El Teorema Fundamental de la Aritmética

Ana Ofelia Negrete Fernández

29 de marzo de 2022

1. Introducción

El teorema fundamental de la aritmética afirma que todo entero tiene una descomposición única como producto de primos. Nos referimos a situaciones del tipo

$$8 = 2 \cdot 2 \cdot 2 = 2^3,$$

$$13 = 13^1,$$

$$152 = 2^3 \times 19.$$

Los números primos son los átomos de los números enteros, ya que a partir de multiplicarlos se obtiene cualquier entero, sea éste primo o compuesto. Si z es primo, $z = p^1$. Si z es compuesto, $z = p_1^{k_1} \cdot p_2^{k_2} \cdot p_n^{k_n}$, siendo $p_1, p_2, \ldots, p_n$ números primos. E inversamente, a cualquier número se le puede encontrar su descomposición. Es este hecho lo que hoy demostraremos.

Hay una infinidad de primos; Euclides fue el primero en notarlo. Los números primos siguen siendo interesantes para los matemáticos hoy en día; primero por la irregularidad con que van apareciendo en la recta numérica y porque hay muchas cosas que aún no se sabe acerca de su raro comportamiento. Por ejemplo, se conjetura que hay infinitos "primos gemelos", es decir, se cree que siempre es posible encontrar dos primos a y b que estén distanciados en dos unidades; no importa qué tan alejados estén del cero. El 3 y el 5 son primos gemelos. También los son el 17 y el 19. Cuando los números son muy grandes ya es difícil verificar que cierto número es primo, y si además hay infinitos de ellos, avanzar caso por caso sería interminable. Mejor estrategia es intentar encontrar patrones en estos números, en aras de resolver el problema de un modo más general.

Así, dado un número primo p, éste es de la forma $4n+1$ o de la forma $4n-1$ para alguna $n \in \mathbb{N}$. A su vez, para aquéllos primos que pertenecen a la primera categoría, que son los de la forma $4n+1$, siempre existe su expresión como una suma de cuadrados: $p = 4n + 1 = m^2 + n^2$, $n, m \in \mathbb{Z}$. Pero a los primos de la segunda categoría es imposible expresarlos como suma de cuadrados (puedes demostrar estos dos hechos). El matemático Euler fue el primero en oficialmente verificar estos resultados que actualmente forman parte de un curso básico de teoría de números.

Los números primos también han encontrado aplicaciones en criptografía, pues es bien sabido que si se eligen dos primos p_1 y p_2 tales que al multiplicarlos se obtenga un número compuesto z de más de 100 dígitos, y si luego se establece que p_1 y p_2 sean la contraseña de mi mensaje cifrado pero yo únicamente doy a conocer el número compuesto z a otra persona, entonces a una computadora le resultaría imposible factorizar z en un corto lapso de tiempo. ¡Le tomaría años! De ahí que la contraseña secreta sería indescifrable; más aún si ésta se cambiara cada año.

Ahora, lo que se conoce como el "teorema fundamental de la aritmética" deja de ser válido si consideramos a los enteros como un subconjunto de otra estructura numérica como los complejos. Ya que por ejemplo,

$$12 = (1 + \sqrt{-11})(1 - \sqrt{-11})$$

pero también

$$12 = (2 + \sqrt{-8})(2 - \sqrt{-8}).$$

Esto quiere decir que en $\mathbb{C}$ es posible encontrar dos o más factorizaciones para un mismo entero.

Pero si nos restringimos a $\mathbb{Z}$ (o hasta $\mathbb{R}$), podemos afirmar que la descomposición de un entero en potencias de primos es única salvo por el orden en que se hagan las multiplicaciones. Por ejemplo, $152 = 2{\cdot}2{\cdot}2{\cdot}19 = 2{\cdot}19{\cdot}2^2$, donde el orden de los multiplicandos es distinto en ambas factorizaciones, pero los números a ser multiplicados son exactamente iguales.

2. Propiedades de los números primos

Antes de pasar al teorema del día, recordemos las necesarias definiciones y proposiciones.

Proposición 1. Sean $x, y \in \mathbb{Z}$.

$$x \mid y \iff -x \mid y \iff x \mid -y \iff -x \mid -y \ .$$

Dem. Sea $z \in \mathbb{Z}$ tal que $xz = y$. Así pues, $y = xz = (-1)(-1)(xz) = (-x)(-z)$, lo que demuestra que, x es divisor de y si y sólo si $-x$ también es divisor de y.

Luego, $-x \mid y \iff (-x)(-z) = y \iff (-1)(-x)(-z) = (-1)y \iff (x)(-z) = -y \iff x \mid -y$.

Finalmente, $x \mid -y \iff (x)(-z) = -y \iff (-x)(z) = -y \iff -x \mid -y$.

□

Proposición 2. Sean $n, m \in \mathbb{Z}^+$. Si $n \mid m$, entonces $n \leq m$.

