UCA Universidad de Cádiz

Escuela Superior de Ingeniería
Departamento de Matemáticas

# Apuntes de Matemática Discreta

# 11. Teorema Fundamental de la Aritmética

Francisco José González Gutiérrez

Cádiz, Octubre de 2004

# Lección 11

# Teorema Fundamental de la Aritmética

## Contenido



El concepto de número primo se remonta a la antigüedad. Los griegos poseían dicho concepto, así como una larga lista de teoremas y propiedades relacionados con él. Los cuatro ejemplos siguientes aparecen en los *Elementos de Euclides*:

- Todo entero positivo distinto de 1 es un producto de números primos.
- Teorema fundamental de la Aritmética: "Todo entero positivo puede descomponerse de manera única como un producto de números primos".
- Existen infinitos números primos.

– Podemos obtener una lista de los números primos por medio del método conocido como la *Criba de Eratóstenes.*

## 11.1 Números Primos

Observemos que si $a$ es cualquier número entero mayor que 1, entonces

$$a = a \cdot 1, \text{ con } 1 \in \mathbb{Z}, \text{ es decir, } a \text{ es un divisor de } a.$$

$$a = 1 \cdot a, \text{ con } a \in \mathbb{Z}, \text{ es decir, } 1 \text{ es un divisor de } a.$$

luego todo número entero $a > 1$ tiene, al menos, dos divisores, el 1 y el propio $a$.

### 11.1.1 Definición

*Diremos que el número entero $p > 1$ es un número primo si los únicos divisores positivos que tiene son 1 y $p$. Si un número entero no es primo, lo llamaremos compuesto.*

En el conjunto de los diez primeros números enteros positivos son primos 2, 3, 5 y 7, siendo compuestos 4, 6, 8, 9 y 10.

**Nota 11.1** Obsérvese que de la definición de número primo se sigue que

$$p \text{ es primo si, y sólo si es imposible escribir } p = ab \text{ con } a, b \in \mathbb{Z} \text{ y } 1 < a, b < p.$$

### 11.1.2 Números Primos entre sí

*Dados dos números enteros a y b, diremos que son primos entre sí, cuando el máximo común divisor de ambos sea 1.*

La definición anterior admite generalización a una familia de números enteros $a_1, a_2, \ldots, a_n$. Dichos números serán primos entre sí, cuando

$$\text{m.c.d.}(a_1, a_2, \ldots\ldots, a_n) = 1$$

**Ejemplo 11.1** Demostrar que cualquiera que sea $n \in \mathbb{Z}$, los números $3n+11$ y $2n+7$ son primos entre sí.

Solución

Observemos lo siguiente:

$$2(3n + 11) + (-3)(2n + 7) = 6n + 22 - 6n - 21 = 1$$

luego por el corolario **??**, se sigue que

$$\text{m.c.d.}\,(3n + 11, 2n + 7) = 1$$

Veamos otra forma de probar lo mismo. Si $d = \text{m.c.d.}(3n+11, 2n+7)$, entonces

$$\left.\begin{array}{l} d|3n+11 \\ \text{y} \\ d|2n+7 \end{array}\right\} \implies d|2(3n+11)-3(2n+7)$$

$$\implies d|6n+22-6n-21$$

$$\implies d|1$$

$$\overset{d>0}{\implies} d=1$$

Por lo tanto, ambos números son primos entre sí. ∎

### 11.1.3 Proposición

*Todo número compuesto posee, al menos, un divisor primo.*

Demostración

Probaremos que

*Si un número entero a es compuesto, entonces tiene, al menos, un divisor primo*

Lo haremos por contradicción, es decir supondremos que la proposición anterior es falsa o lo que es igual que su negación es verdadera, o sea,

*El número entero a es compuesto y, sin embargo, no tiene divisores primos.*

Entonces, el conjunto

$$C = \left\{n \in \mathbb{Z}^+ : n \geqslant 2, \text{ compuesto y sin divisores primos}\right\}$$

es no vacío ya que, al menos, $a \in C$.

Pues bien, como $C$ es un subconjunto no vacío de $\mathbb{Z}^+$, por el principio de buena ordenación tendrá un primer elemento $m$. Entonces,

$$m \in C \implies \left\{\begin{array}{l} m \text{ es compuesto} \\ \text{y} \\ m \text{ no tiene divisores primos} \end{array}\right.$$

$$\implies \left\{\begin{array}{l} \exists m_1 : m_1 \neq 1,\ m_1 \neq m \text{ y } m_1|m \\ \text{y} \\ m_1 \text{ no es primo} \end{array}\right.$$

$$\implies \exists m_1, \text{ compuesto } m_1|m \text{ y } 1 < m_1 < m.$$

Ahora bien, si $m_1$ no tuviera divisores primos, entonces $m_1 \in C$ siendo $m_1 < m$, lo cual es imposible ya que $m$ es el mínimo de $C$, por lo tanto $m_1$ ha de tener, al menos, un divisor primo $p$. Pero

$$\left.\begin{array}{l} p|m_1 \\ m_1|m \end{array}\right\} \implies p|m$$

es decir $m$ tiene un divisor primo lo cual es una contradicción ya que $m \in C$, es decir no tiene divisores primos.

Consecuentemente, la suposición hecha es falsa, y, por lo tanto, si un número es compuesto, entonces ha de tener, al menos, un divisor primo. ∎

Euclides demostró en el libro IX de los Elementos que existían infinitos números primos. La argumentación que utilizó ha sido considerada desde siempre como un modelo de elegancia matemática.

### 11.1.4 Teorema

*Existen infinitos números primos.*

Demostración

Supongamos lo contrario, es decir la cantidad de números primos existente es finita, pongamos, por ejemplo, que sólo hay $k$ números primos,

$$p_1, p_2, \ldots\ldots, p_k.$$

Pues bien, sea $m$ el producto de todos ellos más 1, es decir,

$$m = p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k + 1$$

Entonces,

$$m \neq p_i,\ i = 1, 2, \ldots, k$$

es decir es distinto de todos los primos que existen, luego no puede ser primo, de aquí que sea compuesto y, por el teorema anterior, tendrá, al menos, un divisor primo que tendrá que ser uno de los existentes, o sea, existe $p_j$ con $j \in \{1, 2, \ldots\ldots, k\}$ tal que

$$p_j \,|m$$

y como

$$p_j \,|p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k$$

entonces dividirá a la diferencia de ambos,

$$p_j \,|m - p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k$$

luego,

$$p_j \,|1$$

de aquí que $p_j = 1$ ó $p_j = -1$ y esto es imposible ya que $p_j$ es primo.

De la contradicción a la que hemos llegado, se sigue que la suposición hecha es falsa y, por tanto, existen infinitos números primos.

**Nota 11.2** Directamente de la demostración del teorema anterior, puede deducirse que si $p_1, p_2, \ldots\ldots, p_n$ son los $n$ primeros números primos, entonces el siguiente, $p_{n+1}$, ha de ser, a lo sumo, igual al producto de los anteriores más 1, es decir,

$$p_{n+1} \leqslant (p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_n) + 1$$

En efecto, sea

$$m = p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_n + 1$$

- Si $m$ es primo, entonces $p_n < m$ y, por tanto,

  $$p_{n+1} \leqslant m$$

- Si $m$ no es primo, entonces es compuesto siendo sus factores primos diferentes de los $p_1, p_2, \ldots, p_n$, ya que como hemos visto en la demostración del teorema, ninguno de los $p_i$, $1 \leqslant i \leqslant n$, puede dividir a $m$.

