# MATEMÁTICA DISCRETA
## Teoría de Números

Prof. Sergio Salinas

Facultad de Ingeniería
Universidad Nacional de Cuyo

Agosto 2024


# Divisibilidad

# Divisibilidad

## Definición

***Algoritmo de la División***: *Si* $a, b \in \mathbb{Z}$, *con* $b > 0$, *entonces existen valores únicos para* $q, r \in \mathbb{Z}$ *donde* $a = qb + r, 0 \leq r < b$.

## Definición

*Sean* $n$ *y* $d$ *enteros,* $d \neq 0$. *Se dice que* $d$ *divide a* $n$ *si existe un entero* $q$ *que satisface* $n = dq$ *donde* $q$ *se llama el cociente y* $d$ *el divisor o factor de* $n$. *Si* $d$ *divide a* $n$, *se escribe* $d \mid n$. *Si* $d$ *no divide a* $n$, *se escribe* $d \nmid n$.

Se observa que si $n$ y $d$ son enteros positivos y $d \mid n$, entonces $d \leq n$. Si $d \mid n$, existe un entero $q$ tal que $n = d \cdot q$. Como $n$ y $d$ son enteros positivos, $1 \leq q$. Por lo tanto, $d \leq dq = n$. Ya sea que un entero $d > 0$ divida o no a un entero $n$, se obtiene un cociente único $q$ y un residuo $r$ es decir que existen enteros únicos $q$ (cociente) y $r$ (residuo) que satisfacen $n = d \cdot q + r$, $0 \leq r < d$. El residuo $r$ es igual a cero si y sólo si $d$ divide a $n$.

## Ejemplo

Como $21 = 3 \cdot 7$, 3 divide a 21 y escribimos $3 \mid 21$. El cociente es 7; 3 recibe el nombre de divisor o factor de 21.

## Teorema

*Sean $m$, $n$ y $d$ enteros.* [a]

1. *Si $d \mid m$ y $d \mid n$, entonces $d \mid (m+n)$.*
2. *Si $d \mid m$ y $d \mid n$, entonces $d \mid (m-n)$.*
3. *Si $d \mid m$, entonces $d \mid mn$.*

---

[a] Ver demostración en libro Matemáticas Discretas de Richard Johnsonbaugh página 184.

# Números Primos

## Definición

*Sea n un número entero dónde $n > 1$ entonces:*

1. *El número n es **primo** si los únicos divisores positivos son 1 y n.*
2. *El número n es **compuesto** en caso que no es primo.*

## Definición

*Los números **coprimos** (**números primos entre sí** o **primos relativos**), son dos números enteros a y b cuyo su máximo común divisor (MCD) es igual a 1.*

## Ejemplos de números

- Primos: $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \dots\}$
- Compuestos: $C = \{4, 6, 9, 10, 12, 15, 18, 20, 21, 25, 28, 30, \dots\}$
- Coprimos: $CP = \{(8, 15), (9, 28), (14, 25), (21, 22), (35, 48), (12, 25), (17, 30), (18, 35), \dots\}$

# Números Primos

Si un entero $n > 1$ es compuesto, entonces tiene un divisor positivo tal que $1 < d < n$. Para determinar si un entero positivo $n$ es compuesto, es suficiente con probar si alguno de los enteros $2, 3, \cdots, n-1$ divide a $n$.

## Ejemplo

Por inspección, se encuentra que ningún número de la lista $2, 3, 4, 5, \cdots, 41, 42$ divide a 43; entonces 43 es primo.
Se verifica la lista $2, 3, 4, 5, \cdots, 449, 450$ en busca de divisores potenciales de 451, se encuentra que 11 divide a 451 ($451 = 11 \cdot 41$); así, 451 es compuesto.

## Teorema

*Un entero positivo n mayor que 1 es compuesto si y sólo si n tiene un divisor d que satisface* $2 \leq d \leq \sqrt[2]{n}$. [a]

[a] Ver demostración en libro Matemáticas Discretas de Richard Johnsonbaugh página 185.

