_1 la\ solución\ fundamental\ de\ x^2 - dy^2 = 1.$
$\Rightarrow \forall x_n, y_n \in \mathbb{Z}\ definidas\ por$
$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, \qquad n = 1,2,3, \ldots$
$son\ una\ solución\ positiva.$

Demostración:
$Se\ tienen\ x_1, y_1 > 0\ \&\ x_n, y_n \in \mathbb{Z}^+$
$Se\ considera\ asimismo\ que\ x_1^2 - dy_1^2 = 1\ por\ definición$
$x_n^2 - dy_n^2 = \left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) = \left(x_1 + y_1\sqrt{d}\right)^n\left(x_1 - y_1\sqrt{d}\right)^n$
$= (x_1^2 - dy_1^2)^n = 1^n = 1$
$\therefore x_n^2 - dy_n^2 = 1\ \&\ x_n, y_n\ es\ una\ solución\ positiva.$

Q.E.D.

Teorema 5

$Si\ x_1, y_1 es\ la\ solución\ fundamental, entonces\ para\ toda\ solución\ positiva\ x_n, y_n \in \mathbb{Z}\ están\ determinados\ por:$

$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n \quad n = 1,2,3, \ldots$

Demostración:

$Ad\ absurdum, la\ solución\ u, v\ no\ se\ obtiene\ a\ través\ de$

$\left(x_1 + y_1\sqrt{d}\right)^n \ni \left(x_1 + y_1\sqrt{d}\right)^n < u + v\sqrt{d} < \left(x_1 + y_1\sqrt{d}\right)^{n+1}$

$\Rightarrow x_n + y_n\sqrt{d} < u + v\sqrt{d} < \left(x_n + y_n\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)$

$\left(x_n - y_n\sqrt{d}\right)\left(x_n + y_n\sqrt{d}\right) < \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right)$

$< (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d})(x_n - y_n\sqrt{d})$

$Dado\ que\ x_n^2 - dy_n^2 = 1\ \ se\ tiene$

$1 < \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right) < x_1 + y_1\sqrt{d}$

$Se\ definen\ las\ siguientes\ expesiones\ de\ s, r \in \mathbb{Z}$

$r + s\sqrt{d} = (x_n - y_n\sqrt{d})(u + v\sqrt{d})$

$Sean:\ \ r = x_n u - y_n v d \quad\ s = x_n v - y_n u$

$\Rightarrow r^2 - ds^2 = (x_n^2 - dy_n^2)(u^2 - dv^2) = 1:$

$1 < r + s\sqrt{d} < x_1 + y_1\sqrt{d}$

$Se\ procede\ a\ demostrar\ que\ r, s\ son\ soluciones\ positivas:$

$Si\ 1 < r + s\sqrt{d}\ \&\ \left(r + s\sqrt{d}\right)\left(r - s\sqrt{d}\right) = 1 \Rightarrow 0 < r - s\sqrt{d} < 1$

$\Rightarrow 2r = \left(r + s\sqrt{d}\right) + \left(r - s\sqrt{d}\right) > 1 + 0 > 0$

$\Rightarrow 2s\sqrt{d} = \left(r + s\sqrt{d}\right) - \left(r - s\sqrt{d}\right) > 1 - 1 = 0$

$\Rightarrow r, s > 0\ \&\ x_1 < r\ \&\ y_1 < s$

$\Rightarrow x_1 + y_{1\sqrt{d}} < r + s\sqrt{d}\ (\rightarrow\leftarrow)$

Q.E.D.

Ejemplo

- Determinación de números que son triangulares y cuadrados al mismo tiempo.

$$n^2 = \frac{m(m+1)}{2}, \qquad n, m \in \mathbb{Z}$$

$$8n^2 = 4m(m+1) = 4m^2 + 4m = (2m+1)^2 - 1$$
$$\Rightarrow x = 2m + 1 \ \& \ y = 2n$$
$$\Rightarrow 2y^2 = x^2 - 1$$
$$\Rightarrow x^2 - 2y^2 = 1$$

Perspectiva algebraica

- Se define $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$
- $\mathbb{Z}[\sqrt{d}]$ es un anillo conmutativo con $1 = 1 + 0\sqrt{d}$

- Se busca describir las unidades de $\mathbb{Z}[\sqrt{d}]$.

- Conjugado: $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ entonces su conjugado es $a - b\sqrt{d}$

- Norma: La norma de $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ es el entero:

$$N(x + y\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

Perspectiva algebraica

- La solubilidad de la ecuación de Pell $x^2 - dy^2 = 1$ es equivalente a describir los elementos del anillo $\mathbb{Z}[\sqrt{d}]$ con norma 1:

$$N(x + y\sqrt{d}) = x^2 - dy^2 = 1$$