Unidad 4 / Escenario 7

Lectura fundamental

# Números enteros

## Contenido



**Palabras clave:** números enteros, divisibilidad, números primos

# Introducción

En ciencias de la computación uno de los conjuntos numéricos que posee amplia aplicación es el conjunto de los números enteros ($\mathbb{Z}$). Estando presente en campos como la teoría de la información, arquitectura de computadores, computación gráfica y análisis de algoritmos. El estudio de este conjunto y sus propiedades se conoce como **teoría de números**. Por lo tanto, el objetivo de la lectura es presentar la estructura, los conceptos básicos y propiedades esenciales de este conjunto numérico.

**Definición 1.** El conjunto de los números enteros, $\mathbb{Z}$ corresponde a:

$$\mathbb{Z} = \{-x : x \in \mathbb{N}, x \neq 0\} \cup \mathbb{N}$$

Es decir, el conjunto de los números enteros corresponde a $\{-1, -2, -3, \ldots\} \cup \{0, 1, 2, 3, \ldots\}$. En este conjunto existen las operaciones de adición $(+)$, sustracción $(-)$ y multiplicación $(\cdot)$, además se define la relación de orden $a \leq b$. Es a través de estas operaciones y relación que se definirán nuevos objetos y conceptos.

# 1. Divisibilidad

Aunque la división entre números enteros no es una operación definida en todos los casos, por ejemplo el resultado de $7 \div 3$ no es un número entero, es posible definir a través de esta la siguiente relación:

**Definición 2.** Si $a, b \in \mathbb{Z}$, $a \neq 0$ se dice que $a$ *divide* $b$ si existe un número entero $c$ tal que $b = ac$. Esta situación se denota como

$$a \mid b$$

De forma equivalente, $a \mid b$ si $b \div a$ es un número entero.

**Ejemplo 1.**

1. $3 \mid 15$ dado que existe un entero $c$ tal que $3c = 15$, en este caso $c = 5$
2. $-4 \mid 12$ dado que $-4 \cdot (-3) = 12$
3. Para todo entero $a \neq 0$ se tiene que $a \mid 0$ dado que $a \cdot 0 = 0$
4. $7 \mid 7$ puesto que $7 \cdot 1 = 7$

Cuando $a$ **no divide** a $b$ se denota por:

$$a \nmid b$$

El siguiente teorema presenta algunas propiedades de la relación de divisibilidad.

**Teorema 1.** Si $a, b, c \in \mathbb{Z}$. Entonces:

1. $a \mid a$, $a \mid -a$
2. $1 \mid a$, $-1 \mid a$
3. Si $a \mid b$ entonces $a \mid bc$
4. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$
5. Si $a \mid b$ y $a \mid c$ entonces $a \mid (bx + cy)$ para todo $x, y \in \mathbb{Z}$
6. Si $a \mid b$ y $b \mid a$ entonces $a = b$ o $a = (-b)$

Las propiedad 1 indica que la relación de divisibilidad es reflexiva. La propiedad 4 establece que la divisibilidad es transitiva. Sobre los números enteros la relación no es antisimétrica, pero si se restringe a los números naturales, la relación de divisibilidad es una relación de orden.

La propiedad 5 menciona que si $a$ divide a los números $b$ y $c$ entonces divide a cualquier combinación lineal $bx + cy$ de estos números.

La demostración de algunas de estas propiedades se presenta a continuación. Revisarlas con detalle brindará una comprensión de las propiedades.

***Demostración:*** El lector puede demostrar las propiedades 1, 2 y 3 siguiendo la definición de divisibilidad. Se demostrará los numerales 4, 5 y 6:

(4):

$$\begin{aligned}
& a \mid b \wedge b \mid c \\
\Rightarrow\ & ax = b \wedge by = c \quad \text{para algún } x, y \in \mathbb{Z} \quad \langle \text{ definición de: } \mid \ \rangle \\
\Rightarrow\ & (ax)y = c \quad \langle \text{ sustitución de } b \text{ por } ax \ \rangle \\
\Rightarrow\ & a(xy) = c \quad \langle \text{ propiedad asociativa de la multiplicación } \rangle \\
\Rightarrow\ & a \mid c \quad \langle \text{ definición de: } \mid \ \rangle
\end{aligned}$$

