Teorema Fundamental de la Aritmética

El teorema fundamental de la aritmética, o teorema de factorización única, afirma que cualquier número natural mayor que 1 puede descomponerse (¡de manera única!) como producto de potencias de números primos. Este resultado resalta la importancia de los números primos, ya que ellos conforman los bloques de construcción de cualquier número (mayor que 1).

Teorema fundamental de la aritmética: Sea $n \in \mathbb{Z}^+$ con $n > 1$. Entonces, existen números primos $p_1 < p_2 < \cdots < p_r$ y $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}^+$ tales que

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Más aún, la descomposición anterior para n es única, en el siguiente sentido:

Si $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ donde $q_1 < q_2 < \cdots < q_s$ son primos y $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{Z}^+$, entonces $r = s$, $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_r = q_s$, y $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, $\ldots$, $\alpha_r = \beta_s$.

A la hora de demostrar el teorema anterior, para su mejor entendimiento, vamos a romperlo en varias partes, y demostraremos cada una de ellas. Primero unos ejemplos.

Ejemplos:

(1) $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13.$

(2) $10800 = 2 \cdot 5400 = 2 \cdot 10^2 \cdot 54 = 2^2 \cdot 10^2 \cdot 27$
$= 2^2 \cdot 10^2 \cdot 3^3 = 2^2 \cdot 3^3 \cdot 10^2$

(3) $1024 = 2^{10}$

Parte 1: $n \in \mathbb{Z}^+$, $n > 1$. Existen números primos $p_1 \leq p_2 \leq \cdots \leq p_n$ tales que

$$n = p_1 \cdot p_2 \cdots p_n. \quad (*)$$

En otras palabras, todo entero mayor que 1 se descompone como producto de números primos.

· Demostración: Usamos inducción sobre n.

- $n = 2$: Al ser 2 primo, la descomposición es

$$n = 2,$$

y el resultado se sigue.

- Dado $n > 2$, supongamos que el resultado se cumple para cualquier $m \in \mathbb{Z}^+$ con

$$2 \leq m < n.$$

Si $n = p$ es primo, la descomposición a buscar es $n = p$. Supongamos entonces que n es compuesto, es decir,

$$n = m_1 \cdot m_2 \quad \text{con} \quad 1 < m_1 \leq m_2 < n$$

Por la hipótesis inductiva, se tiene que

$$m_1 = p_1^1 \, p_2^1 \cdots p_{r_1}^1 \quad y \quad m_2 = p_1^2 \, p_2^2 \cdots p_{r_2}^2$$

donde $p_1^1 \leq p_2^1 \leq \cdots \leq p_{r_1}^1$ y $p_1^2 \leq p_2^2 \leq \cdots \leq p_{r_2}^2$ son primos. Luego,

$$n = m_1 m_2 = p_1^1 \cdot p_2^1 \cdots p_{r_1}^1 \cdot p_1^2 \cdot p_2^2 \cdots p_{r_2}^2$$

$$n = p_1 \cdot p_2 \cdots p_r,$$

donde $r = r_1 + r_2$, $p_1 \leq p_2 \leq \cdots \leq p_r$ y

$p_1, p_2, \ldots, p_r \in \{p_1^1, p_2^1, \ldots, p_{r_1}^1, p_1^2, p_2^2, \ldots, p_{r_2}^2\}$. ∎

Para probar la unicidad de la descomposición (* nos hará falta el siguiente lema auxiliar.

Lema: Si $p, p_1, \ldots, p_r$ son números primos y $p \mid p_1 \cdots p_r$, entonces $p = p_i$ para algún $i \in \{1, \ldots, r\}$.

<u>Demostración</u>: Usaremos inducción sobre n.

- $n = 2$: $p \mid p_1 \cdot p_2$. Supongamos que $p \neq p_1$, ya que en el caso $p = p_1$ no hay nada que probar. Por un resultado anterior,

$$p \text{ primo y } p \mid p_1 \cdot p_2 \Rightarrow p \mid p_2.$$

Ahora, como p y p_2 son primos, la condición $p \mid p_2$ implica que $p = p_2$.

- Supongamos que el resultado se cumple para cualquier producto de $n-1$ números primos.

Sea $b = p_2 \cdots p_n$. Luego, $p \mid p_1 \cdot b$.

Por un resultado previo,

$$p \text{ primo} \Rightarrow p \mid p_1 \text{ o } p \mid b.$$

Si $p \mid p_1$ entonces $p = p_1$, por ser p_1 primo.

