Teoría de Números

En teoría de números el universo del discurso es el conjunto de números enteros $\mathbb{Z}$. Muchas de sus propiedades tienen que ver con divisibilidad.

Definición

Si $a \mid b$ entonces a se llama divisor (ó factor) de b y b se llama múltiplo de a.

Nótese que la relación de *múltiplo* es la relación inversa de divisibilidad. Esto es

$$a \mid b \Leftrightarrow b \text{ es múltiplo de } a \Leftrightarrow b \mid^{-1} a.$$

Teorema

Sean $a, b, c \in \mathbb{Z}$. Entonces

1. *si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$;*
2. *si $a \mid b$ entonces $a \mid bc$;*
3. *si $a \mid b$ y $b \mid c$ entonces $a \mid c$.*

Demostración.

1. Tenemos que existen $k_1, k_2 \in \mathbb{Z}$ tales que $b = k_1 a$ y $c = k_2 a$, luego

$$\begin{aligned} b + c &= k_1 a + k_2 a \\ &= (k_1 + k_2) a \end{aligned}$$

   con $k_1 + k_2 \in \mathbb{Z}$. Entonces, por definición, $a \mid (b + c)$.
2. Tarea.
3. Tarea.

Corolario

Sean $a, b, c \in \mathbb{Z}$. *Si* $a \mid b$ *y* $a \mid c$ *entonces* $a \mid (mb + nc)$, *para cualesquiera* $m, n \in \mathbb{Z}$.

Demostración.

Si $a \mid b$ y $a \mid c$ entonces $a \mid mb$ y $a \mid nc$ por (2) del teorema inmediato anterior. Luego, por (1) del mismo teorema, $a \mid (mb + nc)$. $\square$

Recordemos:

Definición

Un número $p \in \mathbb{N}$ es primo si cumple:

1. $p > 1$;
2. *los únicos divisores positivos de p son 1 y p.*

Ejemplo

El número 7 es primo porque $7 > 1$ y además sus únicos divisores positivos son 1 y 7.

Ejemplo

Son primos: $2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47$.

Definición

Un número $n \in \mathbb{N}$ se dice compuesto si cumple que

1. $n > 1$
2. *n no es primo*

Ejemplo

El número 9 es compuesto porque $9 > 1$ y $3 \mid 9$ por lo que 9 no es primo.

Teorema (Fundamental de la Aritmética)

Sea $n \in \mathbb{Z}$ tal que $n > 1$. Entonces n se puede escribir como un producto de números primos de forma única.

La razón de ser del teorema fundamental del la aritmética es que, dado un $n \in \mathbb{Z}$ con $n > 1$, cumple uno de dos casos: n es primo ó compuesto.

- Si $n = p$ es primo, entonces n se considera el producto de un sólo primo: p.
- Si n es compuesto entonces se puede escribir como un producto de enteros $n = m_1 m_2$ con $1 < m_1 < n$ y $1 < m_2 < n$. Entonces a cada uno de éstos factores se le puede aplicar el mismo razonamiento recursivamente. Eso es, m_1 es primo o compuesto; similarmente m_2 es primo o compuesto. Etc.

Para la unicidad del teorema fundamental de la aritmética se requiere más trabajo.
El producto del teorema fundamental de la aritmética se conoce como *factorización prima*.

Ejemplo

Encontrar la factorización prima de 100.

Sol.

$$\begin{aligned} 100 &= 2 * 50 \\ &= 2 * 2 * 25 \\ &= 2 * 2 * 5 * 5 \end{aligned}$$

Luego la factorización prima de 100 es:

$$100 = 2^2 * 5^2.$$

Ejemplo

Encontrar la factorización prima de 999.

Sol.

$$\begin{aligned} 999 &= 3 * 333 \\ &= 3 * 3 * 111 \\ &= 3 * 3 * 3 * 37, \end{aligned}$$

entonces, como 37 es primo, la factorización prima de 999 es

$$999 = 3^3 * 37.$$

Ejemplo

Encontrar la factorización prima de 641.

Sol.

La factorización prima de 641 es

$$641 = 641$$

pues 641 es primo. □

Para verificar que 641 es primo con relativa facilidad se puede usar el *criterio de la raíz*.

Teorema (Criterio de la raíz)

Si $n \in \mathbb{N}$ es un número compuesto, entonces existe p primo tal que $p \mid n$ y $p \leq \sqrt{n}$.

Dem. Si n es compuesto entonces tiene un divisor a tal que $1 < a < n$. Entonces existe $k \in \mathbb{N}$ tal que $n = ka$. Nótese que $k > 1$.