(5):

$$\begin{aligned}
& a \mid b \wedge a \mid c \\
\Rightarrow\ & a \cdot r = b \wedge a \cdot t = c \quad \text{para algún } r, t \in \mathbb{Z} \quad \langle \text{ definición de: } \mid \quad \rangle \\
\Rightarrow\ & a \cdot r \cdot x = b \cdot x \wedge a \cdot t \cdot y = c \cdot y \text{ para cualquier } x, y \in \mathbb{Z} \quad \langle \text{ propiedad de la igualdad entre números enteros } \rangle \\
\Rightarrow\ & arx + aty = bx + cy \quad \langle \text{ propiedad de la igualdad } \rangle \\
\Rightarrow\ & a(rx + ty) = bx + cy \quad \langle \text{ factor común } \rangle \\
\Rightarrow\ & a \mid bx + cy \quad \langle \text{ definición de: } \mid \quad \rangle
\end{aligned}$$

(6):

$$\begin{aligned}
& a \mid b \wedge b \mid a \\
\Rightarrow\ & a \cdot r = b \wedge b \cdot t = a \quad \text{para algún } r, t \in \mathbb{Z} \quad \langle \text{ definición de: } \mid \quad \rangle \\
\Rightarrow\ & (ar)t = a \quad \langle \text{ sustitución de } b \text{ por } ar \quad \rangle \\
\Rightarrow\ & a(rt) = a \quad \langle \text{ propiedad asociativa de la multiplicación } \rangle \\
\Rightarrow\ & rt = 1 \quad \langle \text{ propiedad cancelativa } \rangle \\
\Rightarrow\ & (r = 1 \wedge t = 1) \text{ o } (r = -1 \wedge t = -1) \quad \langle \text{ análisis de casos } rt = 1 \rangle \\
\Rightarrow\ & a = b \text{ o } a = -b \quad \langle \text{ sustitución en } a \cdot r = b \wedge b \cdot t = a \rangle
\end{aligned}$$

$\diamondsuit$

Para observar la aplicación de estas propiedades, revise con detalle los siguientes ejemplos.

**Ejemplo 2.** Probar que $15 \mid (30^5 - 45)$

***Solución:*** Observe que $15 \mid 30$ y $15 \mid 45$ entonces aplicando la propiedad 5 del teorema 1 con $x = 30^4$ , $y = -1$ entonces:

$$15 \mid \left(30 \cdot 30^4 + 45 \cdot (-1)\right)$$

luego

$$15 \mid \left(30^5 - 45\right)$$

$\diamondsuit$

**Ejemplo 3.** Probar que $100 \mid (11^{10} - 1)$.

***Solución:*** Observe que:

$$\begin{aligned}
11^{10} - 1 &= (10+1)^{10} - 1 \\
&= 10^{10} + \binom{10}{1}10^9 + \binom{10}{2}10^8 + \cdots \binom{10}{8}10^2 + \binom{10}{9}10 + 1 - 1 \quad \langle \text{ teorema del binomio} \rangle \\
&= 10^{10} + \binom{10}{1}10^9 + \binom{10}{2}10^8 + \cdots \binom{10}{8}10^2 + \binom{10}{9}10 \\
&= 10^{10} + \binom{10}{1}10^9 + \binom{10}{2}10^8 + \cdots \binom{10}{8}10^2 + 10 \cdot 10 \\
&= 10^{10} + \binom{10}{1}10^9 + \binom{10}{2}10^8 + \cdots \binom{10}{8}10^2 + 10^2
\end{aligned}$$

Ahora, $100 \mid 10^{10}$, $100 \mid 10^9$, $\ldots$, $100 \mid 10^2$ entonces aplicando la propiedad 5 del teorema 1 se obtiene que:

$$100 \mid \left(10^{10} + \binom{10}{1}10^9 + \binom{10}{2}10^8 + \cdots \binom{10}{8}10^2 + 10^2\right)$$

luego

$$100 \mid (11^{10} - 1)$$

$\diamondsuit$

**Ejemplo 4.** Probar que para todo $n \geq 1$, $2 \mid n(n+1)$

***Solución:*** Dado que en este caso se desea probar una propiedad para los números naturales mayores o iguales a 1 entonces se utilizará el principio de inducción matemática con $Q(k) : 2 \mid k(k+1)$.