## Definición

*Un procedimiento conocido como la **Criba de Eratóstenes**, puede utilizarse para encontrar todos los primos que no exceden a un entero positivo especificado.*

1. *Se escriben todos los números de 2 a n.*
2. *Se inicia el procedimiento con la siguiente variable $i = 2$.*
3. *Los enteros que son divisibles entre i, aparte del i, se eliminan de la lista.*
4. *Luego, se busca el siguiente número primo que no se haya eliminado y se asigna a la variable i.*
5. *Se repite el procedimiento desde el paso 2 hasta sólo queden los números primos y ya no puedan eliminarse más números de la lista.*

**Ejemplo del cálculo de los números primos entre 2 y 50 utilizando la scriba de Eratóstenes**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ | 11 |
| ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ |
| ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ | 31 |
| ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ | 41 |
| ~~42~~ | 43 | ~~44~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | ~~49~~ | ~~50~~ | |

## Prueba para determinar si un entero es primo

Este algoritmo determina si el entero $n > 1$ es primo. Si $n$ es primo, el algoritmo regresa 0. Si $n$ es compuesto, el algoritmo regresa un divisor $d$ que satisface $2 \leq d \leq \sqrt{n}$. Para probar si $d$ divide a $n$, el algoritmo verifica si el residuo al dividir $n$ entre $d$, $n$ mod $d$, es cero.

Entrada: $n$

Salida: $d$

```
es_primo(n) {
    for d = 2 to ⌊√n⌋
        if(n mod d == 0)
            return d
    return 0
}
```

# Ejercicio

## Ejercicio

Utilizar distintos números primos y compuestos para demostrar el funcionamiento del algoritmo presentado previamente.

# Números Primos

- Para $n = 1274$, el algoritmo regresa el número primo 2 y $1274 = 2 \cdot 637$.
- Para $n = 637$, el algoritmo regresa el número primo 7 y $637 = 7 \cdot 91$.
- Para $n = 91$ el algoritmo regresa el número primo 7 y $91 = 7 \cdot 13$.
- Finalmente, para n $= 13$, el algoritmo regresa 0 porque 13 es número primo.

Al combinar las ecuaciones anteriores se tiene 1274 como producto de primos:
$1274 = 2 \cdot 637 = 2 \cdot 7 \cdot 91 = 2 \cdot 7 \cdot 7 \cdot 13$.

# Teorema Fundamental de la Aritmética

## Teorema fundamental de la aritmética

*Cualquier entero mayor que 1 se puede expresar como un producto de primos. Más aún, si los primos se escriben en orden no decreciente, la factorización es única. En símbolos, si*

$$n = p_1 p_2 \cdots p_i,$$

*donde las* $p_k$ *son primos y* $p_1 \leq p_2 \leq \ldots \leq p_i$, *y*

$$n = p'_1 p'_2 \cdots p'_j,$$

*donde las* $p'_k$ *son primos y* $p'_1 \leq p'_2 \leq \ldots \leq p'_i$, *entonces* $i = j$ *y*

$$p_k = p'_k \qquad \text{para toda } k = 1, \ldots, i.$$

# Números Primos

**Teorema**

*El número de primos es infinito. (Ver demostración en libro Matemáticas Discretas de Richard Johnsonbaugh página 187).*

# Máximo Común Divisor

## Definición

*Sean $m$ y $n$ enteros diferentes de cero. Un divisor común de $m$ y $n$ es un entero que divide tanto a $m$ como a $n$. El máximo común divisor, escrito $mcd(m, n)$ es el divisor común de $m$ y $n$ más grande.*

## Ejemplo

Por ejemplo, el máximo común divisor de 4 y 6 es 2 y el máximo común divisor de 3 y 8 es 1.

# Máximo Común Divisor

Se usa el concepto de máximo común divisor cuando se verifica si una fracción $\frac{m}{n}$, donde $m$ y $n$ son enteros, está simplificada.
Si el máximo común divisor de $m$ y $n$ es 1, $\frac{m}{n}$ está simplificada; de otra manera, es posible reducir $\frac{m}{n}$.
Por ejemplo, $\frac{4}{6}$ no está reducida porque el máximo común divisor de 4 y 6 es 2, no 1.
Podemos dividir 4 y 6 entre 2. La fracción $\frac{3}{8}$ está simplificada porque el máximo común divisor de 3 y 8 es 1.

## Ejemplo

El máximo común divisor de 30 y 105 se encuentra observando sus factorizaciones primas $30 = 2 \cdot 3 \cdot 5$ y $105 = 3 \cdot 5 \cdot 7$.
Un divisor común de 30 y 105 es 3 ya que aparece en la factorización prima de ambos números. Por la misma razón, 5 también es un divisor común de 30 y 105. Además, $3 \cdot 5 = 15$ también es un divisor común de 30 y 105. Puesto que no hay un producto mayor de primos que sea común a los dos, 30 y 105, se concluye que 15 es el máximo común divisor de 30 y 105.