Si ocurriera que $k > \sqrt{n}$ y $a > \sqrt{n}$ entonces, multiplicando lado a lado éstas desigualdades obtenemos que

$$\underbrace{ak}_{n} > \underbrace{\sqrt{n}\sqrt{n}}_{n}$$

es decir, $n > n$: absurdo.

Así, necesariamente ocurre que $k \leq \sqrt{n}$ ó $a \leq \sqrt{n}$:

1. Si $k \leq \sqrt{n}$ entonces, por el teorema fundamental de la aritmética, existe p primo tal que $p \mid k$. Además, por definición de k, $k \mid n$, luego por transitividad $p \mid n$. También $p \leq k \leq \sqrt{n}$. En resumen, hemos obtenido:

$$p \text{ primo, } p \leq \sqrt{n} \text{ y } p \mid n.$$

2. Si $a \leq \sqrt{n}$, entonces, de nuevo por el teorema fundamental de la aritmética, existe q primo tal que $q \mid a$ y se procede como en el caso anterior para obtener

$$q \text{ primo, } q \leq \sqrt{n} \text{ y } q \mid n.$$

Ejemplo

El número 641 es primo porque si fuera compuesto existiría un primo p tal que $p \mid 641$ y $p \leq \sqrt{641} \approx 25.31$, de donde $p = 2, 3, 7, 11, 13, 17, 19$ ó 23. Pero ninguno de éstos primos divide a 641. Por lo tanto 641 es primo.

La relación de divisivilidad y el *algoritmo de la división* están a su vez relacionados.

Teorema (Algoritmo de la división)

Sea $a \in \mathbb{Z}$ y d un entero positivo. Entonces existen q, r enteros tales que

$$a = qd + r \text{ y } 0 \leq r < d.$$

Tales enteros q, r son únicos.

Notación: El número $q = a$ **div** d se llama el *cociente* al dividir a por d. Mientras que $r = a$ **mod** d se llama el *residuo* al dividir a por d.

El algoritmo de la divisón no es ás que la notación de "casita" al dividir enteros:

$$\begin{array}{rl} & q \\ d & \overline{)\,a} \\ & r \end{array}$$

Ejemplo

Tenemos que

$$\begin{array}{rrrr} & 1 & 2 & 8 \\ 5 & \vert 6 & 4 & 1 \\ & 1 & 4 & \\ & & 4 & 1 \\ & & & 1 \end{array}$$

que se obtuvo con el llamado *algoritmo largo de la división*. Esto indica la siguiente ecuación:

$$641 = 128 * 5 + 1.$$

De donde

$$128 = 641 \textbf{ div } 5, \quad 1 = 641 \textbf{ mod } 5.$$

Nótese que se cumplen las siguientes equivalencias:

$$d \mid a \Leftrightarrow 0 = a \ \mathbf{mod}\ d \Leftrightarrow a/d \in \mathbb{Z}.$$

Ejemplo

$$2 \nmid 641 \text{ pues } 0 \neq 641 \ \mathbf{mod}\ 2 = 1;$$
$$3 \nmid 641 \text{ pues } 641/3 \notin \mathbb{Z};$$
$$7 \nmid 641 \text{ pues } 641/7 \notin \mathbb{Z}.$$

Ejemplo

Calcular el residuo de -11 dividido por 3.

Sol.

Tenemos que

$$\begin{array}{r|r} & -4 \\ \hline 3 & -11 \\ & 1 \end{array}$$

esto es:

$$-11 = -4 * 3 + 1.$$

Entonces

$$1 = -11 \ \textbf{mod}\ 3.$$

Obsérvese que el poner

$$\begin{array}{rr} & -3 \\ 3 & \big| \overline{-11} \\ & -2 \end{array}$$

es incorrecto porque el residuo NO cumple $0 \leq -2 < 3$, a pesar de que es correcta la ecuación

$$-11 = -3 * 3 - 2$$

Teorema

Hay una infinidad de números primos.

Ejemplo

Muestre que el número 101 es primo.

Sol.

Por el criterio de la raíz: si 101 fuera compuesto entonces existiría un primo p tal que $p|101$ y $p \leq \sqrt{101} \approx 10.05$. Entonces $p = 2, 3, 5$ ó 7. Pero $2 \nmid 101$ pues $101/2 \notin \mathbb{Z}$, $3 \nmid 101$ pues $101/3 \notin \mathbb{Z}$, $5 \nmid 101$ pues $101/5 \notin \mathbb{Z}$, y ni $7 \nmid 101$ pues $101/7 \notin \mathbb{Z}$. En cualquier caso se obtiene una contradicción. Por lo tanto 101 es primo. $\square$