**Caso base:** Si $n = 1$ entonces $n(n+1) = 2$ y como

$$2 \mid 2$$

entonces $2 \mid n(n+1)$ y por lo tanto el caso base $(Q(1))$ se cumple.

**Paso inductivo:** Suponiendo que $Q(n) : 2 \mid n(n+1)$ se cumple, utlizando el hecho que:

$$\begin{aligned}(n+1)((n+1)+1) &= n(n+1) + n + (n+1) + 1 \\ &= n(n+1) + 2n + 2\end{aligned}$$

y que $2 \mid 2n$ y $2 \mid 2$ entonces por la propiedad 5 del teorema 1 se concluye que

$$2 \mid (n(n+1) + 2n + 2) = (n+1)(n+2)$$

con lo cual la propiedad $Q(n+1) : 2 \mid (n+1)(n+2)$ se cumple.

En el caso que $a \mid b$ se dice que $a$ es un **divisor** de $b$. Por ejemplo, $-6$ es un divisor de 30 dado que $-6 \mid 30$.

**Definición 3.** Un entero positivo $p > 1$ se denomina un número *primo* si los únicos divisores positivos son 1 y $p$. Un número entero positivo mayor a 1 que no sea primo se denomina *compuesto*.

**Ejemplo 5.**

- $p = 13$ es un número primo, dado que sus únicos divisores positivos son 1 y 13.
- $n = 507$ es un número compuesto, dado que 39 es un divisor positivo de $n$ distinto de 1 y 507.

**Teorema 2.** Si $n$ es un número compuesto, entonces existe un número primo $p$ tal que $p \mid n$.

***Demostración:*** Supongamos que existen números enteros $n$ compuestos para los cuales ningún número primo $p$ satisface $p \mid n$. Sea $B$ la colección de estos números, como $B \neq \emptyset$ entonces $B$ tiene elemento mínimo $k$ (principio de buen orden). Como $k \in B$ entonces $k$ es compuesto, por lo tanto existen enteros positivos $a_1, a_2$ tales que $k = a_1a_2$ y $1 < a_1, a_2 < k$, así que $a_1 \notin B$ entonces $a_1$ es un número primo o divisible por un número primo, con lo cual existe $p$ primo tal que $p \mid a_1$ y como $a_1 \mid k$ entonces $p \mid k$, lo que es una contradicción. $\diamondsuit$

**Teorema 3.** Existen infinitos números primos.

***Demostración:*** Suponga que existen finitos números primos, sea $p_1, p_2, \ldots, p_k$ la lista de todos los primos. Construya el número $d = p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k + 1$, este número no puede ser primo dado que $d > p_j$ para $j = 1, 2, \ldots, k$ y la lista de todos los primos es $p_1, p_2, \ldots, p_k$. Por lo tanto $d$ es un número compuesto y por el teorema 2 se tiene que existe un primo $p_l$ tal que $p_l \mid d$, pero $p_l \mid p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k$ luego por la propiedad 5 del teorema 1 se tiene que $p_l \mid (d - p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k)$ es decir $p_l \mid 1$, lo que es una contradicción. $\diamondsuit$

## 1.1. Máximo común divisor

**Definición 4.** Sean $a, b \in \mathbb{Z}$ enteros, se dice que un entero positivo $c$ es un *divisor común* de $a$ y $b$ si $c \mid a$ y $c \mid b$.

Es decir, un número $c$ es un divisor común de los números enteros $a$ y $b$ si las divisones $a \div c$ y $b \div c$ son exactas.