  Supongamos que $m_1$ es el menor factor primo de $m$, entonces $p_n < m_1$. En efecto, si $p_n$ fuese mayor o igual que $m_1$, entonces

  $$m_1 \leqslant p_n \Longrightarrow \exists j \in \{1, 2, \ldots\ldots, n\} : m_1 = p_j \Longrightarrow p_j \,|m$$

  lo cual, hemos visto, es imposible, por tanto,

  $$p_n < m_1$$

  de aquí que

  $$p_{n+1} \leqslant m_1 < m$$

**Ejemplo 11.2** Demostrar que si $p \neq 5$ es un número primo impar, entonces $p^2-1$ ó $p^2+1$ es divisible por 10.

Solución

Por el teorema de existencia y unicidad del cociente y resto, existen $q$ y $r$, enteros y únicos tales que

$$p = 5q + r, \text{ con } 0 \leqslant r < 5$$

y como $p$ es primo, $r$ no puede ser cero, luego

$$p = 5q + r, \text{ con } r = 1, 2, 3 \text{ ó } 4$$

Además, por hipótesis $p$ es impar. Entonces,

$$p \text{ es impar} \Longrightarrow p+1 \text{ es par} \Longrightarrow 2|p+1$$

Antes que nada probaremos que

$$r \text{ es impar} \iff q \text{ es par}$$

En efecto,

$$\begin{array}{rcl} r \text{ es impar} & \iff & r+1 \text{ es par} \\ & \iff & 2|r+1 \\ & \iff & 2|p-5q+1 \\ & \overset{2|p+1}{\iff} & 2|5q \\ & \iff & 2|q \\ & \iff & q \text{ es par} \end{array}$$

Pues bien,

- Si $r$ es impar, entonces $q$ es par. Tomando $q = 2q_1$ con $q_1 \in \mathbb{Z}^+$, tendremos

$$\left.\begin{array}{l} p^2 = 25q^2 + 10qr + r^2 \\ q = 2q_1 \end{array}\right\} \Longrightarrow p^2 = 100q_1^2 + 20q_1r + r^2$$
$$\Longrightarrow p^2 - r^2 = 10(10q_1^2 + 2q_1r)$$
$$\Longrightarrow 10|p^2 - r^2$$

  y habrá dos opciones, $r = 1$ ó $r = 3$. Entonces,

$$\left.\begin{array}{l} r = 1 \\ 10|p^2 - r^2 \end{array}\right\} \Longrightarrow 10|p^2 - 1$$

ó

$$\left.\begin{array}{l} r = 3 \\ 10|p^2 - r^2 \end{array}\right\} \Longrightarrow 10|p^2 - 9 \overset{10|10}{\Longrightarrow} 10|p^2 - 9 + 10 \Longrightarrow 10|p^2 + 1$$

- Si $r$ es par, entonces $q$ ha de ser impar. Tomando $q = 2q_1 + 1$ con $q_1$ entero no negativo.

$$\left.\begin{array}{l} p^2 = 25q^2 + 10qr + r^2 \\ q = 2q_1 + 1 \end{array}\right\} \Longrightarrow p^2 = 100q_1^2 + 100q_1 + 25 + 20q_1r + 10r + r^2$$
$$\Longrightarrow p^2 - r^2 - 25 = 10(10q_1^2 + 10q_1 + 2q_1r + r)$$
$$\Longrightarrow 10|p^2 - r^2 - 25$$

y habrá dos opciones, $r = 2$ ó $r = 4$. Entonces,

$$\left.\begin{array}{l} r = 2 \\ 10|p^2 - r^2 - 25 \end{array}\right\} \implies 10|p^2 - 29 \overset{10|30}{\implies} 10|p^2 - 29 + 30 \implies 10|p^2 + 1$$

ó

$$\left.\begin{array}{l} r = 4 \\ 10|p^2 - r^2 - 25 \end{array}\right\} \implies 10|p^2 - 41 \overset{10|40}{\implies} 10|p^2 - 41 + 40 \implies 10|p^2 - 1$$

luego en cualquier caso $p^2 - 1$ ó $p^2 + 1$ es divisible por 10. ∎

**Ejemplo 11.3** Demostrar:

(a) El cuadrado de todo número entero es de la forma $4k$ ó $4k + 1$.

(b) Si $p_n$ es el $n-$ésimo número primo, entonces ningún entero de la forma $P_n = (p_1 \cdot p_2 \cdot \cdots \cdot p_n) + 1$ es un cuadrado.

Solución

(a) En efecto, por el teorema de existencia y unicidad de cociente y resto (**??**), cualquier número entero $n$ puede escribirse en la forma

$$n = 4q + r, \text{ con } 0 \leqslant r < 4$$

de aquí que

$$n^2 = 16q^2 + 8q + r^2 = 4(4q^2 + 2q) + r^2 = 4k + r^2, \text{ con } k \in \mathbb{Z}$$

y ahora pueden ocurrir cuatro casos:

$$\left.\begin{array}{l} r = 0 \\ n^2 = 4k + r^2 \end{array}\right\} \implies n^2 = 4k$$

ó

$$\left.\begin{array}{l} r = 1 \\ n^2 = 4k + r^2 \end{array}\right\} \implies n^2 = 4k + 1$$

ó

$$\left.\begin{array}{l} r = 2 \\ n^2 = 4k + r^2 \end{array}\right\} \implies n^2 = 4k + 4 \implies n^2 = 4(k + 1) \implies n^2 = 4k_1, \text{ con } k_1 \in \mathbb{Z}$$

ó

$$\left.\begin{array}{l} r = 3 \\ n^2 = 4k + r^2 \end{array}\right\} \implies n^2 = 4k + 9 \implies n^2 = 4(k + 2) + 1 \implies n^2 = 4k_1 + 1, \text{ con } k_1 \in \mathbb{Z}$$

luego en cualquier caso $n^2$ puede escribirse en la forma $4k$ ó $4k + 1$.

(b) Los $p_i$, para $1 \leqslant i \leqslant n$, son números primos, luego todos, excepto $p_1$, que es 2, son impares de aquí que el producto $p_2 \cdot p_3 \cdots p_n$ sea impar. Por el teorema de existencia y unicidad de cociente y resto se podrá escribir en la forma

$$p_2 \cdot p_3 \cdots p_n = 4q + r, \text{ con } 0 \leqslant r < 4$$

y como ha de ser impar, $r$ sólo puede ser 1 ó 3. Pues bien,

– Si $r = 1$, entonces

$$\begin{aligned} p_2 \cdot p_3 \cdots p_n = 4q+1 &\implies p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 2(4q+1)+1 \\ &\implies P_n = 8q+3 \\ &\implies P_n = 4(2q)+3 \end{aligned}$$

– Si $r = 3$, entonces

$$\begin{aligned} p_2 \cdot p_3 \cdots p_n = 4q+3 &\implies p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 2(4q+3)+1 \\ &\implies P_n = 8q+7 \\ &\implies P_n = 4(2q+1)+3 \end{aligned}$$

luego en cualquier caso, $P_n$ es de la forma $4k+3$, con $k$ entero. Por lo tanto, según el apartado (a), no es un cuadrado.

**Ejemplo 11.4** En $\mathbb{Z}^+$ definimos la siguiente relación:

$$a \mathscr{R} b \iff a \text{ y } b \text{ son primos entre sí}$$

Estudiar las propiedades de la relación.

Solución

1. Reflexiva. Dado cualquier $a \in \mathbb{Z}^+$, se verifica que

$$\text{m.c.d.}\,(a,a) = a$$

luego $\mathscr{R}$ no es reflexiva.