Dem. Sea $x \in \mathbb{Z}^+$ tal que $nx = m$. Ya que $x > 0, n > 0, m > 0$, entonces $0 < n \leq nx = m$. Por transitividad, $n \leq m$.

□

La noción de divisibilidad nos permite definir lo que es un número primo:

Definición (Número primo). Un entero $z \in \mathbb{Z}$ es primo si y sólo si tiene exactamente cuatro divisores: $1,\ -1,\ z$ y $-z$.

Proposición 3. 2 es primo.

Dem. Supongamos que $x \in \mathbb{Z}$ divide a 2. Como x es divisor de 2 y $-x$ también lo es, asumamos sin pérdida de generalidad, $x > 0$. Como $x \leq 2$, entonces $x = 1$ o $x = 2$. Luego, 2 tiene exactamente cuatro divisores, que son 1, 2, -1 y -2.

Proposición 4. Sean $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ y $(a, b) = 1$, entonces $a \mid c$.

Dem. Esto fue detallado en la sección de máximo común divisor.

Proposición 5. Sean $z, p \in \mathbb{Z}$, con p primo. Si $p \nmid z$, entonces $(p, z) = 1$.

Dem. Ya que $(p, z) > 0$ y (p, z) debe dividir tanto a z como a p, entonces $(p, z) \in \{1, p\}$. Por lo que, si $p \nmid z$, entonces $(p, z) \neq p$ y forzosamente, $(p, z) = 1$.

Ahora bien, en la sección de Ideales y divisibilidad se mencionó que los ideales surgieron como una generalización de propiedades elementales que cumplen los enteros. Mejor aún, propiedades que los números primos cumplen en específico también son generalizables a lo que se conoce como ideales primos. Ahí se trató como un caso particular de ideal primo, la siguiente propiedad que cumplen los primos en $\mathbb{Z}$:

Proposición 6. Sea $p \in \mathbb{Z}$, p primo. Si $p \mid ab,\ \ a, b \in \mathbb{Z}$, entonces $p \mid a$ o $p \mid b$.

Dem. Si $p \mid a$ no hay nada que demostrar.

Sea p primo tal que $p \nmid a$. Entonces, por la proposición 4, $(p, a) = 1$. Como $p \mid ab$ y $(p, a) = 1$, entonces $p \mid b$ (proposición 3).

3. Demostración del teorema fundamental de la aritmética

Teorema fundamental de la aritmética. Si $z \in \mathbb{Z}^+$, con $z > 1$, existe un único $k \in \mathbb{N}$ y únicos $p_1, p_2, \ldots, p_k$ números primos tales que $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.

Consideremos el número $1060 = 2^2 \cdot 5 \cdot 53$. Ciertamente, para este caso existe $k = 4,\ 4 \in \mathbb{N}$, tal que $1060 = p_1 \cdot p_2 \cdot p_3 \cdot p_4$, con $p_1 = 2, p_2 = 2, p_3 = 5, p_4 = 53$. Y si intentáramos factorizar tal número varias veces, sólo lo conseguiríamos expresar como producto de estos cuatro números, tanto que aseguraríamos que la factorización es única (aunque el por qué de esto no es tan evidente).

¿Pero cómo podríamos demostrar que la aseveración es cierta para cualquier $z \in \mathbb{Z}^+$? Inducción parece un buen camino; primero verificar que el enunciado es válido para el caso base $n = 2$, luego suponer que todos los enteros menores que z también son válidos, y finalmente usar esto para ver que z mismo también es factorizable como producto de primos.

Una vez concluido que siempre existe una factorización, demostraremos su unicidad.

Dem.- Procedemos a probar la existencia de la factorización en primos, por inducción sobre z:

Caso base. Ya que $z > 1$, la base inductiva es $z = 2$. 2 es primo y 2 divide a 2, por lo que su factorización en primos es él mismo.

Base inductiva. Suponemos que $z > 2$ y que todo $w \in \mathbb{Z}^+$ menor a z también tiene una factorización en primos.

Por demostrar: z tiene una factorización en primos.

Si z es primo, existe su factorización $z = z$. Supongamos entonces que z no es primo. Por definición de número compuesto, $z = ab$, y además podemos suponer $a > 0$ ($-a$ también es divisor de z, por lo que no importa cuál se elija, si a o $-a$). Dado que $z > 0$ y $a > 0$, y como el producto de números positivos es positivo, $b > 0$.

Como a es distinto de z, entonces $b \neq 1$, de modo que $b \geq 2$. Observamos entonces que $a < z$, de lo contrario, $a \geq z$ y $b \geq 2$ implicaría que $z = ab \geq 2z$, lo cual es una contradicción pues $2z$ es positivo, estrictamente mayor a z. Y por el mismo argumento, $b < z$.