Si $p \mid b$, entonces por la hipótesis inductiva se tiene que $p = p_i$ para algún $i \in \{2, \dots, n\}$. $\blacksquare$

Parte 2: La descomposición (*) es única en el siguiente sentido:

Si $n = q_1 \cdot q_2 \cdots q_s$ con $q_1 \leq q_2 \leq \cdots \leq q_s$ números primos, entonces $r = s$ y

$$p_1 = q_1, \; p_2 = q_2, \; \ldots, \; p_r = q_s.$$

• Demostración: Supongamos que tenemos dos descomposiciones de n en factores primos

$$p_1 \cdot p_2 \cdots p_r = n = q_1 \cdot q_2 \cdots q_s \cdot \quad (**)$$

Luego, claramente $p_1 \mid q_1 q_2 \cdots q_s$. Por el lema anterior $p_1 = q_{i_1}$ para algún $i_1 \in \{1, 2, \ldots s\}$. Continuando de esta manera, se tiene que

$$p_1 = q_{i_1}, \; p_2 = q_{i_2}, \; \ldots, \; p_r = q_{i_r} \quad (***)$$

con $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, s\}$.

Supongamos $r < s$. Entonces, al cancelar los primos $p_1, p_2, \ldots, p_r$ de la igualdad $(**)$, nos queda una expresión de la forma

$$1 = q_{j_1} q_{j_2} \cdots q_{j_t},$$

lo cual es una contradicción ya que implicaría que $q_{j_1} = q_{j_2} = \cdots = q_{j_t} = 1$.

La suposición $r > s$ también arroja una contradicción similar. Por lo tanto, $r = s$.

Finalmente, dado a que los conjuntos $\{p_1, p_2, \ldots, p_r\}$ y $\{q_1, \ldots, q_s\}$ están ordenados de manera creciente, las igualdades en $(***)$ se convierten en:

$$p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_r = q_r. \quad \blacksquare$$

Observación: En la descomposición

$$n = p_1' p_2' \cdots p_{r'}'$$

con $p_1' \leq p_2' \leq \cdots \leq p_{r'}'$ primos, pueden aparecer repeticiones de los p_i'. Luego, se puede reescribir n como

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

donde $\alpha_i \in \mathbb{Z}^+$ es el número de repeticiones de p_i.

Veamos algunas aplicaciones del teorema fundamental de la aritmética.

Aplicación 1: Infinitud de los números primos

Si bien es bastante conocido el hecho de que existen infinitos números primos, su demostración no es algo tan trivial. Hoy en día existen muchas demostraciones de la infinitud de los números primos, y una de ellas aplica el teorema fundamental de la aritmética.

Proposición: Existen infinitos números primos.

- **Demostración:** Supongamos que la cantidad de primos existentes es finita, y sea

$$p_1 < p_2 < \cdots < p_m$$

la lista de todos los números primos.

Consideremos ahora el siguiente número:

$$N = p_1 \cdot p_2 \cdots p_m + 1.$$

Claramente, $N \neq p_i$ para todo $i \in \{1, \dots, m\}$. Luego, se tiene que N es compuesto. Por el teorema fundamental de la aritmética, N se descompone como producto de potencias de los p_i. Entonces, existe $i \in \{1, \dots, m\}$ tal que $p_i \mid N$. Por otro lado, $p_i \mid p_1 p_2 \cdots p_m$, por lo cual $p_i \mid 1$.

$p_i \mid 1 \Rightarrow p_i = 1$, lo cual es una contradicción por ser p_i primo.

Entonces, N no puede ser compuesto (es decir, es primo), obteniendo así otra contradicción ya que

$$N \notin \{p_1, p_2, \ldots, p_m\}.$$

Por lo tanto, existen infinitos números primos. ■

Aplicación 2 (cálculos alternativos del máximo común divisor y del mínimo común múltiplo):

Dados dos enteros $a, b > 0$, es posible hallar el máximo común divisor y el mínimo común múltiplo entre ellos a partir de sus descomposiciones en factores primos.

Proposición: Sean $a, b \in \mathbb{Z}^+$ con descomposiciones en factores primos dadas por

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \quad y \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m \in \mathbb{N}$. Entonces:

1) $mcd(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m}$ donde

$$\gamma_i = \min\{\alpha_i, \beta_i\} \text{ con } i \in \{1, 2, \ldots, m\}.$$

2) $mcm(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_m^{\delta_m}$ donde

$$\delta_i = \max\{\alpha_i, \beta_i\} \text{ con } i \in \{1, 2, \ldots, m\}.$$

Antes de dar una demostración a las fórmulas anteriores, entendamos primero cómo aplicarlas.

