UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

La Ecuación $xa + yb = c$

Alan Reyes-Figueroa

Teoría de Números

(Aula 05) 18.julio.2023

La ecuación $xa + yb = c$

Recordemos:

Teorema (Teorema de Bézout)

Para todo $a, b \in \mathbb{Z}$, existen $M, N \in \mathbb{Z}$ tales que $Ma + Nb = d$, $d = (a, b)$.

Propiedad

La ecuación diofantina $xa + yb = c$ admite solución en $\mathbb{Z}$ si, y sólo si, $d \mid c$, donde $d = (a, b)$.

Si (x_o, y_o) es una solución particular de la ecuación, entonces todas las otras soluciones son de la forma

$$x = x_o + \tfrac{b}{d}t, \qquad y = y_o - \tfrac{a}{d}t, \qquad t \in \mathbb{Z}.$$

Prueba: ($\Rightarrow$) Como $d = (a, b)$ existen enteros $r, s \in \mathbb{Z}$ con $a = dr$, $b = ds$.

La ecuación $xa + yb = c$

Si existe una solución $(x_o, y_o) \in \mathbb{Z}^2$, entonces

$$c = x_o a + y_o b = x_o(dr) + y_o(ds) = d(x_o r + y_o s) \quad \Rightarrow \quad d \mid c.$$

($\Leftarrow$) Sea $d \mid c$. Entonces $c = dq$, para algún $q \in \mathbb{Z}$. Por el Teorema de Bézout, existen enteros $M, N \in \mathbb{Z}$ tales que $d = Ma + Nb$. Entonces

$$(Mq)a + (Nq)b = (Ma + Nb)q = dq = c,$$

y $(Mq, Nq) \in \mathbb{Z}^2$ es una solución de $xa + yb = c$.

Para la segunda afirmación del teorema, supongamos que se conoce una solución $(x_o, y_o) \in \mathbb{Z}^2$ de la ecuación dada. Si $(x', y') \in \mathbb{Z}^2$ es cualquier otra solución, entonces $ax_o + by_o = c = ax' + by'$. Lo anterior es equivalente a $a(x' - x_o) = b(y_o - y')$.

La ecuación $xa + yb = c$

Tenemos $a(x' - x_0) = b(y_0 - y')$.
De nuevo, como $d = (a, b)$, existen enteros primos relativos r y s, tales que $a = dr$, $b = ds$. Sustituyendo estos valores en la ecuación anterior y cancelando el factor común d, entonces

$$r(x' - x_0) = s(y_0 - y').$$

La situación es ahora la siguiente: $r \mid s(y_0 - y')$, con $(r, s) = 1$. Del lema de Euclides, $r \mid y_0 - y'$; ó, en otras palabras, $y_0 - y' = rt$ para algún número entero $t \in \mathbb{Z}$.
Sustituyendo, obtenemos

$$x' - x_0 = st.$$

Esto lleva a las fórmulas

$$x' = x_0 + st = x_0 + \tfrac{b}{d}t, \qquad y' = y_0 - rt = y_0 - \tfrac{a}{d}t.$$

La ecuación $xa + yb = c$

Sin importar el valor de $t \in \mathbb{Z}$, estos valores satisfacen la ecuación diofantina, pues

$$\begin{aligned} ax' + by' &= a\left(x_0 + \tfrac{b}{d}t\right) + b\left(y_0 - \tfrac{a}{d}t\right) = (ax_0 + by_0) + \Big(\underbrace{\tfrac{ab}{d} - \tfrac{ab}{d}}_{=0}\Big)t \\ &= c \end{aligned}$$

Entonces, existen infinitas soluciones a la ecuación, una para cada $t \in \mathbb{Z}$, en la forma requerida. □

