Ecuaciones Diofantinas II: Ecuación de Pell

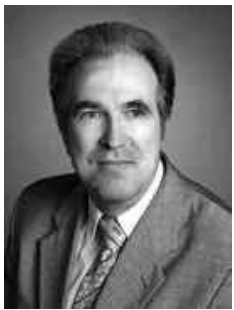
Majo Gil

Teoría de Números

Contexto histórico

Recordemos que existen varios tipos de ecuaciones diofánticas, ya que estas dependen de los exponentes de sus variables. Lastimosamente, para las ecuaciones no lineales no existe un procedimiento general para resolverlas.

¿Cómo sabemos esto?
En 1970 Yuri Matiyasévich, luego de 20 años de trabajo, logró demostrar que no es posible encontrar un algoritmo que nos diga si una ecuación diofántica tiene soluciones o no las tiene.



¿Crisis?

No exactamente, aunque
no tengamos un procedimiento para todas las ecuaciones diofánticas existen casos particularesd que sí podemos resolver.

Contexto histórico

En 1657, Fermat, mandó el siguiente desafío a los matemáticos ingleses:

Dado un número cualquiera que no es un cuadrado existe un número infinito de cuadrados tal que si el cuadrado es multiplicado por el número dado y la unidad es añadida al producto el resultado es un cuadrado.

En otros términos, existen infinitos enteros x^2, y^2, d, donde d no es cuadrado tal que se cumple que $dy^2 + 1 = x^2$

Contexto histórico

¿Quiénes lograron la solución?

Algunos matemáticos proporcionaron soluciones para números racionales, por lo que no fueron aceptadas por Fermat. Finalmente fueron Brouncker y Wallis, particularmente Brouncker, quienes lograron resolver los casos particulares propuestos ($d = 61, 109, 149$) y además dieron un procedimiento general para llegar a la solución para cualquier valor de d.

Entonces...¿Tenemos un método para solucionarlas?

Algo así. El principal problema de este método, y de todos los otros trabajados es que no se puede asegurar que el método funcione siempre, es decir, el método se aplicaba a una ecuación con un valor d concreto y se podían obtener las soluciones x^2 y y^2. **PERO** en ningún momento se demuestra que el método era válido para *todos* los casos.

Contexto histórico

¿Qué tiene que ver Pell con todo esto?

John Pell fue un matemático inglés que vivió durante el siglo XVII. La razón por la que estas ecuaciones llevan su nombre parecer ser un error cometido por Euler al asociar el método de resolución anteriormente mencionado a Pell en vez de a Brouncker, quien vimos fue quien desarrolló el método, el cuál veremos más adelante. Como Euler era muy famoso y respetado, es entendible por qué este error no fue cuestionado y tomado como verdadero. Consiguientemente, a las ecuaciones

$$x^2 - dy^2 = 1$$

las conocemos como **ecuaciones de Pell**, aunque Pell probablemente no tuvo nada que ver con esto.

Algunos ejemplos

$d = 2$

$(x, y) = (3, 2), (17, 12)$

$d = 3$

$(x, y) = (2, 1), (7, 4), (26, 15)$

$d = 7$

$(x, y) = (127, 48), (2024, 765), (32257, 12192)$

$d = 29$

$(x, y) = (70, 13), (3699, 430), (9801, 1820)$

Lemas y definiciones

Definición 1*

Un irracional cuadrático α se dice que es reducido si α es mayor que 1 y su conjugado α', está entre -1 y 0

Teorema 1*

Si $\alpha > 1$ es un irracional cuadrático reducido, entonces la fracción continua para α es periódica pura

Teorema 2*

Si para un irracional cuadrático reducido $\alpha = [\overline{a_1, a_2, ..., a_n}]$ detonamos a $\beta = [\overline{a_n, a_{n-1}, ..., a_1}]$ la fracción continua de α con el periodo al revés, entonces $-\frac{1}{\beta} = \alpha'$ es la raíz conjugada de la ecuación satisfecha por α