Todos los números menores que z eran factorizables como producto de primos, así que, por la hipótesis de inducción, existen $s \in \mathbb{N}$ y $q_1, \ldots, q_s$ primos tales que $a = q_1 \cdot q_2 \cdot ... \cdot q_s$. Asimismo existen $t \in \mathbb{N}$ y $r_1, \ldots, r_t$ números primos tales que $b = r_1 \cdot r_2 \cdot \ldots \cdot r_t$.

Por lo anterior, $z = (q_1 \cdot q_2 \cdot ... \cdot q_s)(r_1 \cdot r_2 \cdot \ldots \cdot r_t)$, un producto de primos, y esto termina la primera parte de la prueba.

Procedemos ahora a demostrar la unicidad, suponiendo que existen dos factorizaciones diferentes para z. Entonces el conjunto

$$A = \{z \in \mathbb{Z}^+ \mid z > 1, \text{y } z \text{ tiene dos factorizaciones en primos}\} \neq \emptyset.$$

Tratándose de números positivos y por lo tanto, naturales, por el principio del buen orden, existiría un elemento mínimo en A, llamémosle u. Así,

$$u = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

con k distinto de l, o con $p_1 \cdot p_2 \cdot \ldots \cdot p_k \neq q_1 \cdot q_2 \cdot \ldots \cdot q_l$. Asumamos además que el orden de los factores p_i y q_j es no decreciente.

Agrupando términos, $(p_1)(p_2 \cdot \ldots \cdot p_k) = q_1 \cdot q_2 \cdot \ldots \cdot q_l$, es decir $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_l$. Y por las proposiciones 6 y 5, $p_1 \mid q_1$ o bien, $(p_1, q_1) = 1$.

Si $p_1 \mid q_1$, como q_1 es primo, sus divisores son únicamente $1, -1, q_1$ y $-q_1$. Pero p_1 es primo mayor que cero y 1 no es primo. Así, $p_1 = q_1$.

En el segundo caso, es decir, si $(p_1, q_1) = 1$, entonces, por la proposición 5, $p_1 \mid q_2 \cdot q_3 \cdot \ldots \cdot q_l$. Y nuevamente surgen dos casos: $p_1 \mid q_2$ o $(p_1, q_2) = 1$. En el primer caso, $p_1 \mid q_2$ implica $p_1 = q_2$. En el segundo caso, $(p_1, q_2) = 1$ implica $p_1 \mid q_3 \cdot q_4 \cdot \ldots \cdot q_k$.

Iterando el proceso, se atravesaría la lista de q_js hasta llegar a que $p_1 = q_{l-1} \cdot q_l$. Entonces, o bien $p_1 = q_{l-1}$ o bien $p_1 = q_l$. Concatenando con todo lo que ya se tenía, concluimos que $p_1 = q_1$ o $p_1 = q_2$ o $\ldots$ o $p_1 = q_l$. De modo que p_1 es uno de los factores primos en $q_1 \cdot q_2 \cdot \ldots \cdot q_l$, digamos $p_1 = q_j$ para cierta $j \in \mathbb{N}$.

Simétricamente sucede lo mismo; es decir, ya que $u = (q_1)(q_2 \cdot \ldots \cdot q_l) = p_1 \cdot \ldots \cdot p_k$, entonces q_1 divide a $p_1 \cdot \ldots \cdot p_k$, de donde iniciando el mismo proceso del anterior párrafo y analizando todos los casos, se obtendría que $q_1 = p_1$ o $q_1 = p_2$ o $\ldots$ o $q_1 = p_k$. Por lo que q_1 es alguno de los factores primos en $p_1 \cdot \ldots \cdot p_k$, digamos que $q_1 = p_i$. Así,

$$p_i \leq q_1 \leq q_j \leq p_1.$$

Por lo tanto,

$$p_1 = q_1.$$

Así, usando la ley de cancelación en $\mathbb{Z}$, $p_1 \cdot p_2 \cdot \ldots \cdot p_k = p_1 \cdot q_2 \cdot \ldots \cdot q_l$ implica que

$$u_1 = p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_l,$$

con $u_1 < u$.

Volviendo a iterar todo el procedimiento y concatenando, al final se obtiene que $p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_k = q_l$, y así deducimos que $k = l$. Por lo tanto, cada término en la primera y la segunda factorización de u es exactamente igual. Pero esto contradice el hecho de que o las factorizaciones eran distintas, o k era distinto de l.

La contradicción sucedió por suponer que existía un conjunto $A \neq \emptyset$ de enteros con dos o más factorizaciones. Así pues, $A = \emptyset$.

□

4. Ejercicios

- Encuentra la factorización en primos de 100, 130, 1960, 109 y 713.
- Encuentra los conjuntos de divisores positivos de cada uno de los números del inciso anterior.
- Hallar el menor múltiplo positivo de 945 que sea un cuadrado.
- Hallar el número de divisores de 2160 y calcular su suma.