**Ejemplo 6.** Un divisor común de $-15$ y $75$ es $5$, dado que $5 \mid -15$ y $5 \mid 75$

**Ejemplo 7.** Los divisores comunes de $140$ y $210$ son $1, 2, 5, 7, 70$.

**Definición 5.** Si $a, b \in \mathbb{Z}$ donde $a \neq 0$ o $b \neq 0$, el máximo de los divisores comunes de $a, b$ se denomina *máximo común divisor* de $a$ y $b$ y se denota por $mcd(a, b)$.

**Ejemplo 8.**

1. $mcd(140, 210) = 70$
2. $mcd(42, 70) = 14$
3. $mcd(231, 1820) = 7$

**Teorema 4.** Sean $a, b \in \mathbb{Z}$ donde $a \neq 0$ o $b \neq 0$ entonces $c \in \mathbb{Z}$ positivo es el *máximo común divisor* de $a$ y $b$ si:

1. $c \mid a$ y $c \mid b$
2. Para cualquier divisor común $s$ de $a, b$ se tiene que $s \mid c$

Pero, ¿cómo se halla $mcd(a, b)$ para $a, b$ enteros positivos?. Una opción es calcular los divisores comunes de $a$, $b$ y luego seleccionar el máximo, este método es ineficiente si los valores de $a$ y $b$ son grandes. El siguiente teorema proporciona un procedimiento efectivo en términos computacionales para determinar $mcd(a, b)$.

**Teorema 5** (Algoritmo de Euclides.). Si $a, b \in \mathbb{Z}$ positivos con $a < b$ entonces aplicando el siguiente algoritmo:

$$\begin{array}{lr}
\textbf{Paso 1: Hallar } q_1, r_1 \text{ tal que } a = b \cdot q_1 + r_1 & 0 < r_1 < b \\
\textbf{Paso 2: Hallar } q_2, r_2 \text{ tal que } b = r_1 \cdot q_2 + r_2 & 0 < r_2 < r_1 \\
\textbf{Paso 3: Hallar } q_3, r_3 \text{ tal que } r_1 = r_2 \cdot q_3 + r_3 & 0 < r_3 < r_2 \\
\vdots & \\
\textbf{Paso i: Hallar } q_i, r_i \text{ tal que } r_{i-2} = r_{i-1} \cdot q_i + r_i & 0 < r_i < r_{i-1} \\
\vdots & \\
\textbf{Continuar hasta que } r_k = 0. &
\end{array}$$

Se tiene que

$$mcd(a, b) = r_{k-1}$$

**Ejemplo 9.** Determinar $mcd(687, 234)$.

***Solución:*** Aplicando el algoritmo de Euclides, se obtiene:

$$\begin{aligned}
\textbf{Paso 1: } & 687 = 234(2) + 219 \\
\textbf{Paso 2: } & 234 = 219(1) + 15 \\
\textbf{Paso 3: } & 219 = 15(14) + 9 \\
\textbf{Paso 4: } & 15 = 9(1) + 6 \\
\textbf{Paso 5: } & 9 = 6(1) + 3 \\
\textbf{Paso 6: } & 6 = 3(3) + 0
\end{aligned}$$

por lo tanto $mcd(687, 234) = 3$ ♢

**Ejemplo 10.** Determinar $mcd(250, 111)$.

***Solución:*** Aplicando el algoritmo de Euclides, se obtiene:

$$\begin{aligned}
\textbf{Paso 1: } & 250 = 111(2) + 28 \\
\textbf{Paso 2: } & 111 = 28(3) + 27 \\
\textbf{Paso 3: } & 28 = 27(1) + 1 \\
\textbf{Paso 4: } & 27 = 1(27) + 0
\end{aligned}$$

por lo tanto $mcd(250, 111) = 1$ ♢

**Ejemplo 11.** Determinar $mcd(1001, 275)$.

***Solución:*** Aplicando el algoritmo de Euclides, se obtiene:

$$\begin{aligned}
\textbf{Paso 1: } & 1001 = 275(3) + 176\\
\textbf{Paso 2: } & 275 = 176(1) + 99\\
\textbf{Paso 3: } & 176 = 99(1) + 77\\
\textbf{Paso 4: } & 99 = 77(1) + 22\\
\textbf{Paso 5: } & 77 = 22(3) + 11\\
\textbf{Paso 6: } & 22 = 11(2) + 0
\end{aligned}$$

por lo tanto $mcd(1001, 275) = 11$ ♢

El máximo común divisor satisface las siguientes propiedades:

