El Teorema Fundamental de la Aritmética

Alan Reyes-Figueroa

Teoría de Números

(Aula 07) 25.julio.2025

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 $1 \leq k \leq n$.

<u>Prueba</u>: 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 $1 \leq k \leq n$.

<u>Prueba</u>: 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,

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

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 $p_1 \geq q_1$.

Teorema Fundamental de la Aritmética

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

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

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

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

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. $\square$

UNIVERSIDAD DEL VALLE DE GUATEMALA