2. Simétrica. Sean $a$ y $b$ dos números enteros positivos cualesquiera, entonces

$$\begin{aligned} a \mathscr{R} b &\iff a \text{ y } b \text{ son primos entre sí} \\ &\iff \text{m.c.d.}(a,b) = 1 \\ &\iff b \text{ y } a \text{ son primos entre sí} \\ &\iff \text{m.c.d.}(b,a) = 1 \\ &\iff b \mathscr{R} a \end{aligned}$$

luego $\mathscr{R}$ es simétrica.

3. Transitiva. Dados tres enteros positivos cualesquiera $a, b$ y $c$,si $a$ y $b$ son primos entre sí y $b$ y $c$ también lo son, $a$ y $c$ no tienen porque serlo. En efecto,

$$\begin{aligned} &4 \text{ y } 5 \text{ son primos entre sí.} \\ &5 \text{ y } 8 \text{ son primos entre sí.} \end{aligned}$$

sin embargo,

$$\text{m.c.d.}\,(4,8) = 4$$

luego 4 y 8 no son primos entre sí y $\mathscr{R}$ no tiene la propiedad transitiva.

**Ejemplo 11.5** Estúdiese

(a) si los números $2p$ y $4p+3$ son primos entre sí, cualquiera que sea $p$ entero.

(b) idem para los números $2p+1$ y $3p+2$.

Solución

(a) En efecto, sea $d = \text{m.c.d.}(2p, 4p+3)$. Entonces,

$$\left.\begin{array}{l} d\,|2p \Longrightarrow d\,|(-2)2p \Longrightarrow d\,|-4p \\ \text{y} \\ d\,|4p+3 \end{array}\right\} \Longrightarrow d\,|-4p+4p+3 \Longrightarrow d\,|3 \Longrightarrow d=3$$

luego no son primos entre sí.

(b) Sea $d = \text{m.c.d.}\,(2p+1, 3p+2)$. Entonces,

$$\left.\begin{array}{l} d\,|2p+1 \Longrightarrow d\,|(-3)(2p+1) \Longrightarrow d\,|-6p-3 \\ \text{y} \\ d\,|3p+2 \Longrightarrow d\,|2(3p+2) \Longrightarrow d\,|6p+4 \end{array}\right\} \Longrightarrow d\,|-6p-3+6p+4 \Longrightarrow d\,|1$$

luego,

$$\text{m.c.d.}\,(2p+1, 3p+2) = 1$$

es decir, son primos entre sí.

**Ejemplo 11.6** Demostrar que todo número primo mayor que 3 puede escribirse en la forma

(a) $4q+1$ ó $4q+3$ para algún $q \in \mathbb{Z}^+$.

(b) $6q+1$ ó $6q+5$ para algún $q \in \mathbb{Z}^+$.

Solución

Sea $p > 3$ un número primo.

(a) Por el teorema de existencia y unicidad de cociente y resto, existen $q$ y $r$ tales que

$$p = 4q + r : 0 \leqslant r < 4$$

Si $r = 0$ ó $r = 2$, entonces $p$ sería divisible por 2 y no sería primo, luego $r$ ha de ser 1 ó 3 y, consecuentemente,

$$p = 4q+1 \text{ ó } p = 4q+3$$

(b) Al igual que en el apartado (a),

$$p = 6q + r : 0 \leqslant r < 6$$

y si $r = 0$ ó $r = 2$ ó $r = 4$, entonces $p$ sería divisible por 2 y si $r = 3$ sería divisible por 3, luego $r$ ha de ser 1 ó 5, de aquí que

$$p = 6q+1 \text{ ó } p = 6q+5$$

## 11.2 Criba de Eratóstenes

Una vez conocida la existencia de infinitos números primos, se plantea un nuevo problema cual es la forma en que dichos números están distribuidos en el conjunto de los números naturales. Este problema es complicado y se conocen sólo resultados parciales. Un primer método para resolver esta cuestión fue establecido en el siglo III a.c. por Eratóstenes[1]; recibe el nombre de *Criba de Eratóstenes* en honor a su autor y es consecuencia del siguiente teorema cuya primera demostración rigurosa se debe a Fermat.

### 11.2.1 Teorema

*Si un número entero mayor que* 1 *no tiene divisores primos menores o iguales que su raíz, entonces es primo.*

Demostración

Sea $p$ entero estrictamente mayor que 1. Utilizamos el método de demostración por la contrarrecíproca, es decir veremos que

*si $p$ no es primo, entonces existe, al menos, un divisor primo de $p$ menor o igual que su raíz.*

En efecto, si $p$ no es primo, entonces es compuesto y por la proposición 11.1.3 tendrá, al menos, un divisor primo $a$. Veamos que es menor o igual que la raíz de $p$. En efecto,

$$a|p \Longrightarrow p = aq, \text{ con } 1 < a < p, \text{ y } q \in \mathbb{Z} : 1 < q < p.$$

Además, si suponemos que $a \leqslant q$, entonces

$$a \leqslant q \Longrightarrow a^2 \leqslant aq \Longrightarrow a^2 \leqslant p \Longrightarrow a \leqslant \sqrt{p}.$$

Así pues, hemos encontrado un divisor primo de $p$ menor o igual que la raíz de $p$.

**Ejemplo 11.7** Supongamos que queremos saber si el 9 es primo. Entonces, como $\sqrt{9} = 3$, los números primos menores o iguales que 3 son el 2 y el propio 3. 2 no es divisor de 9, pero 3 si lo es, luego 9 no es primo.

Obsérvese que al ser las raíces de 10, 11, 12, 13, 14 y 15 menores que 4, los números primos menores o iguales que ellas son, también, 2 y 3, luego el criterio anterior puede emplearse para ver si estos números son o no primos. En efecto,

El 10 no es primo ya que 2 es divisor de 10.

2 y 3 no son divisores de 11, luego el 11 es primo.

El 12 no es primo ya que es múltiplo de 2.

[1] Astrónomo, geógrafo, matemático y filósofo griego (Cirene 284 a.c.-Alejandría 192 a.c.). Vivió durante mucho tiempo en Atenas, antes de ser llamado a Alejandría (245 a.c.) por Tolomeo III, quien le confió la educación de sus hijos y luego la dirección de la biblioteca. Sus aportaciones a los diversos campos de la ciencia fueron muy importantes, pero sobre todo es conocido como matemático, por su célebre *criba* -que conserva su nombre- para encontrar los números primos, y por el *mesolabio*, instrumento de cálculo para resolver el problema de la media proporcional. Fue el primero en medir de un modo exacto la longitud de la circunferencia de la Tierra. Para ello determinó la amplitud del arco meridiano entre Siena y Alejandría: sabiendo que en el solsticio de verano el sol en Siena se hallaba en la vertical del lugar, ya que los rayos penetraban en los pozos más profundos, midió, con la ayuda de la sombra proyectada por un gnomon, el ángulo formado, en Alejandría, por los rayos solares con la vertical. En razón de la propagación rectilínea de los rayos solares y del paralelismo existente entre ellos, el ángulo así medido correspondía al ángulo formado en el centro de la Tierra por el radio terrestre de Siena y el de Alejandría, obteniendo así la amplitud del arco interceptado por estas dos ciudades sobre el meridiano. Luego midió sobre el terreno la dimensión de este arco. Obtuvo para la circunferencia entera, es decir, para el meridiano, 252000 estadios, o sea, casi 40 millones de m. Luego repitió este cálculo, basándose en la distancia de Siena a Méroe, que creyó estaba también sobre el mismo meridiano, y obtuvo un resultado concorde.

13 no es múltiplo de 2 ni de 3 por lo tanto es primo.

El 14 no es primo ya que 2 es divisor de 14.

El 15 no es primo ya que es múltiplo de 3.