Lemas y definiciones

Lema 1*

Para cualesquier N entero positivo, que no es un cuadrado perfecto, entonces $\sqrt{N} = [a_1, \overline{a_2, a_3, ..., a_n, 2a_1}]$ para algún n

Demostración Sea a_1 el entero más grande menor a $\sqrt{N}$ entonces $\sqrt{N} + a_1 > 1$ y su conjugado $-\sqrt{N} + a_1$ se encuentra entre -1 y 0, de modo que $\sqrt{N} + a_1$ es reducido. Si $\sqrt{N} = [a_1, \overline{a_2, a_3, ..., a_n, 2a_1}]$ entonces, aplicando el Teorema 1

$$\begin{aligned} \sqrt{N} + a_1 = & \quad [\overline{2a_1, a_2, a_3, ..., a_n}] \\ = & \quad [2a_1, \overline{a_2, a_3, ..., a_n, 2a_1}] \\ \Longrightarrow & \quad \sqrt{N} = [a_1, \overline{a_2, a_3, ..., a_n, 2a_1}] \end{aligned}$$

■

Lemas y definiciones

Ejemplo: $\sqrt{29}$

$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$

Ejemplo: $\sqrt{19}$

$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$

Lemas y definiciones

Lema 2*

Exceptuando el término $2a_1$, la parte periódica de la fracción continua de $\sqrt{N}$ es simétrica

Demostración Veamos que, dado que $\sqrt{N} = [a_1, \overline{a_2, a_3, ..., a_n, 2a_1}]$ obtenemos que $\sqrt{N} - a_1 = [0, a_2, a_3, ..., a_n, 2a_1]$, y entonces, podemos ver que

$$\begin{array}{rcl} \frac{1}{\sqrt{N}-a_1} & = & [\overline{a_2, a_3, ..., a_n, 2a_1}] \\ \frac{1}{\sqrt{N}-a_1} & = & [\overline{a_n, a_{n-1}, ..., 2a_1}] \ \textit{Teorema 2} \end{array}$$

Donde $a_1 - \sqrt{N}$ es el conjugado de $a_1 + \sqrt{N}$. Por el Teorema 15.6 (Stefan), entonces $a_n = a_2, a_{n-1} = a_3, ..., 2a_1 = 2a_1$. De modo que, exceptuando $2a_1$, la parte periódica de la fracción continua de $\sqrt{N}$ es simétrica

■

Cálculo de una solución

Teorema 3*

Sea $d > 1$ libre de cuadrados y supongamos que $\sqrt{d} = [a_1, \overline{a_2, ..., a_n, 2a_1}$. Entonces $p_n^2 - dq_n^2 = (-1)^n$ y $p_{2n}^2 - dq_{2n}^2 = 1$. Como consecuencia, si n es impar, $(x, y) = (p_n, q_n)$ es una solución de $x^2 - dy^2 = -1$ y (p_{2n}, q_{2n}) de $x^2 - dy^2 = 1$. Si n es par, $(x, y) = (p_n, q_n)$ es solución de $x^2 - dy^2 = 1$

Demostración Veamos que la fracción continua de $\sqrt{d}$ es lo único que necesitamos para resolver la ecuación $x^2 - dy^2 = \pm 1$. Sabemos que

$$\sqrt{d} = [a_1, \overline{a_2, a_3, ..., a_n, 2a_1}] = [a_1, a_2, a_3, ..., a_n, \alpha_{n+1}]$$

donde

$$\alpha_{n+1} = [\overline{2a_1, a_2, a_3, ..., a_n}] = \sqrt{d} + a_1$$

. Y recordemos por lo presentado anteriormente (Rudik) que podemos escribir

$$\sqrt{d} = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

Cálculo de una solución

donde $p_{n-1}, q_{n-1}, p_n, q_n$ son los enteros ya conocidos, que facilitan las convergentes $C_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ y $C_n = \frac{p_n}{q_n}$ justo antes del término $2a_1$. Ahora, si sustituimos α_{n+1} tenemos que