**Teorema 6** (Propiedades del *mcd.*)**.**

1. Si $a, b$ son enteros no ambos nulos. Entonces $mcd(a, b) = 1$ sí y solo sí existen enteros $x, y$ tales que $ax + by = 1$.
2. Si $d = mcd(a, b)$, entonces $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
3. Si $a \mid bc$ y $mcd(a, b) = 1$ entonces $a \mid c$.
4. Si $p$ es un número primo y $p \mid ab$ entonces $p \mid a$ o $p \mid b$
5. Si $a \mid c$, $b \mid c$ y $mcd(a, b) = 1$ entonces $ab \mid c$

**Ejemplo 12.** Si $a = 18$, $b = 35$ entonces $2a - b = 1$, por lo tanto $mcd(a, b) = 1$.

**Ejemplo 13.** Como $mcd(1001, 275) = 11$ entonces $mcd\left(\frac{1001}{11}, \frac{275}{11}\right) = 1$.

**Ejemplo 14.** Demostrar que si $12 \mid 13x$ entonces $x = 12 \cdot k$ para algún $k \in \mathbb{Z}$.

***Solución:*** Como $12 \mid 13x$ y $mcd(12, 13) = 1$ entonces por el teorema anterior se tiene que $12 \mid x$ y por la definición de divisibilidad se concluye que $x = 12k$ para algún $k \in \mathbb{Z}$. ♢

Para terminar esta sección se presenta la siguiente definición que será necesaria en la lectura del siguiente escenario.

**Definición 6.** Si $a$ y $b$ son enteros ambos no nulos y $mcd(a, b) = 1$ entonces se dice que $a$ y $b$ son **primos relativos**.

**Ejemplo 15.** Los números 18 y 35 son primos relativos, dado que $mcd(18, 35) = 1$

## *1.2. Mínimo común múltiplo*

**Definición 7.** Sean $a$ y $b$ dos enteros no nulos su **mínimo común múltiplo** es el menor múltiplo común de los números $a$ y $b$. Se denota por $mcm(a, b)$

**Ejemplo 16.** Si $a = 30$, $b = 18$ entonces los múltiplos comunes son: $90, 180, 270, \ldots$. Por lo tanto el mínimo común múltiplo de $a$ y $b$ es 90.

**Ejemplo 17.** Si $a = 12$, $b = 14$ entonces lo múltiplos comunes son: $84, 168, 252, \ldots$. Por lo tanto $mcm(12, 14) = 90$.

El siguiente teorema describe las propiedades que caracterizan al $mcm$ de dos números.

**Teorema 7.** Sean $a$ y $b$ dos enteros no nulos, entonces $c = mcm(a, b)$ sí y solo sí,

- $c > 0$
- $a \mid c$ y $b \mid c$
- Si para algún $t \in \mathbb{Z}$ se tiene que $a \mid t$ y $b \mid t$ entonces $c \mid t$.

Pero el teorema que brinda un procedimiento eficiente para calcular el $mcm$ de dos números es el siguiente:

**Teorema 8.** Si $a$ y $b$ son enteros no nulos, entonces:

$$mcm(a, b) = \frac{|ab|}{mcd(a, b)}$$

donde $|x|$ es la función valor absoluto.

**Ejemplo 18.** Calcular $mcm(1001, 275)$.

***Solución:*** Por el teorema anterior,

$$mcm(1001, 275) = \frac{|1001 \cdot 275|}{mcd(1001, 275)} = \frac{275275}{11} = 25025$$

$\diamondsuit$

# 2. Teorema fundamental de la aritmética

El siguiente teorema establece, de manera general, que los números primos son los bloques sobre los cuales se “construyen” los números enteros positivos.

