1. Teorema Fundamental de la Aritmética

Teorema 1.1 (Teorema Fundamental de la Aritmética)**.** *Todo entero mayor que 1 puede escribirse de forma única como un producto de números primos, salvo el orden de los factores.*

Demostración. La demostración se divide en dos partes: existencia y unicidad.

Existencia: Procedemos por inducción sobre $n \in \mathbb{N}$, con $n > 1$.

Caso base: $n = 2$. Como 2 es primo, ya es producto de un único primo.

Paso inductivo: Supongamos que todo entero k, con $2 \leq k < n$, se puede expresar como producto de primos. Si n es primo, ya está expresado como producto de primos. Si n no es primo, entonces existe a, b tales que $n = ab$, con $1 < a < n$ y $1 < b < n$. Por hipótesis inductiva, a y b se escriben como productos de primos, por lo tanto n también.

Unicidad: Supongamos que un número n tiene dos descomposiciones distintas en primos:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde todos los p_i y q_j son primos. Usamos inducción y el hecho de que si un primo p divide un producto, entonces divide al menos uno de los factores (propiedad fundamental de los primos).

Se puede mostrar que p_1 debe coincidir con alguno de los q_j. Reordenando, cancelamos ese factor común y repetimos el argumento. Finalmente, llegamos a que ambas factorizaciones son iguales salvo el orden.

■

Corolario 1.1.1. *La cantidad de representaciones de un número natural como producto de primos es finita y única, salvo el orden de los factores.*

Lema 1.2. *Si un número primo p divide al producto ab, entonces p divide a a o a b.*