El Teorema Fundamental de la Aritmética

Alan Reyes-Figueroa

Teoría de Números (Aula 04) 20.julio.2021

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_0, y_0) es una solución particular de la ecuación, entonces todas las otras soluciones son de la forma

$$x = x_0 + \tfrac{b}{d}t, \qquad y = y_0 - \tfrac{a}{d}t, \qquad t \in \mathbb{Z}.$$

<u>Prueba</u>: $(\Rightarrow)$ 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 $(x_0, y_0) \in \mathbb{Z}^2$, entonces

$$c = x_0 a + y_0 b = x_0(dr) + y_0(ds) = d(x_0 r + y_0 s) \quad \Rightarrow \quad d \mid c.$$

$(\Leftarrow)$ 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 $(x_0, y_0) \in \mathbb{Z}^2$ de la ecuación dada. Si $(x', y') \in \mathbb{Z}^2$ es cualquier otra solución, entonces $ax_0 + by_0 = c = ax' + by'$. Lo anterior es equivalente a $a(x' - x_0) = b(y_0 - y')$.

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

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

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

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, $\log_2 a < N \log_2 10$.

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

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 $n \leq n + 1 = \log_\varphi \varphi^{n+1} \leq \log_\varphi a$.

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

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).

Números Primos

Definición

Un entero $p > 1$ es llamado un número ***primo*** *si sus únicos divisores positivos son 1 y p. Un número mayor a 1 que no es primo se llama* ***compuesto****.*

Ejemplo:

$2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 91, 97, \ldots$

Propiedad

Si p es primo y $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.

Prueba: Si $p \mid a$, acabó. Supongamos entonces que $p \nmid a$. Como los únicos divisores positivos de p son 1 y p, entonces $(p, a) = 1$. Por el Lema de Euclides, entonces $p \mid b$. $\square$

Corolario

Si p es primo y $p \mid a_1 a_2 \cdots a_n$, entonces $p \mid a_k$ para algún k, donde $1 \leq k \leq n$.

Prueba: Por inducción sobre n, el número de factores.
Cuando $n = 1$, la conclusión es inmediata; para $n = 2$, el resultado es el contenido de la propiedad anterior.
Suponga que $n > 2$ y que siempre que p divide al producto de menos de n factores, divide al menos uno de los factores. Ahora $p \mid a_1 a_2 \cdots a_n$. De la propiedad anterior, $p \mid a_n$ ó $p \mid a_1 a_2 \cdots a_{n-1}$. Si $p \mid a_n$, listo! En el caso, $p \mid a_1 a_2 \cdots a_{n-1} \;\Rightarrow\; p \mid a_k$, para algún $1 \leq k \leq n-1$. En cualquier caso, p divide uno de los factores. $\square$

Corolario

Si $p, q_1, q_2, \ldots, q_n$ son primos y $p \mid q_1 q_2 \cdots q_n$, entonces $p = q_k$, para algún $1 \leq k \leq n$.

Prueba: Del colorario arriba sabemos que $p \mid q_k$ para algún $1 \leq k \leq n$. Como q_k es primo, q_k sólo tiene divisores positivos 1 ó q_k. Entonces $p = 1$ ó $p = q_k$. Pero p al ser primo, satisface $p > 1$. Portanto, $p = q_k$. $\square$

Teorema (Teorema Fundamental de la Aritmética)

Todo entero positivo $n > 1$ es primo o es producto de primos. Esta representación es única, a menos del orden en los factores.

Prueba: Se $n > 1$. Entonces n es primo o es compuesto. En el primer caso, no hay nada que probar. Si n es compuesto, entonces existe un entero d que satisface $d \mid n$ y $1 < d < n$.
Elija p_1 el menor entre todos esos enteros d (esto es posible por el principio de buen orden). Entonces, p_1 es primo. De lo contrario, también tendría un divisor q con $1 < q < p_1$; pero entonces $q \mid p_1$ y $p_1 \mid n \;\Rightarrow q \mid d$, lo que contradice la elección de p_1 como el menor divisor positivo de n.

Portanto, podemos escribir $n = p_1 n_1$, donde p_1 es primo y $1 < n_1 < n$. Caso contrario, repetimos el argumento anterior para producir un segundo número primo p_2 tal que $n_1 = p_2 n_2$, con $1 < p_2, n_2 < n_1$, esto es

$$n = p_1 p_2 n_2, \qquad 1 < n_2 < n_1.$$

Si n_2 es primo, no es necesario ir más lejos. De lo contrario, escriba $n_2 = p_3 n_3$, con p_3 primo.

Continuando este proceso, la secuencia decreciente $n > n_1 > n_2 > \ldots > 1$, no puede continuar indefinidamente, de modo que después de un número finito de pasos n_{k-1} es un primo, digamos p_k. Así, obtenemos la existencia de una factoración en primos

$$n = p_1 p_2 \cdots p_k.$$

Para la unicidad, supongamos que n admite dos representaciones como producto de primos de dos formas; decir,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdot q_s, \qquad r \leq s,$$

donde p_i y q_j son todos primos, escritos en magnitud creciente de modo que $p_1 \leq p_2 \leq \ldots \leq p_r$ y $q_1 \leq q_2 \leq \ldots \leq q_s$. Como $p_1 \mid q_1 q_2 \cdots q_s$, por el el Corolario 2 anterior, $p_1 = q_k$ para algún $1 \leq k \leq s$. Esto implica que $p_1 \geq q_1$.

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un razonamiento similar produce $q_1 \geq p_1$, de modo que $p_1 = q_1$ Podemos cancelar este factor común y obtener

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdot q_s.$$

Repetimos el agrumento anterior para obtener $p_2 = q_2$ y, a su vez,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdot q_s.$$

Continuando de esta forma, si la desigualdad $r < s$ fuese válida, eventualmente tendríamos que $1 = q_{r+1} q_{r+2} \ldots q_s$, lo cual es absurdo, ya que cada $q_j > 1$. Por lo tanto, $r = s$, lo que hace idénticas las dos factoraciones de n. Esto completa la prueba. $\square$