$$\begin{aligned} \sqrt{d} = & \ \frac{(\sqrt{d}+a_1)p_n+p_{n-1}}{(\sqrt{d}+a_1)q_n+q_{n-1}} \implies \\ \sqrt{d}(\sqrt{d}+a_1)q_n + q_{n-1}\sqrt{d} & = (\sqrt{d}+a_1)p_n + p_{n-1} \implies \\ dq_n + (a_1q_n + q_{n-1})\sqrt{d} & = (a_1p_n + p_{n-1}) + p_n\sqrt{d} \end{aligned}$$

de modo que $p_{n-1} = dq_n - a_1p_n$ y $q_{n-1} = p_n - a_1q_n$.
Ahora, recordemos, por el Teorema 15.3 (Pallais) que $p_nq_{n-1} - q_np_{n-1} = (-1)^n$, de modo que si sustituimos tenemos que $p_n(p_n - a_1q_n) - q_n(dq_n - a_1p_n) = (-1)^n$ y al simplificar tenemos que $p_n^2 - dq_n^2 = (1)^n$

Cálculo de una solución

Para n par

$$p_n^2 - dq_n^2 = (-1)^n = 1$$

de modo que las soluciones a la ecuación de Pell serán $(x_1, y_1) = (p_n, q_n)$
Para n impar Las soluciones $(x_1, y_1) = (p_n, q_n)$ se cumplirán para
$p_n^2 - dq_n^2 = (-1)^n = -1$. Veamos que para obtener las soluciones para $x^2 - dy^2 = 1$, debemos buscar en el segundo periodo de la fracción continua de $\sqrt{d}$, de este modo, se toma el término a_{2n}, ya que

$$p_{2n}^2 - dq_{2n}^2 = (-1)^{2n} = 1$$

de modo que $(x_1, y_1) = (p_{2n}, q_{2n})$■

Calcular una solución

Ejemplo: $x^2 - 29y^2 = 1$

$$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$$

$$a_n = a_5 \implies C_10 = \frac{70}{27}$$

$$(x_1, y_1) = (9801, 1820)$$

$$(9801)^2 - 29(1820)^2 = 96059601 - 96059600 = 1$$

Calcular una solución

Ejemplo: $x^2 - 19y^2 = 1$

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$$

$$a_n = a_6 \implies C_6 = \frac{170}{39}$$

$$(x_1, y_1) = (170, 39)$$

$$(170)^2 - 29(30)^2 = 28900 - 28899 = 1$$

Aproximaciones Racionales

Teorema 15.9 (Wilfredo)

Sea ξ un número irracional cualesquiera, entonces

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

Aproximaciones Racionales

Teorema 4*

Sea ξ un número irracional cualesquiera y $c_i = \frac{p_i}{q_i}, i \in \mathbb{N}$ el i-ésimo convergente de la fracción continua de ξ. Si $r, s \in \mathbb{Z}$ con $s > 0$ y k es un entero positivo tal que $|s\xi - r| < |q_k\xi - p_k|$ entonces $s \geq q_{k+1}$. Además, si $\frac{r}{s}$ es un número racional tal que

$$\left|\xi - \frac{r}{s}\right| < \frac{1}{2s^2}$$

entonces $\frac{r}{s}$ es una convergente de la fracción continua de ξ

Demostración Supongamos por contradicción que $1 \leq y < q_{k+1}$, considerando el siguiente sistema de ecuaciones lineales