Por tanto,

- Números primos entre 2 y 24. Aquellos que no sean múltiplos de 2, ni de 3.
- Números primos entre 2 y 48. Aquellos que no sean múltiplos de 2, ni de 3, ni de 5.
- Números primos entre 2 y 120. Aquellos que no sean múltiplos de 2, ni de 3, ni de 5, ni de 7.
- Así sucesivamente, podríamos encontrar todos los números primos.

**Ejemplo 11.8** Encontrar todos los números primos que hay entre los 100 primeros números naturales.

Solución

Dado que la raíz de 100 es 10 y los números primos menores que 10 son 2, 3, 5 y 7, los números buscados son todos aquellos que no sean múltiplos de 2, ni de 3, ni de 5, ni de 7.

La *Criba de Eratóstenes* consiste en eliminar el 1 y todos los múltiplos de estos números. Los que quedan son los números primos entre 1 y 100. En la tabla siguiente dichos números figuran con fondo blanco.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 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 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

**Ejemplo 11.9** Estúdiese si el 811 es primo utilizando la Criba de Eratóstenes.

Solución

$\sqrt{811} = 28.5$ y los números primos menores o iguales que 28.5 son 2, 3, 5, 7, 11, 13, 17, 19 ó 23 y dado que ninguno de estos números divide a 811, concluimos que dicho número es primo.

## 11.3 Teorema Fundamental de la Aritmética

En este apartado veremos que cualquier entero $n$ mayor que 1 es primo o puede escribirse como un producto de números primos.

Este resultado, que tiene un equivalente en el libro IX de los *Elementos* de Euclides, se conoce con el nombre de *Teorema fundamental de la aritmética*.

### 11.3.1 Lema de Euclides

*Si un número entero divide al producto de otros dos y es primo con uno de ellos, entonces divide al tercero.*

Demostración

En efecto, sean $a$, $b$ y $c$ tres números enteros, tales que $a$ divida a $b \cdot c$ y sea primo con $b$. Como m.c.d. $(a, b) = 1$, por el corolario **??**, existirán dos números enteros $p$ y $q$ tales que

$$pa + qb = 1$$

Por otra parte, si $a$ divide a $bc$, como $a$ divide a $a$, dividirá a cualquier combinación lineal con coeficientes enteros de $a$ y $bc$. En particular,

$$a|pac + qbc$$

es decir,

$$a|(pa + qb)c$$

luego,

$$a|c$$

### 11.3.2 Corolario

*Sea $p$ un número entero mayor que 1. Las siguientes afirmaciones son equivalentes:*

*(a) $p$ es un número primo.*

*(b) Si $p$ divide a un producto de dos números enteros, entonces divide a uno de los dos.*

Demostración

(a) $\Longrightarrow$ (b). Probaremos que para cualquier par de enteros, $a$ y $b$,

$$p \text{ es primo} \Longrightarrow (p|ab \Longrightarrow p|a \text{ ó } p|b)$$

o lo que es igual,

$$p \text{ es primo y } p|ab \Longrightarrow p|a \text{ ó } p|b$$

Lo haremos por contradicción. En efecto, supongamos que

$$p \text{ es primo y } p|ab \text{ y } p\not|a \text{ y } p\not|b$$

Pues bien,

- si $p$ no es divisor de $a$, como $p$ es primo, el único divisor común de $a$ y de $p$ es 1, luego $a$ y $p$ son primos entre sí, es decir,

  $$p|ab \text{ y m.c.d.}(a, p) = 1.$$

  Aplicamos el lema de Euclides y $p|b$ lo cual contradice la suposición hecha.

– Si $p$ no divide a $b$ se hace igual.

(b) $\Longrightarrow$ (a). Probaremos que para cualquier par de enteros, $a$ y $b$,

$$(p|ab \Longrightarrow p|a \text{ ó } p|b) \Longrightarrow p \text{ es primo.}$$

Utilizaremos el método de demostración por la contrarrecíproca, es decir probaremos que pueden encontrarse dos enteros $a$ y $b$ tales que

$$p \text{ no es primo} \Longrightarrow p|ab \text{ y } p\not|a \text{ y } p\not|b.$$

En efecto, si $p$ no es primo, entonces es compuesto luego tendrá, además de 1 y $p$, otro divisor $a$, es decir, existe $a$ tal que $a|p$. Pues bien,

$$a|p \Longrightarrow \exists b \in \mathbb{Z} : p = ab$$

siendo $1 < a < p$ y $1 < b < p$. Además,

– $p\not|a$. En efecto, si $p|a$, entonces

$$\left.\begin{array}{l} p|a \\ \text{y} \\ a|p \end{array}\right\} \Longrightarrow a = p$$

lo cual es imposible.

– $p\not|b$. Igual.

Así pues, hemos encontrado dos enteros $a$ y $b$ tales que $p|ab$ y $p\not|a$ y $p\not|b$.

### 11.3.3 Corolario

*Si un número primo divide al producto de varios números enteros, entonces ha de dividir, al menos, a uno de ellos.*

Demostración

En efecto, sea $p$ un número primo y supongamos que

$$p\,|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

entonces,

$$p\,|a_1 \cdot (a_2 \cdot a_3 \cdot \cdots \cdot a_n)$$

y aplicando el corolario anterior

$$p\,|a_1 \;\text{ ó } p\,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

– Si $p\,|a_1$, el corolario está demostrado, de lo contrario

$$p\,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

luego,

$$p\,|a_2 \cdot (a_3 \cdot \cdots \cdot a_n)$$

y, nuevamente por el corolario anterior,

$$p\,|a_2 \;\text{ ó } p\,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

– Si $p \,|a_2$, el corolario está demostrado, de lo contrario

$$p \,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

luego,

$$p \,|a_3 \cdot (a_4 \cdot \cdots \cdot a_n)$$

Repitiendo el proceso un número finito de veces, encontraremos, al menos, un $a_i$, $1 \leqslant i \leqslant n$, tal que $p \,|a_i$.

**Ejemplo 11.10** Demostrar que si $p, q_1, q_2, \ldots, q_r$ son primos y $p \,|q_1 \cdot q_2 \cdots q_r$, entonces existe algún $i = 1, 2, \ldots, r$ tal que $p = q_i$

Solución

En efecto, por el corolario 11.3.3 $p$ divide a $q_i$ para algún $i$ entre 1 y $r$. Ahora bien, como $q_i$ es primo, los únicos divisores que tiene son el 1 y el mismo $q_i$, y al ser $p > 1$, tendrá que ser necesariamente $p = q_i$.

**Ejemplo 11.11** Demostrar que el número $\sqrt{2}$ es irracional.

Solución

Si $\sqrt{2}$ fuese racional, entonces podría expresarse como un cociente de dos enteros $a$ y $b$ primos entre sí (fracción irreducible), es decir,

$$\sqrt{2} = \frac{a}{b} : \text{m.c.d.}\,(a, b) = 1$$

Pues bien, elevando al cuadrado ambos miembros de esta igualdad, resulta:

$$\sqrt{2} = \frac{a}{b} \Longrightarrow 2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \Longrightarrow 2 \,|aa$$

luego por el corolario 11.3.3

$$2 \,|a$$

y, consecuentemente, existe un entero $q$ tal que

$$a = 2q$$

entonces,

$$a = 2q \Longrightarrow a^2 = 4q^2 \Longrightarrow 2b^2 = 4q^2 \Longrightarrow b^2 = 2q^2 \Longrightarrow 2 \,\big|b^2 \Longrightarrow 2 \,|bb$$

y, nuevamente por el corolario 11.3.3, se sigue que

$$2 \,|b$$

Así pues, 2 es un divisor común de $a$ y $b$, lo cual es una contradicción ya que estos dos números son primos entre sí, luego la suposición hecha es falsa y $\sqrt{2}$ es irracional.