<u>Ejemplo</u>: Hallar el máximo común divisor y el mínimo común múltiplo de $a = 1650$ y $b = 7800$

$$a = 1650 = 2 \cdot 5 \cdot 165 = 2 \cdot 5 \cdot 3 \cdot 55 = 2 \cdot 3 \cdot 5^2 \cdot 11$$
$$b = 7800 = 78 \cdot 100 = 2^2 \cdot 5^2 \cdot 2 \cdot 39 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$$

$$a = 2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13^0$$
$$b = 2^3 \cdot 3 \cdot 5^2 \cdot 11^0 \cdot 13$$

$$\Rightarrow mcd(a,b) = 2 \cdot 3 \cdot 5^2 \cdot 11^0 \cdot 13^0 = 150$$
$$mcm(a,b) = 2^3 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13 = 85800.$$

- **Demostración:**

1) Sea $\gamma_i = \min\{\alpha_i, \beta_i\}$ con $i \in \{1, 2, \dots, m\}$, y considere

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m}.$$

Veamos que si $c|a$ y $c|b$, entonces $c|d$. Esto implicará que $d = mcd(a, b)$.

Por el teorema fundamental de la aritmética, podemos escribir c como

$$c = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_m^{\varepsilon_m}$$

con $\varepsilon_i \in \mathbb{N}$ para todo $i \in \{1, 2, \dots, m\}$.

$$c | a \Rightarrow \varepsilon_i \leq \alpha_i \text{ para todo } i \in \{1, 2, \dots, m\}.$$
$$c | b \Rightarrow \varepsilon_i \leq \beta_i \text{ para todo } i \in \{1, 2, \dots, m\}.$$

$$\varepsilon_i \leq \alpha_i \text{ y } \varepsilon_i \leq \beta_i \Rightarrow \varepsilon_i \leq \min\{\alpha_i, \beta_i\} = \gamma_i$$
para todo $i \in \{1, 2, \dots, m\}$.

Lo anterior implica que $c|d$, y por lo tanto

$$d = mcd(a, b).$$

2) Sabemos que $mcm(a,b) = \dfrac{ab}{mcd(a,b)}$.

Por la parte anterior, tenemos que

$$mcm(a,b) = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \, p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}}{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m}} = \frac{p_1^{\alpha_1+\beta_1} \, p_2^{\alpha_2+\beta_2} \cdots p_m^{\alpha_m+\beta_m}}{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m}}$$

$$= p_1^{\alpha_1+\beta_1-\gamma_1} \, p_2^{\alpha_2+\beta_2-\gamma_2} \cdots p_m^{\alpha_m+\beta_m-\gamma_m}.$$

Tenga en cuenta que

$$\alpha_i + \beta_i = mín\{\alpha_i, \beta_i\} + máx\{\alpha_i, \beta_i\}$$

$$\alpha_i + \beta_i = \gamma_i + \delta_i, \quad \text{para todo } i \in \{1, 2, \dots, m\}.$$

Luego, $mcm(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_m^{\delta_m}$. ■

Aplicación 3 (cantidad de divisores y cuadrados perfectos):

Dado $a \in \mathbb{Z}^+$, denotemos por $Div_+(a)$ al conjunto de divisores positivos de a.

Proposición: Para $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \in \mathbb{Z}^+$, $a \geq 2$, p_i factores primos distintos y $\alpha_i \in \mathbb{Z}^+$ para todo $i \in \{1, 2, \dots, m\}$. Entonces,

$$card(Div_+(a)) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1).$$

<u>Demostración</u>: Sea $c \in Div_+(a)$. Por el teorema fundamental de la aritmética, sabemos que

$$c = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_m^{\varepsilon_m}$$

donde $\varepsilon_i \in \mathbb{N}$ y $\varepsilon_i \leq \alpha_i$ para todo $i \in \{1, 2, \dots, m\}$.