$$p_k x + p_{k+1} y = r$$

$$q_k x + q_{k+1} y = s$$

Aproximaciones Racionales

Utilizando eliminación Gaussiana y el Teorema 15.3 (Pallais) obtenemos que

$$x = (-1)^{k-1}(sp_{k+1} - rq_{k+1})$$

$$y = (-1)^{k-1}(rq_k - sp_k)$$

. Debemos demostrar ahora que x, y son no nulos y de distinto signo. Supongamos que $x = 0 \implies \frac{r}{s} = \frac{p_{k+1}}{q_{k+1}}$. Dado que $(p_{k+1}, q_{k+1}) = 1$, entonces $q_{k+1} \mid s,\ q_{k+1} \leq s (\rightarrow\leftarrow)$. Tomemos ahora $y = 0$, entonces $r = p_k x$, $s = q_k x$, de modo que

$$|s\xi - r| = |x|\,|q_k\xi - p_k| \geq |q_k\xi - p_k|\,(\rightarrow\leftarrow)$$

, luego x, y son ambos no nulos. Supongamos que $y < 0$. Como $q_k x = s - q_{k+1}y$ con $q_i > 0$, tenemos $x > 0$. Si $y > 0$, entonces $q_{k+1}y \geq q_{k+1} > s$, tenemos $q_k x = s - q_{k+1}y < 0$, luego $x < 0$.

Aproximaciones Racionales

Por otra parte, si k es impar, tenemos que

$$\frac{p_k}{q_k} < \xi < \frac{p_{k+1}}{q_{k+1}}$$

si k es par, tenemos que

$$\frac{p_{k+1}}{q_{k+1}} < \xi < \frac{p_k}{q_k}$$

De igual manera vemos que $q_k\xi - p_k$ y $q_{k+1}\xi - p_{k+1}$ tienen signos opuestos, finalmente $x\left(q_k\xi - p_k\right)$ e $y\left(q_{k+1\xi - p_{k+1}}\right)$ tienen el mismo signo, y de modo que

$$\begin{aligned} |s\xi - r| &= \left|\left(q_k x + q_{k+1}y\right)\xi - \left(p_k x + p_{k+1}y\right)\right| \\ &= \left|x\left(q_k\xi - p_k\right) + y\left(q_{k+1}\xi - p_{k+1}\right)\right| \\ &= |x|\left|q_k\xi - p_k\right| + |y|\left|q_{k+1}\xi - p_{k+1}\right| \quad \geq |x|\left|q_k\xi - p_k\right| \geq \left|q_k\xi - p_k\right| \end{aligned}$$

. $(\rightarrow\leftarrow) \therefore s \geq q_{k+1}$.

Aproximaciones Racionales

Para la siguiente parte, supongamos que $\frac{x}{y}$ no es una convergente de la fracción continua de ξ, es decir $\frac{x}{y} \neq \frac{p_i}{q_i}$ para todo i. Sea k el entero no negativo más grande tal que $y \geq q_k$, entonces $y \geq q_0 = 1$ y $q_k \to \infty$ si $k \to \infty$. Entonces $q_k \leq s \leq q_{k+1}$ y por lo demostrado anteriormente, tenemos que

$$|q_k\xi - p_k| \leq |s\xi - r| = s\left|\xi - \frac{r}{s}\right| < \frac{1}{2s},$$

de modo que $\left|\xi - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}$. Como $\frac{r}{s} \neq \frac{p_k}{q_k}$, tenemos que $|sp_k - rq_k| \geq 1$ así

$$\begin{aligned}\frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| = \left|\frac{p_k}{q_k} - \frac{r}{s} + \xi - \xi\right| \\ &\leq \left|\xi - \frac{p_k}{q_k}\right| + \left|\xi - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2}\end{aligned}$$

Esto implica que $\frac{1}{2sq_k} < \frac{1}{2s^2}$, así que $q_k > s(\to\leftarrow)\blacksquare$

Solución general de la ecuación de Pell

Teorema 5*

Sean k, d enteros con $d > 0$ libre de cuadrados y $|k| < \sqrt{d}$. Sea (x, y) una solución de la ecuación $x^2 - dy^2 = k$ con $x, y > 0$. Entonces $\frac{x}{y}$ es una convergente de $\sqrt{d}$

Demostración. **Para** k **positivo** Tenemos que

$$0 < x - y\sqrt{d} = \frac{k}{x + y\sqrt{d}} < \frac{\sqrt{d}}{x + y\sqrt{d}} = \frac{1}{y(\frac{x}{y\sqrt{d}} + 1)} < \frac{1}{y(\frac{x}{\sqrt{d}} + y)} < \frac{1}{2y^2}$$

. Dado que $x > y\sqrt{d}$ vemos que

$$\left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2y^2}$$

y por el Teorema 4* $\frac{x}{y}$ es una convergente de $\sqrt{d}$.