Corolario

Si $(a, b) = 1$ y si $(x_0, y_0) \in \mathbb{Z}^2$ es una solución particular de la ecuación diofantina $xa + yb = c$, entonces todas las soluciones son de la forma

$$x = x_0 + bt, \qquad y = y_0 - at, \qquad t \in \mathbb{Z}.$$

Estimativa de Lamé

Sean $a \geq b \geq 0$. Recordemos que si el Algoritmo de Euclides hace $k+1$ divisiones para hallar $d = (a, b)$, entonces en cada paso $r_{k+1} = q_k r_{k-1} + r_k$, $q_k \geq 1$, $b > r \geq 0$, se tiene

$$a = qb + r \geq b + r > 2r, \;\Rightarrow\; r < \tfrac{a}{2}.$$

Similarmente, $r_1 < \frac{b}{2} \leq \frac{a}{2}$, $r_2 < \frac{r}{2} < \frac{a}{4}$, $r_3 < \frac{r_1}{2} < \frac{b}{4} \leq \frac{a}{4}$, ..., y en general

$$r_{2j} < \tfrac{a}{2^j}, \qquad r_{2j+1} < \tfrac{a}{2^j} \qquad \text{para } j = 1, 2, \ldots, (k+1)/2.$$

Por otro lado, existe $t \in \mathbb{Z}^+$ tal que $a < 2^t \;\Rightarrow\; \log_2 a < t \;\Rightarrow\; r_{2t} < \frac{a}{2^t} < 1 \;\Rightarrow r_{2t} = 0$. (*i.e.*, el algoritmo acaba a lo sumo en $2t$ pasos)

Si a tiene N dígitos en su representación decimal, entonces $a < 10^N$. Luego, $\log_2 a < N \log_2 10$.

Estimativa de Lamé

Así

$$k+1 = 2t \leq 2\big(\lfloor \log_2 a \rfloor + 1\big) \leq 2\big(N\lfloor \log_2 10 \rfloor + 1\big) \approx 6.6N.$$

(Lamé, 1844).

Se puede mostrar que para que el Algoritmo de Euclides efectúe n pasos ($n = k+1$), se debe tomar al menos $a = F_{n+2},\ b = F_{n+1}$.
En particular $n < 2\log_2 a \ \Rightarrow \ \frac{n}{2} < \log_2 a \ \Rightarrow \ a > 2^{n/2}$.

Recordemos la **Fórmula de** Binet (1843)

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Como $\left(\frac{1-\sqrt{5}}{2}\right)^n \to 0$, cuando $n \to \infty$, podemos simplificar

Estimativa de Lamé

$$F_n \approx \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n = \tfrac{1}{\sqrt{5}}\varphi^n,$$

donde $\varphi = \frac{1+\sqrt{5}}{2}$ es la razón aúrea. (*i.e.*, los F_n se parecen a los φ^n)

Recordemos que φ satisface $\varphi^2 - \varphi - 1 = 0$, de modo que $\varphi^2 = \varphi + 1$.
Afirmamos que $F_n \geq \varphi^{n-1}$, para todo $n \geq 1$.

$F_1 = 1 \geq \varphi^0$, $F_2 = 2 \geq \varphi$. Asumiendo la hipótesis inductiva que $F_k \geq \varphi^{k-1}$ siempre que $k \leq n$, entonces $F_{n+1} = F_n + F_{n-1} \geq \varphi^{n-1} + \varphi^{n-2} = \varphi^{n-2}(\varphi + 1) = \varphi^{n-2}\varphi^2 = \varphi^n$, lo que completa la afirmación.

Luego, $a = F_{n+2} \geq \varphi^{n+1}$ y vale que $n \leq n + 1 = \log_\varphi \varphi^{n+1} \leq \log_\varphi a$.

Estimativa de Lamé

De esta última desigualdad, obtenemos

$$n \leq \log_{\varphi} a = \frac{\log_{10} a}{\log_{10} \varphi} \approx 4.7851..(\log_{10} a) < 5 \log_{10} a \leq 5N.$$

(Teorema de Lamé, 1844).