**Teorema 9** (Teorema fundamental de la aritmética.)**.** Todo entero $n > 1$ o es un número primo o se puede factorizar como el producto de primos. Este producto es único salvo el orden de los factores.

**Ejemplo 19.** Como 60 no es un número primo entonces se puede factorizar como producto de primos, en este caso la factorización corresponde a: $2^2 \cdot 3 \cdot 5$

**Ejemplo 20.** El número 173 es un número primo.

**Ejemplo 21.** Como 3600 no es un número primo entonces se puede factorizar como porducto de primos, en este caso la factorización es: $2^4 \cdot 3^2 \cdot 5^2$

A partir del teorema de la aritmética, existe otro procedimiento para calcular el $mcd(a, b)$ dado por el siguiente teorema.

**Teorema 10.** Si $a, b$ son enteros positivos, con $a = \prod_{i=1}^{k} p_i^{a_i}$, $b = \prod_{i=1}^{k} p_i^{b_i}$ donde $p_i$ es primo, $a_i \geq 0$, $b_i \geq 0$ para todo $i$. Entonces:

$$mcd(a, b) = \prod_{i=1}^{k} p_i^{t_i}$$

donde $t_i = \min\{a_i, b_i\}$

**Ejemplo 22.** Determinar $mcd(60, 150)$.

***Soluci ´on:*** La factorización en primos de 60 es $2^2 \cdot 3 \cdot 5$, la factorización en primos de 150 es $2 \cdot 3 \cdot 5^2$ entonces al observar cuáles son los primos comunes y seleccionar en cada caso el de menor exponente se obtiene:

$$mcd(60, 150) = 2 \cdot 3 \cdot 5 = 30$$

$\diamondsuit$

**Ejemplo 23.** Determinar $mcd(28761579, 412776)$.

***Solución:*** La factorización en primos de 28761579 es $3^2{\cdot}7^4{\cdot}11^3$, la factorización en primos de 412776 es $2^3{\cdot}3^4{\cdot}7^2{\cdot}13$ entonces al observar cuáles son los primos comunes y seleccionar en cada caso el de menor exponente se obtiene: $mcd(28761579, 412776) = 3^2 \cdot 7^2 = 441$

$\diamondsuit$

La dificultad de seguir este proceso para hallar el máximo común divisor de dos enteros positivos, está en la necesidad de calcular la factorización en primos de cada uno de los números, lo cual es un proceso ineficiente en la mayoría de casos.

# 3. Algunos hechos de los números primos

A lo largo de la lectura se han presentado algunas propiedades de los números primos, la idea es presentar algunos hechos que son de uso frecuente.

Con relación al teorema 2 se tiene el siguiente resultado.

**Teorema 11.** Si $n$ es un número compuesto, entonces $n$ tiene un divisor primo menor o igual a $\sqrt{n}$.

***Demostración:*** Si $n$ es un número compuesto, entonces existen un número primo $p < n$ tal que $p \mid n$. Por lo tanto $n = px$ para algún $x \in \mathbb{Z}$. Ahora, si $p > \sqrt{n}$ y $x > \sqrt{n}$ entonces $px > (\sqrt{n})^2 = n$ lo que no es correcto, por lo tanto o $p \leq \sqrt{n}$ o $x \leq \sqrt{n}$. Si $p \leq \sqrt{n}$ entonces la demostración termina, pero si $p > \sqrt{n}$ entonces $x \leq \sqrt{n}$; por el teorema fundamental de la aritmética $x$ puede ser un número primo o existe un primo $p'$ tal que $p' \mid x$, en ambos casos existe $p' \leq \sqrt{n}$ primo tal que $p' \mid n$. $\diamondsuit$

De este teorema se sigue que si ningún primo $p \leq \sqrt{n}$ satisface que $p \mid n$ entonces $n$ es primo. Lo que se resume en el siguiente test de primalidad:

**Test de primalidad:** Sea $n$ un entero positivo, si para todo $p$ número primo $p \leq \sqrt{n}$ se tiene que $p \nmid n$ entonces $n$ es un número primo.