Solución general de la ecuación de Pell

Para k negativo Dado que

$$y^2 - \frac{x^2}{d} = \frac{-k}{d}$$

entonces

$$0 < y - \frac{x}{\sqrt{d}} = \frac{-\left(\frac{k}{d}\right)}{y + \frac{x}{\sqrt{d}}} < \frac{1}{y\sqrt{d} + x} = \frac{1}{x(1 + \frac{y\sqrt{d}}{x})}$$

de modo que

$$\left| \frac{1}{\sqrt{d}} - \frac{y}{x} \right| < \frac{1}{2x^2}$$

Por el Teorema 4*, $\frac{x}{y}$ es convergente de $\xi = \frac{1}{\sqrt{d}}$.

Solución general de la ecuación de Pell

Veamos entonces que si $\sqrt{d} = [a_1, a_2, ...]$ entonces $\frac{1}{\sqrt{d}} = [0, a_1, a_2, ...]$ de modo que los convergentes de $\frac{1}{\sqrt{d}}$ tienen la forma $\{\frac{1}{C_n}\}$ donde $\{C_n\}$ son los convergentes de $\sqrt{d}$

Solución general de la ecuación de Pell

Teorema 6

Sea $\frac{p_n}{q_n}$ el n-ésimo convergente de la fracción continua de $\sqrt{d}$ con d entero. Entonces $p_n + q_n\sqrt{d}$ es una unidad en $\mathbb{Z}[\sqrt{d}]$ ssi $\sqrt{d} = [a_1\overline{a_1, ..., a_n, 2a_1}]$. Si esto ocurre, entonces $d(p_n + q_n\sqrt{d}) = (-1)^n$

Demostración. Supongamos que $p_n^2 - dq_n^2 = \pm 1$. Sabemos que $\sqrt{d}$ está entre los converegentes $\frac{p_n}{q_n}$ y $\frac{p_{n+1}}{q_{n+1}}$. De modo que el signo de $\frac{p_n}{q_n} - \sqrt{d}$ es el mismo que el de $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}$, y por la igualdad $p_{n+1}q_n - p_nq_{n+1} = (-1)^{n+1}$, el signo será $(-1)^n$. Por otro lado, $p_n + q_n\sqrt{d}$ es positivo, por tanto tenemos

$$p_n^2 - dq_n^2 = \left(p_n + q_n\sqrt{d}\right)\left(p_n - q_n\sqrt{d}\right) = (-1)^n$$

Tenemos $\sqrt{d} = [a_1, a_2 \ldots, a_n, \alpha]$. Resolviendo esta ecuación para encontrar α, tenemos por tanto

$$\sqrt{d} = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}$$

Solución general de la ecuación de Pell

Esto nos da que $\left(p_n - q_n\sqrt{d}\right)\alpha = -\left(p_{n-1} - q_{n-1}\sqrt{d}\right)$, multiplicando por $p_n + q_n\sqrt{d}$, tenemos

$$\alpha = (-1)^{n+1}\left(p_{-1} - q_{n-1}\sqrt{d}\right)\left(p_n + q_n\sqrt{d}\right)$$

Recordando que $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$, tenemos

$$\alpha = c + \sqrt{d}, \quad \text{donde} \quad c = (-1)^n\left(p_n p_{n-1} - q_n q_{n-1} d\right)$$

$$\sqrt{d} = \left[a_1, \ldots, a_n, c + \sqrt{d}\right] = [a_1, \overline{a_2, \ldots, a_n, c + a_1}]$$