# Máximo Común Divisor

## Teorema

*Sean $m$ y $n$ enteros, $m > 1$, $n > 1$, con factorizaciones primas*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

*y*

$$n = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}.$$

*(Si el primo $p_i$ no es un factor de $m$, se hace $a_i = 0$. De manera similar, si el primo $p_i$ no es un factor de $n$, se hace $b_i = 0$.) Entonces*

$$\text{mcd}(m, n) = p_1^{\text{mín}(a_1,b_1)} p_2^{\text{mín}(a_2,b_2)} \cdots p_n^{\text{mín}(a_n,b_n)}.$$

## Ejemplo

$82320 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0$
$950796 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1$
Por el teorema anterior:
$mcd(82320, 950796) = 2^{min(4,2)} \cdot 3^{min(1,2)} \cdot 5^{min(1,0)} \cdot 7^{min(3,4)} \cdot 11^{min(0,1)} =$
$2^2 \cdot 3^1 \cdot 5^0 \cdot 7^3 \cdot 11^0 = 4116$

No se conoce un algoritmo eficiente para calcular los factores primos de un número. Sin embargo, luego se presentará el algoritmo de Euclides, que proporciona una manera eficiente de calcular el máximo común divisor.

# Mínimo Común Múltiplo

## Definición

*Sean $m$ y $n$ enteros positivos. Un múltiplo común de $m$ y $n$ es un entero que es divisible tanto entre $m$ como entre $n$. El mínimo común múltiplo, escrito $mcm(m, n)$, es el múltiplo común positivo más pequeño de $m$ y $n$.*

# Mínimo Común Múltiplo

## Teorema

*Sean $m$ y $n$ enteros, $m > 1$, $n > 1$, con factorizaciones primas*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

*y*

$$n = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}.$$

*(Si el primo $p_i$ no es un factor de $m$, se deja $a_i = 0$. De manera similar, si el primo $p_i$ no es un factor de $n$, se deja $b_i = 0$). Entonces*

$$\text{mcm}(m, n) = p_1^{\text{máx}(a_1,b_1)} p_2^{\text{máx}(a_2,b_2)} \quad p_n^{\text{máx}(a_n,b_n)}.$$

# Mínimo Común Múltiplo

## Ejemplo

El mínimo común múltiplo de 30 y 105, $mcm(30, 105)$, es 210 porque 210 es divisible entre los dos (30 y 105) y, por inspección, ningún entero positivo menor que 210 es divisible por ambos, 30 y 105.

## Ejemplo

Podemos encontrar el mínimo común múltiplo de 30 y 105 observando sus factorizaciones primas $30 = 2 \cdot 3 \cdot 5$ y $105 = 3 \cdot 5 \cdot 7$

La factorización prima de $mcm(30, 105)$ debe contener a 2, 3 y 5 como factores para que 30 divida a $mcm(30, 105)$. También debe contener a 3, 5 y 7 para que 105 divida a $mcm(30, 105)$. El número más pequeño con esta propiedad es $2 \cdot 3 \cdot 5 \cdot 7 = 210$, es decir que $mcm(30, 105) = 210$.

# Mínimo Común Múltiplo

## Ejemplo

$82320 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0$
$950796 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1$
$mcm(82320, 950796) = 2^{max(4,2)} \cdot 3^{max(1,2)} \cdot 5^{max(1,0)} \cdot 7^{max(3,4)} \cdot 11^{max(0,1)} =$
$2^4 \cdot 3^2 \cdot 5^1 \cdot 7^4 \cdot 11^1 = 19015920$

# Mínimo Común Múltiplo

## Teorema

*Para cualesquiera enteros positivos $m$ y $n$, $mcd(m,n) \cdot mcm(m,n) = mn$.* [a]

[a] Ver demostración en libro Matemáticas Discretas de Richard Johnsonbaugh página 190.

# Algoritmo de Euclides

El algoritmo de Euclides es un algoritmo antiguo, conocido y eficiente para encontrar el máximo común divisor de dos enteros. El algoritmo euclidiano se basa en el hecho de que si $r = a \mod b$, entonces $mcd(a, b) = mcd(b, r)$.

## Teorema

*Si $a$ es un entero no negativo, $b$ es un entero positivo y $r = a \mod b$, entonces $mcd(a, b) = mcd(b, r)$.*

# Algoritmo de Euclides

## Ejemplo

- $105 \mod 30 = 15$, entonces $mcd(105, 30) = mcd(30, 15)$.
- $30 \mod 15 = 0$, entonces $mcd(30, 15) = mcd(15, 0)$.
- $mcd(15, 0) = 15$, entonces
  $mcd(105, 30) = mcd(30, 15) = mcd(15, 0) = 15$.