**Ejemplo 11.12** Demostrar que la $\sqrt[3]{5}$ es un número irracional.

Solución

En efecto, supongamos que no lo fuese, entonces existirán dos números enteros $a$ y $b$ primos entre sí tales que

$$\sqrt[3]{5} = \frac{a}{b}$$

elevando al cubo ambos miembros de la igualdad, tendremos

$$5 = \frac{a^3}{b^3} \Longrightarrow a^3 = 5b^3 \Longrightarrow 5 \,\big|a^3$$

de donde se sigue, al ser 5 un número primo, que

$$5 \,|a$$

luego existe un número entero $q$ tal que

$$a = 5q \Longrightarrow a^3 = 5^3q^3 \Longrightarrow 5b^3 = 5^3q^3 \Longrightarrow b^3 = 5^2q^3 \Longrightarrow 5 \,|b^3$$

por tanto,

$$5 \,|b$$

Concluimos, pues, que 5 es un divisor común de $a$ y de $b$, lo cual contradice el hecho de que estos dos números sean primos entre sí, luego la suposición hecha es falsa y $\sqrt[3]{5}$ es un número irracional.

**Ejemplo 11.13** Probar que si $n$ no es la $k$-ésima potencia de ningún número entero, entonces $\sqrt[k]{n}$ es irracional cualesquiera que sean $n$ y $k$ enteros positivos.

Solución

Sean $n$ y $k$ naturales cumpliendo las condiciones del enunciado y supongamos que $\sqrt[k]{n}$ es un número racional.

Entonces, podrá expresarse como un cociente de dos números enteros primos entre sí, es decir, existirán $a$ y $b$ de $\mathbb{Z}$, tales que

$$\sqrt[k]{n} = \frac{a}{b}, \text{ con m.c.d. } (a, b) = 1$$

elevando a $k$ ambos miembros de esta igualdad, resulta

$$\sqrt[k]{n} = \frac{a}{b} \Longrightarrow n = \frac{a^k}{b^k} \Longrightarrow a^k = n \cdot b^k \Longrightarrow n \,|a^k \,.$$

Si

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$$

es la descomposición de $n$ en factores primos, ha de existir un $i$ entre 1 y $t$ tal que $\alpha_i$ no sea múltiplo de $k$ ya que por hipótesis $n$ no es la $k$-ésima potencia de un número entero.

Pues bien, como $n \,|a^k$ , $a^k$ ha de tener todos los factores primos de $n$ con exponentes iguales o mayores, luego tendremos que

$$p_i^{\alpha_i} \,|a^k$$

y $p_i$ debe aparecer en la descomposición en factores primos de $a$, luego

$$a = p_i^s q$$

donde $q$ y $p_i$ son primos entre sí y $\alpha_i < k \cdot s$ ya que como vimos anteriormente, $\alpha_i$ no es múltiplo de $k$, por tanto,

$$a^k = p_i^{ks} \cdot q^k$$

Así pues,

$$\begin{aligned} nb^k = a^k \quad &\Longrightarrow \quad p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k = p_i^{ks} \cdot q^k \\ &\Longrightarrow \quad p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k = p_i^{ks - \alpha_i} \cdot q^k \end{aligned}$$

luego,

$$p_i \,|p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k$$

y como $p_i$ no divide a $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$, entonces

$$p_i \,|b^k$$

y al ser $p_i$ un número primo, se sigue que

$$p_i \,|b$$

y como

$$p_i \,|a$$

tendremos que $p_i \neq 1$ es un divisor común de $a$ y $b$ lo cual contradice el hecho de que $a$ y $b$ sean primos entre sí, por tanto la suposición hecha es falsa y $\sqrt[k]{n}$ es irracional.

### 11.3.4 Teorema Fundamental de la Aritmética

*Cualquier número entero $n$ mayor que 1 puede escribirse de manera única, salvo el orden, como un producto de números primos.*

Demostración

Sea $a$ un número entero mayor que 1. Probaremos, primero, que $a$ puede escribirse como un producto de números primos y, posteriormente, veremos que esa descomposición es, salvo en el orden de los factores, única.

⁕ *Descomposición.*

- Si $a$ es primo, consideramos el número como un producto de un sólo factor y el teorema está demostrado.
- Si $a$ no es primo, entonces es compuesto, y la proposición 11.1.3 asegura que tendrá, al menos, un divisor primo.

Sea $p_1$ el menor divisor primo de $a$. Entonces existirá un entero $a_1$ tal que

$$a = p_1 a_1$$

- Si $a_1$ es primo, entonces el teorema está demostrado.
- Si $a_1$ no es primo, será compuesto y aplicando de nuevo la proposición 11.1.3 tendrá, al menos, un divisor primo.

Sea $p_2$ el menor divisor primo de $a_1$, entonces existirá un entero $a_2$ tal que

$$a_1 = p_2 a_2, \text{ con } a_1 > a_2$$

sustituyendo esta igualdad en la anterior, tendremos que

$$a = p_1 p_2 a_2$$

Repitiendo el proceso un número finito de veces, obtendremos

$$a_1 > a_2 > a_3 > \cdots > a_{k-1}$$

con

$$a = p_1 p_2 p_3 \cdots p_{k-1} a_{k-1}$$

donde $a_{k-1}$ es primo o es la unidad, entonces tomando $a_{k-1} = p_k$, si es primo o $a_{k-1} = 1$, se sigue que

$$\begin{array}{l} a = p_1 p_2 p_3 \cdots p_{k-1} \\ \text{ó} \\ a = p_1 p_2 p_3 \cdots p_{k-1} p_k \end{array}$$

y $a$ está escrito como un producto de factores primos.

⁕ *Unicidad.* Supongamos lo contrario, es decir $a$ puede descomponerse en producto de factores primos de dos formas distintas:

$$a = p_1 p_2 p_3 \cdots p_k, \text{ siendo los } p_i \text{ primos para } 1 \leqslant i \leqslant k$$

y

$$a = q_1 q_2 q_3 \cdots q_r, \text{ siendo los } q_j \text{ primos para } 1 \leqslant j \leqslant r.$$

Supondremos, también, que el número de factores es distinto, o sea, $k \neq r$. Tomaremos, sin perder generalidad por ello, $k < r$. Pues bien,

$$\begin{array}{rcl} a = p_1(p_2 p_3 \cdots p_k) & \Longrightarrow & p_1 \,|a \\ & \Longrightarrow & p_1 \,|q_1 q_2 q_3 \cdots q_r \\ & \Longrightarrow & p_1 \,|q_j \text{ para algún } j \text{ entre 1 y } r. \ \{\text{Corolario 11.3.3}\} \\ & \Longrightarrow & p_1 = q_j, \text{ ya que } q_j \text{ es primo y } p_1 \neq 1. \end{array}$$

Podemos suponer que $j = 1$. Si no lo fuese bastaría con cambiar el orden de los factores. Tendremos, pues, que $p_1 = q_1$ y

$$p_1 p_2 p_3 \cdots p_k = p_1 q_2 q_3 \cdots q_r$$

de donde, al ser $p_1 \neq 0$, se sigue que

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_r$$

Sea ahora

$$a_1 = p_2 p_3 \cdots p_k$$

y

$$a_1 = q_2 q_3 \cdots q_r.$$

Entonces $a_1 < a$, y

$$\begin{aligned} a_1 = p_2(p_3 p_4 \cdots p_k) &\implies p_2 \,|a_1 \\ &\implies p_2 \,|q_2 q_3 q_4 \cdots q_r \\ &\implies p_2 \,|q_j \text{ para algún } j \text{ entre 2 y } r. \ \{\text{Corolario 11.3.3}\} \\ &\implies p_2 = q_j, \text{ ya que } q_j \text{ es primo y } p_2 \neq 1. \end{aligned}$$

Y, ahora, podemos suponer que $j = 2$. Bastaría cambiar el orden de los factores si no fuese así. Tendríamos que $p_2 = q_2$ y, por lo tanto,

$$p_2 p_3 \cdots p_k = p_2 q_3 \cdots q_r$$

y, al ser $p_2 \neq 0$, tendremos que

$$p_3 p_4 \cdots p_k = q_3 q_4 \cdots q_r$$

y llamando

$$a_2 = p_3 p_4 \cdots p_k$$

y

$$a_2 = q_3 q_4 \cdots q_r.$$

se tiene que $a_2 < a_1 < a$.