Notamos que elegir c es equivalente a elegir la m-upla $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m)$. Entonces,

$$\begin{aligned}
\operatorname{card}(Div_+(a)) &= \operatorname{card}\left\{(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m) \in \mathbb{N}^m \,/\, \varepsilon_i \leq \alpha_i, \ \forall i \in \{1, 2, \dots, m\}\right\} \\
&= \operatorname{card}\{0, 1, \dots, \alpha_1\} \times \operatorname{card}\{0, 1, \dots, \alpha_2\} \\
&\qquad \times \cdots \times \operatorname{card}\{0, 1, \dots, \alpha_m\} \\
&= (1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_m). \ \blacksquare
\end{aligned}$$

<u>Proposición</u>: Dado $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \in \mathbb{Z}^+$, $a \geq 2$, entonces a es un cuadrado perfecto si y solamente si $2 \mid \alpha_i$ para todo $i \in \{1, 2, \dots, m\}$. De manera más general, existe $b \in \mathbb{Z}^+$ y $r \in \mathbb{Z}^+$ tales que $a = b^r$ si y solamente si $r \mid \alpha_i$ para todo $i \in \{1, 2, \dots, m\}$.

· <u>Demostración</u>: Probemos la versión general.

Supongamos primero que existen $b \in \mathbb{Z}^+$ y $r \in \mathbb{Z}^+$ tales que $a = b^r$.

Por el teorema fundamental de la aritmética, $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ con $q_1 < q_2 < \cdots < q_n$ primos y $\beta_i \in \mathbb{Z}^+$ para todo $i \in \{1, 2, \dots, n\}$.

Luego,

$$a = (q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n})^r = q_1^{r\beta_1} q_2^{r\beta_2} \cdots q_n^{r\beta_n}.$$

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} = q_1^{r\beta_1} q_2^{r\beta_2} \cdots q_n^{r\beta_n}.$$

Por la unicidad de la descomposición en factores primos, tenemos que

$$m = n, \quad p_1 = q_1, \quad p_2 = q_2, \dots, \quad p_m = q_m, \quad \text{y}$$

$$\alpha_1 = r\beta_1, \quad \alpha_2 = r\beta_2, \dots, \quad \alpha_m = r\beta_m.$$

Entonces, $r \mid \alpha_i$ para todo $i \in \{1, 2, \dots, m\}$.

Ahora supongamos que $r \mid \alpha_i$ para todo $i \in \{1, 2, \dots, m\}$. Luego, existen $\beta_i \in \mathbb{Z}^+$ tales que $\alpha_i = r\beta_i$, y así

$$a = p_1^{r\beta_1} p_2^{r\beta_2} \cdots p_m^{r\beta_m} = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m})^r. \quad \blacksquare$$

Ejemplo: Probar que 2401 es un cuadrado perfecto y hallar la cantidad de divisores positivos.

$$2401 = 7 \cdot 343 = 7 \cdot 7 \cdot 49 = 7^4 = (7^2)^2 = 49^2$$

$\#$ de divisores positivos $= (1+4) = 5$.

Congruencias modulares

Este teórico de Matemática Discreta 2 se da los Lunes y Miércoles a las 11:00. Nótese que no decimos que la clase del Miércoles se da a las $11+48=59$ horas. Esto último resultaría poco práctico. La convención de dividir los días en 24 horas hace que los números 11 y 59 representen la misma hora: las 11:00. Por otro lado, note que 11 y 59 tienen el mismo resto al dividir por 24,

$$11 = 0\cdot 24 + 11$$
$$59 = 2\cdot 24 + 11.$$

Generalizando, cualquier número de la forma $24k+11$ representa las 11:00 dentro del sistema de numeración bajo el cual se rige el reloj. La teoría de congruencias modulares nos ayudará a modelar ésta y otras convenciones conocidas.

Definición: Sea $m \in \mathbb{Z}$ fijo, y $a, b \in \mathbb{Z}$, diremos que <u>a es congruente con b módulo m</u>, denotado por

$$a \equiv b \pmod{m},$$

si $m \mid (a-b)$.

Observaciones:

1. $a \equiv b \pmod{0}$ si y solamente si $a = b$
2. $a \equiv b \pmod{n}$ si y solamente si $a \equiv b \pmod{-n}$.
3. $a \equiv 0 \pmod{n}$ si y solamente si $n \mid a$.
4. Para todo $a, b \in \mathbb{Z}$, existe $0 \leq r < |b|$ tal que $a \equiv r \pmod{b}$.

Ejemplo:

$59 \equiv 11 \pmod{24}$.

Las horas del día se cuentan módulo 24.

Los días de la semana se cuentan módulo 7.

Comencemos caracterizando el concepto de congruencia.

Proposición: $a \equiv b \pmod{n}$ si y solamente si a y b tienen el mismo resto al dividir por n.