**Ejemplo 24.** Demostrar que 109 es un número primo.

***Solución:*** Dado que los primos $p$ menores o iguales a $\sqrt{109}$ son $2, 3, 5, 7$ entonces es necesario verificar que ninguno de ellos divide a 109.

- $2 \nmid 109$ dado que 109 no es par.
- $3 \nmid 109$ dado que 109 no es múltiplo de 3.
- $5 \nmid 109$ dado que 109 no es múltiplo de 5.
- $7 \nmid 109$ dado que 109 no es múltiplo de 7.

Por el test de primalidad, se tiene que 109 es un número primo. $\diamondsuit$

Sea $\pi(x)$ la función que asigna a cada entero positivo $x$ el número de primos menores o iguales a $x$, por ejemplo:

$$\pi(2) = 1, \pi(4) = 2, \pi(11) = 5$$

entonces se tiene el siguiente resultado.

**Teorema 12.**

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\ln(x)}\right)} = 1$$

Lo que implica que $\frac{x}{\ln(x)}$ es una estimación del valor de $\pi(x)$ cuando $x$ es un número muy grande.

**Ejemplo 25.** Determinar una estimación de $\pi(100000)$.

***Solución:*** Por el teorema anterior, se tiene que $\pi(100000) \approx \frac{100000}{\ln(100000)} \approx 8685.9$. Por lo tanto se estima que existen 8685 números primos menores a 100000. $\diamondsuit$

## 4. Ejercicios

Los siguientes ejercicios tienen como objetivo que el estudiante afiance los conceptos presentados en la lectura, no se deben entregar al tutor del m´odulo.

1. Determinar en cada caso si $a \mid b$
   a) $a = 17$, $b = -51$
   b) $a = 11$, $b = 1001$
2. Determinar en cada caso un divisor común de los números dados:
   a) 28, 52
   b) 1521, 1287
3. Determinar en cada caso el máximo común divisor de los números dados:
   a) 28, 52
   b) 25025, 2860
   c) $2^3 \cdot 5 \cdot 7^3$, $2^3 \cdot 7 \cdot 11^3$
4. Descomponer en producto de primos, cada uno de los siguientes números:
   a) 2730
   b) 990
   c) 29393
   d) 625000
5. Un número primo $M$, se denomina un primo de *Mersenne* si existe un número primo $p$ tal que $M = 2^p - 1$. Demostrar que 7 y 127 son primos de Mersenne.
6. Demostrar, usando las propiedades presentadas en la lectura, que $4 \mid (3^{11} - 7)$. [Sugerencia: considerar que $3^{11} = (4-1)^{11}$]
7. Demostrar que para todo $n \geq 1$ se tiene que $6 \mid n(n+1)(n+2)$.
8. Demostrar que si $5 \mid 7x$ para algún $x \in \mathbb{Z}$ entonces $x = 5k$ para algún $k \in \mathbb{Z}$.
9. Demostrar que si $7 \mid z$ y $3 \mid z$ entonces $21 \mid z$.
10. Programar el algoritmo de Euclides para calcular el máximo común divisor de dos números enteros positivos.

# Bibliografía


[1] Apostol, T.M. (1984). *Introducción a la teoría analítica de números*. Reverté

[2] Grimaldi, R. (1998) *Matemáticas discreta y combinatoria*. México: Addison-Wesley Iberoamericana.

[3] Hammack, R. (2013) *Book of proof, second edition*, Editor: Richard Hammack.

[4] Jiménez L., Gordillo J., Rubiano G. (2004) *Teoría de Números [para principiantes]*, Universidad Nacional de Colombia, 2a Edición.

[5] Rosen, K.H. and Morales, J.M.P.(2004). *Matemática discreta y sus aplicaciones*, McGraw-Hill.

## INFORMACIÓN TÉCNICA

**Módulo:** Elementos en Teoría de la Computación
**Unidad 4:** Teoría de números
**Escenario 7:** Números enteros

**Autor:** Diego Arévalo Ovalle

**Asesor Pedagógico:** Óscar Mauricio Salazar
**Diseador Gráfico:** Diego Arévalo Ovalle
**Asistente:** Alejandra Mora