Como $k < r$, si repetimos el proceso $k - 1$ veces, tendremos que

$$a_{k-1} = p_k$$

y

$$a_{k-1} = q_k q_{k+1} \cdots q_r.$$

siendo $a_{k-1} < a_{k-2} < \cdots < a_2 < a_1 < a$. Entonces,

$$\begin{aligned} a_{k-1} = p_k &\implies p_k \,|a_{k-1} \\ &\implies p_k \,|q_k q_{k+1} q_{k+2} \cdots q_r \\ &\implies p_k \,|q_j \text{ para algún } j \text{ entre } k \text{ y } r. \ \{\text{Corolario 11.3.3}\} \\ &\implies p_k = q_j, \text{ ya que } q_j \text{ es primo y } p_k \neq 1 \end{aligned}$$

y, razonando igual que en los pasos anteriores, podemos suponer que $j = k$, o sea, $p_k = q_k$ y,

$$p_k = q_k \cdot q_{k+1} \cdot \cdots \cdot q_r$$

y al ser $p_k \neq 0$, tendremos

$$1 = q_{k+1} \cdot q_{k+2} \cdot \cdots \cdot q_r$$

de donde se sigue que

$$q_{k+1} = q_{k+2} = \cdots = q_r = 1$$

lo cual es imposible ya que estos números son primos, por tanto, $k = r$ y

$$a = p_1 p_2 \cdot p_3 \cdots p_k$$

siendo, pues, la descomposición única.

### 11.3.5 Corolario

*Sea $a$ un número entero tal que $|a| > 1$, entonces $a$ tiene una factorización única de la forma:*

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

*siendo $k \geqslant 1$, los $p_k$ primos distintos con $p_1 < p_2 < \cdots < p_k$ y $\alpha_i \geqslant 1$ para $1 \leqslant i \leqslant k$.*

Demostración

- Si $a > 1$, por el *Teorema fundamental de la aritmética*, $a$ puede descomponerse en factores primos. Agrupamos todos los primos iguales a $p_1$ en el factor $p_1^{\alpha_1}$, hacemos igual con $p_2$, $p_3$, y así sucesivamente hasta $p_k$, obteniendo así la descomposición pedida.

- Si $a$ es negativo, entonces $-a$ es positivo con lo cual bastaría aplicar el razonamiento anterior a $-a$.

**Ejemplo 11.14** Descomponer en factores primos el número 720.

Solución

Obtendremos una descomposición del tipo anterior.

- Empezamos buscando el divisor más pequeño de 720.

  Como

  $$720 = 2 \cdot 360$$

  dicho divisor es, obviamente, el 2.

- Hacemos lo mismo con el 360.

  Dado que

  $$360 = 2 \cdot 180$$

  el divisor más pequeño de 360 es 2.

- Repetimos el proceso sucesivamente, y

$$\begin{aligned} 180 &= 2 \cdot 90 \\ 90 &= 2 \cdot 45 \\ 45 &= 3 \cdot 15 \\ 15 &= 3 \cdot 5 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Ahora bastaría sustituir cada igualdad en la igualdad anterior, y resultaría

$$720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^4 \cdot 3^2 \cdot 5$$

En la práctica suelen disponerse los cálculos en la forma siguiente:

| | |
|---|---|
| 720 | 2 |
| 360 | 2 |
| 180 | 2 |
| 90 | 2 |
| 45 | 3 |
| 15 | 3 |
| 5 | 5 |
| 1 | |

Ahora sólo habrá que contar los números que hay de cada factor, y

$$720 = 2^4 \cdot 3^2 \cdot 5$$

## 11.4 Divisores de un Número

### 11.4.1 Criterio General de Divisibilidad

*Sean $a$ y $b$ dos números enteros tales que $|a|, |b| > 1$. Se verifica que $a$ es divisible por $b$ si, y sólo si $a$ tiene, al menos, todos los factores primos de $b$ con exponentes iguales o mayores.*

Demostración

*"Sólo si".* En efecto, si $a$ es divisible por $b$, entonces existirá un número entero, $q$, tal que

$$a = bq$$

por tanto, $a$ tendrá, al menos, todos los factores primos de $b$ y sus exponentes serán mayores o iguales que los de $a$ dependiendo de que los factores primos de $q$ coincidan o no con los de $b$.

*"Si".* Si $a$ tiene, al menos, todos los factores primos de $b$ con exponentes iguales o mayores, entonces

$$\frac{a}{b} \in \mathbb{Z}$$

luego $a$ es divisible por $b$.

**Nota 11.3** Obsérvese que, según este criterio, los divisores de un número tendrán los mismos factores primos que éste con exponentes iguales o menores.

### 11.4.2 Obtención de todos los Divisores de un Número

*Sea $a$ es un número entero tal que $|a| > 1$ y sea $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ su descomposición en factores primos. Se verifica que $b$ es divisor de $a$ si, y sólo si $b$ es uno de los términos del producto*

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$$

Demostración

*"Sólo si".* En efecto, sea $b$ un divisor de $a$. Entonces, según la nota anterior, $b$ será de la forma

$$b = p_1^i p_2^j \cdots p_k^s, \text{ con } 0 \leqslant i \leqslant \alpha_1,\ 0 \leqslant j \leqslant \alpha_2\ \cdots 0 \leqslant s \leqslant \alpha_k$$

luego $b$ es uno de los términos del producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$$

*"Si".* Recíprocamente, cada término del producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$$

es de la forma:

$$p_1^i p_2^j \cdots p_k^s \text{ con } 0 \leqslant i \leqslant \alpha_1,\ 0 \leqslant j \leqslant \alpha_2\ \cdots 0 \leqslant s \leqslant \alpha_k$$

luego, de nuevo por la nota anterior, es un divisor de $a$.

**Ejemplo 11.15** Veamos una forma práctica y sencilla de calcular todos los divisores de un número. Calcularemos los de 720.

Solución

Según un ejemplo anterior

$$720 = 2^4 \cdot 3^2 \cdot 5$$

entonces los divisores de 720 serán los términos del producto

$$(1 + 2 + 2^2 + 2^3 + 2^4)(1 + 3 + 3^2)(1 + 5) = (1 + 2 + 4 + 8 + 16)(1 + 3 + 3^2)(1 + 5)$$

y una forma práctica de calcularlos todos es la siguiente tabla:

| | 1 | 2 | 4 | 8 | 16 |
|---|---|---|---|---|---|
| $\times 3$ | 3 | 6 | 12 | 24 | 48 |
| $\times 3^2$ | 9 | 18 | 36 | 72 | 144 |
| $\times 5$ | 5 | 10 | 20 | 40 | 80 |
| | 15 | 30 | 60 | 120 | 240 |
| | 45 | 90 | 180 | 360 | 720 |

donde en la primera fila hemos escrito todas las potencias de 2, desde $2^0$ hasta $2^4$. En las filas siguientes hemos colocado ordenadamente todos los productos de la fila anterior por cada una de las potencias de 3, desde 3 hasta $3^2$, y así sucesivamente.