# Algoritmo de Euclides

## Teorema

*Sean $a, b \in \mathbb{Z}^+$ donde definimos $r_0 = a$ y $r_1 = b$ se aplica el algoritmo de la división como sigue:*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, & 0 \leq r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4, & 0 \leq r_4 < r_3 \\
&\vdots & \vdots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2}, & 0 \leq r_{i+2} < r_{i+1} \\
&\vdots & \vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_n r_n
\end{aligned}$$

*Entonces $r_n$ el último resto distinto de cero es igual al mcd$(a, b)$.*

# Identidad de Bézout

**Teorema**

*Dados dos números enteros $a, b \in \mathbb{Z}$, tal que $mcd(a, b) = d$, entonces existen $u, v \in \mathbb{Z}$, tal que $au + bv = d$.*

# Algoritmo de Euclides

## Ejemplo

Calcular el $mcd(250, 111)$ utilizando el algoritmo de Euclides.

# Algoritmo de Euclides

## Ejemplo

Calcular el $mcd(250, 111)$ utilizando el algoritmo de Euclides.

$$\begin{aligned} 250 &= 2(111) + 28, & 0 \leq 28 < 111 \\ 111 &= 3(28) + 27, & 0 \leq 27 < 28 \\ 28 &= 1(27) + 1, & 0 \leq 1 < 27 \\ 27 &= 27(1) + 0 \end{aligned}$$

El resultado es el siguiente $mcd(250, 111) = 1$.

## Importante

Si trabajamos hacia atrás en la tercera ecuación, tendremos que
$1 = 28 - 1(27) = 28 - 1[111 - 3(28)] = (-1)(111) + 4(28) =$
$(-1)(111) + 4[250 - 2(111)] = 4(250) - 9(111) = (250)4 + 111(-9)$ es una combinación lineal de 250 y 111.
La expresión como combinación lineal de 250 y 111 no es única, ya que
$1 = 250[4 - 111k] + 111[-9 + 250k]$, para cualquier $k \in \mathbb{Z}$.
También tenemos que
$mcd(-250, 111) = mcd(250, -111) = mcd(-250, -111) = mcd(250, 111) = 1$

# Algoritmo de Euclides

## Ejemplo

Calcular el $mcd(8n+3, 5n+2)$ utilizando el algoritmo de Euclides.

## Ejemplo

Calcular el $mcd(8n+3, 5n+2)$ utilizando el algoritmo de Euclides.

$$\begin{aligned} 8n+3 &= 1(5n+2)+(3n+1), & 0 &< 3n+1 < 5n+2 \\ 5n+2 &= 1(3n+1)+(2n+1), & 0 &< 2n+1 < 3n+1 \\ 3n+1 &= 1(2n+1)+n, & 0 &< n < 2n+1 \\ 2n+1 &= 2(n)+1, & 0 &< 1 < n \\ n &= n(1)+0 \end{aligned}$$

El resultado es el siguiente $mcd(8n+3, 5n+2) = 1$ para todo $n \geq 1$.

# Algoritmo de Euclides

## Algoritmo euclidiano

Este algoritmo encuentra el máximo común divisor de los enteros no negativos $a$ y $b$, donde no son cero $a$ y $b$.

```
        Entrada:    a y b (enteros no negativos, ambos diferentes de cero)
         Salida:    máximo común divisor de a y b
1.      mcd(a, b) {
2.          // sea a el mayor
3.          if (a < b)
4.              intercambia(a, b)
5.          while (b ¬=0) {
6.              r = a mod b
7.              a = b
8.              b = r
9.          }
10.         return a
11.     }
```

# Algoritmo de Euclides

## Ejercicio

Sean $a = 504$ y $b = 396$ utilizar el algoritmo de Euclides para analizar cada paso realizado para calcular el $mcd(504, 396)$.

**Solución:**

| i | a | b | r |
|---|---|---|---|
| 1 | 504 | 396 | 108 |
| 2 | 396 | 108 | 72 |
| 2 | 108 | 72 | 36 |
| 2 | 72 | 36 | 0 |
| 2 | 36 | 0 | 36 |

Cuadro: Ejemplo mcd(504,396) utilizando el Algoritmo de Euclides.

# Algoritmo de Euclides

**Teorema**

*Si los enteros en un intervalo de 0 a m, $m \geq 8$, ambos diferentes de cero, se introducen al algoritmo euclidiano (pseudocódigo), entonces se requieren cuando mucho* $\log_{\frac{3}{2}} \frac{2m}{3}$ *pasos para obtener una solución.*

# Fin