Solución general de la ecuación de Pell

Para el regreso, suponemos que $\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, c + a_1}]$ para algún entero c, probaremos que $N\left(p_n + q_n\sqrt{d}\right) = (-1)^n$ y $c = a_1$. Por hipótesis $\sqrt{d} = \left[a_1, \ldots, a_n, c + \sqrt{d}\right]$, entonces

$$\sqrt{d} = \frac{(c + \sqrt{d})p_n + p_{n-1}}{(c + \sqrt{d})q_n + q_{n-1}}$$

Podemos expresar el lado derecho como $x + y\sqrt{d}$ y comparamos coeficientes, multiplicando el numerador y denominador por $(c - \sqrt{d})q_n + q_{n-1}$, de manera que

$$\sqrt{d} = \frac{\left(cp_n + \sqrt{d}p_n + p_{n-1}\right)\left(cq_n - \sqrt{d}q_n + q_{n-1}\right)}{N}.$$

donde $N = N\left(cq_n + q_{n-1} + \sqrt{d}q_n\right)$.

Solución general de la ecuación de Pell

De modo que

$$\sqrt{d} = \frac{(cp_n + p_{n-1})(cq_n + q_{n-1}) - dp_nq_n + \sqrt{d}(p_nq_{n-1} - q_np_{n-1})}{N}.$$

Finalmente, tenemos que $N = p_nq_{n-1} - q_np_{n-1} = (-1)^n$. Por el teorema anterior tenemos que $\frac{cq_n+q_{n-1}}{q_n}$ es un convergente de la fracción continua de $\sqrt{d}$ y por tanto $cq_n + q_{n-1} = p_n$. En particular, $N = N\left(p_n + q_n\sqrt{d}\right) = (-1)^n$. La ecuación $cq_n + q_{n-1} = p_n$, implica que $c = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}$, y tenemos

$$\frac{p_n}{q_n} - 1 < c < \frac{p_n}{q_n}.$$

Ya que $\lfloor\sqrt{d}\rfloor \leq \frac{p_n}{q_n} \leq \lfloor\sqrt{d}\rfloor + 1$, por tanto:

$$\lfloor\sqrt{d}\rfloor - 1 < c < \lfloor\sqrt{d}\rfloor + 1.$$

Como c es un entero, tenemos $c = \lfloor\sqrt{d}\rfloor = a_1$. Por lo tanto,

$$\sqrt{d} = \left[a_1, \overline{a_2, \ldots, a_n, 2a_0}\right].$$

Solución general de la ecuación de Pell

Y existen más teoremas, pero a fin de cuentas ¿Qué nos están diciendo todos?

Que tenemos cada vez más criterios para determinar si un par (x, y) es o no es solución de una ecuación de Pell para algún d (debe ser unidad de $\mathbb{Z}[\sqrt{d}]$, debe tener la forma $\zeta^m = (x + y\sqrt{d})^m$ donde $\zeta \in \mathbb{Z}[\sqrt{d}]$, etc.) no tenemos una formula exacta para determinar todas las soluciones.

Referencias

Ecuaciones diofánticas. (s.f.). Universidad del País Vasco. Recuperado 17 de octubre de 2023, de https://www.ehu.eus/ mtpalezp/descargas/olimpdiofa.pdf

Diamond. (2016). La ecuación de pell. Gaussianos. https://www.gaussianos.com/la-ecuacion-de-pell/

Nieto Medina, D. (s.f.). Fracciones continuas. La ecuación de Pell [Trabajo Fin de Grado]. Universidad de Valladolid.

Gliga.
(2005). On continued fractions of the square root of prime numbers. Williams University. https://web.williams.edu/Mathematics/sjmiller/public$_h$*tml*/*mathlab*/*public*$_h$*tml*/*jr*02*fall*/*Per*