### 11.4.3 Número de Divisores de un Número Compuesto

*Si $a$ un número entero tal que $|a| > 1$ y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es su descomposición en factores primos, entonces el número de divisores de $a$ es*

$$N_a = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Demostración

En efecto, según el teorema anterior los divisores de $a$ son los sumandos del producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$$

que tienen a su vez $\alpha_1+1, \alpha_2+1, \ldots, \alpha_k+1$ factores, respectivamente, luego el número total de sumandos posibles y, por tanto, el número de divisores de $a$ es

$$N_a = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$$

**Ejemplo 11.16** En un ejemplo anterior,

$$720 = 2^4 \cdot 3^2 \cdot 5$$

luego el número de divisores de 720 es

$$N_{720} = (4 + 1)(2 + 1)(1 + 1) = 30$$

**Ejemplo 11.17** Determinar dos enteros positivos cuyo máximo común divisor es 18, sabiendo que uno de ellos tiene 21 divisores y el otro tiene 10.

Solución

Sean $a$ y $b$ los números que buscamos. Por el corolario 11.3.5, existirán $p_1, p_2, \ldots, p_k$ y $q_1, q_2, \ldots, q_m$, primos distintos y $\alpha_i \geqslant 1,\ 1 \leqslant i \leqslant k$, $\beta_j \geqslant 1,\ 1 \leqslant j \leqslant m$, enteros, con $p_1 < p_2 < \cdots < p_k$ y $q_1 < q_2 < \cdots < q_m$ tales que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

y

$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$$

Supongamos que $a$ es el que tiene 21 divisores y $b$ el que tiene 10. Entonces, por 11.4.3,

$$N_a = 21 \implies (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1) = 21$$

$y$

$$N_b = 10 \implies (\beta_1 + 1)(\beta_2 + 1)\cdots(\beta_m + 1) = 10$$

luego,

- los $\alpha_i + 1,\ 1 \leqslant i \leqslant k$ son divisores de 21 y su producto es 21. Como los divisores de 21 son $1, 3, 7$ y 21, las opciones posibles son 1 y 21, 21 y 1, 3 y 7 y 7 y 3, es decir el producto anterior tiene, únicamente, dos factores. Si tenemos en cuenta que los $\alpha_i$ no pueden ser cero, las opciones válidas serían

$$(\alpha_1 + 1)(\alpha_2 + 1) = 3 \cdot 7 \implies \alpha_1 = 2 \text{ y } \alpha_2 = 6$$

ó

$$(\alpha_1 + 1)(\alpha_2 + 1) = 7 \cdot 3 \implies \alpha_1 = 6 \text{ y } \alpha_2 = 2.$$

- Razonando de la misma forma con los $\beta_j + 1$ y teniendo en cuenta que los divisores de 10 son $1, 2, 5$ y 10, las opciones válidas son

$$(\beta_1 + 1)(\beta_2 + 1) = 2 \cdot 5 \implies \beta_1 = 1 \text{ y } \beta_2 = 4$$

ó

$$(\beta_1 + 1)(\beta_2 + 1) = 5 \cdot 2 \implies \beta_1 = 4 \text{ y } \beta_2 = 1.$$

Por lo tanto tenemos dos opciones posibles para $a$ y $b$,

$$a = p_1^2 p_2^6 \quad \text{ó} \quad a = p_1^6 p_2^2$$

y

$$b = q_1 q_2^4 \quad \text{ó} \quad b = q_1^4 q_2$$

Por otra parte, el máximo común divisor de $a$ y $b$ es 18, luego $a$ y $b$ son divisibles por 18 y por 11.4.1 $a$ y $b$ han de tener, al menos, todos los factores primos de 18 con exponentes iguales o mayores y, dado que la descomposición en factores primos de 18 es $2 \cdot 3^2$, tendremos que $p_1 = q_1 = 2$, $p_2 = q_2 = 3$ y, por tanto,

$$a = 2^2 3^6 \quad \text{ó} \quad a = 2^6 3^2$$

y

$$b = 2 \cdot 3^4.$$

Pues bien, sean $D_a$ y $D_b$ son los conjuntos de divisores de $a$ y $b$, respectivamente:

- Si $a = 2^2 3^6$ y $b = 2 \cdot 3^4$, entonces

  $$D_a = \left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 2 \text{ y } 0 \leqslant \beta \leqslant 6\right\}$$

  y

  $$D_b = \left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 4\right\}$$

  de aquí que

  $$\text{m.c.d.}(a, b) = \max\left\{D_a \cap D_b\right\} = \max\left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 4\right\} = 2 \cdot 3^4 \neq 2 \cdot 3^2$$

  luego esta opción no es válida.

- Si $a = 2^6 3^2$ y $b = 2 \cdot 3^4$, entonces

  $$D_a = \left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 6 \text{ y } 0 \leqslant \beta \leqslant 2\right\}$$

  y

  $$D_b = \left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 4\right\}$$

  de aquí que

  $$\text{m.c.d.}(a, b) = \max\left\{D_a \cap D_b\right\} = \max\left\{2^\alpha 3^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 2\right\} = 2 \cdot 3^2$$

  y, consecuentemente, esta opción es la solución.

Así pues, los números buscados son:

$$a = 2^6 3^2 = 576$$

y

$$b = 2 \cdot 3^4 = 162$$

### 11.4.4 Suma de los Divisores de un Número Compuesto

*Si $a$ un número entero de valor absoluto es mayor que 1 y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es su descomposición en factores primos, entonces la suma de todos sus divisores es*

$$S = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

Demostración

Según vimos en 11.4.3, los divisores de $a$ son los sumandos del producto,

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$$

luego, la suma buscada viene dada por:

$$S = S_1 \cdot S_2 \cdots S_k$$

donde,

$$S_i = (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}),\ 1 \leqslant i \leqslant k$$

que es la suma de los términos de una progresión geométrica de razón $p_j$. Entonces,

$$S_i = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i} \cdot p_i - 1}{p_i - 1} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

y lo mismo puede hacerse con todos los demás factores.

**Ejemplo 11.18** Calcular la suma de todos los divisores de 720.

Solución

Como $720 = 2^4 \cdot 3^2 \cdot 5$, la suma de todos sus divisores será:

$$S = \frac{2^{4+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 31 \cdot 13 \cdot 6 = 2418$$

**Ejemplo 11.19** Hallar un número entero $a$ que no tiene más factores primos que $2, 5$ y $7$, sabiendo que $5a$ tiene 8 divisores más que $a$ y que $8a$ tiene 18 divisores más que $a$. Calcular también la suma de todos los divisores de $a$.

Solución

Sean $\alpha_1, \alpha_2$ y $\alpha_3$ las veces que se repiten, respectivamente, los factores primos $2, 5$ y $7$ en la factorización de $a$. Tendremos que

$$a = 2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}$$

luego,

$$5a = 2^{\alpha_1} 5^{\alpha_2+1} 7^{\alpha_3}$$
$$8a = 2^{\alpha_1+3} 5^{\alpha_2} 7^{\alpha_3}$$

y de aquí se sigue que el número de divisores de $a$, $5a$ y $8a$ es, respectivamente,

$$\begin{aligned} N_a &= (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \\ N_{5a} &= (\alpha_1 + 1)(\alpha_2 + 2)(\alpha_3 + 1) \\ N_{8a} &= (\alpha_1 + 4)(\alpha_2 + 1)(\alpha_3 + 1) \end{aligned}$$

y por los datos del enunciado,

$$\left.\begin{aligned} N_{5a} &= N_a + 8 \\ N_{8a} &= N_a + 18 \end{aligned}\right\}$$

es decir,

$$\begin{aligned} (\alpha_1 + 1)(\alpha_2 + 2)(\alpha_3 + 1) &= (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) + 8 \\ (\alpha_1 + 4)(\alpha_2 + 1)(\alpha_3 + 1) &= (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) + 18. \end{aligned}$$

Entonces,

$$\left.\begin{array}{rcl}(\alpha_1+1)(\alpha_3+1)(\alpha_2+2-\alpha_2-1) &=& 8\\ (\alpha_2+1)(\alpha_3+1)(\alpha_1+4-\alpha_1-1) &=& 18\end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl}(\alpha_1+1)(\alpha_3+1) &=& 8\\ (\alpha_2+1)(\alpha_3+1) &=& 6\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl}\dfrac{\alpha_1+1}{\alpha_2+1} &=& \dfrac{4}{3}\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl}\alpha_1+1 &=& 4\\ \alpha_2+1 &=& 3\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl}\alpha_1 &=& 3\\ \alpha_2 &=& 2\end{array}\right.$$

y sustituyendo, $\alpha_3 = 1$. Consecuentemente, el número pedido es:

$$a = 2^3 5^2 7 = 8 \cdot 25 \cdot 7 = 1400$$

Veamos ahora la suma de todos sus divisores. Por 11.4.4,

$$S = \frac{2^{3+1}-1}{2-1} \cdot \frac{5^{2+1}-1}{5-1} \cdot \frac{7^{1+1}-1}{7-1} = 3720$$

**Ejemplo 11.20** Un número entero positivo tiene 2 factores primos y 8 divisores. La suma de los divisores es 320. Hallar el número.

Solución

Sea $a$ el número buscado, sean $p_1$ y $p_2$ sus factores primos y $\alpha_1$, $\alpha_2$ el número de veces que se repiten. Entonces,

$$a = p_1^{\alpha_1} p_2^{\alpha_2}$$

y

$$(\alpha_1+1)(\alpha_2+1) = 8$$

De la segunda ecuación se sigue que $\alpha_1 + 1$ y $\alpha_2 + 1$ son dos divisores de 8 tales que su producto es 8. Como los divisores de 8 son 1, 2, 4 y 8, las posibles parejas son 1 y 8, 2 y 4, 4 y 2 y 8 y 1. Teniendo en cuenta que $\alpha_1 \neq 0$ y $\alpha_2 \neq 0$, podemos eliminar la primera y la última. Las posibles opciones son, por tanto,

$$\left.\begin{array}{rcl}(\alpha_1+1)(\alpha_2+1) &=& 2\cdot 4\\ \text{ó} & & \\ (\alpha_1+1)(\alpha_2+1) &=& 4\cdot 2\end{array}\right\} \Longrightarrow \left.\begin{array}{l}\alpha_1 = 1 \quad \text{y} \quad \alpha_2 = 3\\ \text{ó}\\ \alpha_1 = 3 \quad \text{y} \quad \alpha_2 = 1\end{array}\right\}$$

⋇ $\alpha_1 = 1$ y $\alpha_2 = 3$. En este caso, $a = p_1 p_2^3$ y al ser 320 la suma de sus divisores, tendríamos

$$(1+p_1)(1+p_2+p_2^2+p_2^3) = 320$$

luego $1 + p_1$ y $1 + p_2 + p_2^2 + p_2^3$ son divisores de 320 cuyo producto es 320. Como los divisores de 320 son

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 4 | 8 | 16 | 32 | 64 |
| × 5 | 5 | 10 | 20 | 40 | 80 | 160 | 320 |

las opciones posibles, emparejándolos para que su producto sea 320, serían

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $1+p_1$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 |
| $1+p_2+p_2^2+p_2^3$ | 320 | 160 | 80 | 40 | 20 | 10 | 5 |

Ahora bien,

$$p_1 \text{ es primo} \Longrightarrow p_1 \geqslant 2 \Longrightarrow 1+p_1 \geqslant 3$$

luego las dos primeras columnas no pueden ser solución del problema. También,

$$p_2 \text{ es primo} \Longrightarrow p_2 \geqslant 2 \Longrightarrow 1+p_2+p_2^2+p_2^3 \geqslant 15$$

y, por tanto, las dos últimas columnas tampoco son válidas. Por otra parte

$$p_1+1=16 \Longrightarrow p_1=15$$

lo cual es imposible ya que $p_1$ es primo, luego podemos eliminar, también, la quinta columna. Además,

$$1+p_2+p_2^2+p_2^3=80 \Longrightarrow p_2(1+p_2+p_2^2)=79$$

luego $p_2$ sería un divisor de 79 que es primo. Así pues, también podemos prescindir de la tercera columna y, consecuentemente, nos quedaría como única opción posible

$$1+p_1=8$$

y

$$1+p_2+p_2^2+p_2^3=40$$

es decir, $p_1=7$ y $p_2=3$ y, en tal caso, la solución sería

$$a=7\cdot 3^3=189$$

⋇ $\alpha_1=3$ y $\alpha_2=1$. En este caso, $a=p_1^3p_2$ y al ser 320 la suma de sus divisores, tendríamos

$$(1+p_1+p_1^2+p_1^3)(1+p_2)=320$$

luego $1+p_1$ y $1+p_2+p_2^2+p_2^3$ son divisores de 320 cuyo producto es 320. Procediendo de forma análoga al caso anterior:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $1+p_2$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 |
| $1+p_1+p_1^2+p_1^3$ | 320 | 160 | 80 | 40 | 20 | 10 | 5 |

y, consecuentemente, $p_1=3$ y $p_2=7$ y, en tal caso, la solución sería

$$a=3^3\cdot 7=189$$

**Ejemplo 11.21** Un número tiene 24 divisores, su mitad 18 divisores y su triple 28 divisores. Hallar el número y sus divisores.

Solución

Sea $a$ el número buscado y supongamos que su descomposición en factores primos es

$$a=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}.$$

Como su mitad tiene 18 divisores, $a$ ha de ser divisible por 2, luego uno de los factores primos, pongamos $p_1$, ha de ser 2, es decir,

$$a=2^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

y

$$\frac{a}{2}=2^{\alpha_1-1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}.$$

Entonces,

$$N_a = 24 \quad \Longrightarrow \quad (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 24$$

y

$$N_{a/2} = 18 \quad \Longrightarrow \quad (\alpha_1-1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 18.$$

Dividiendo miembro a miembro,

$$\frac{\alpha_1+1}{\alpha_1} = \frac{24}{18} \Longrightarrow \frac{\alpha_1+1}{\alpha_1} = \frac{4}{3} \Longrightarrow \alpha_1 = 3.$$

Así pues,

$$a = 2^3 p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

y si ninguno de los restantes factores primos es 3, entonces,

$$a = 2^3 p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k} \cdot 3$$

luego,

$$N_{3a} = 28 \Longrightarrow (3+1)(\alpha_2+1)\cdots(\alpha_k+1)(1+1) = 28 \Longrightarrow 2(\alpha_2+1)\cdots(\alpha_k+1)(1+1) = 7$$

y esto es imposible ya que 7 es primo. Por lo tanto uno de los factores primos de la descomposición de $a$, digamos $p_2$, ha de ser 3. Entonces,

$$a = 2^3 3^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

y

$$3a = 2^3 3^{\alpha_2+1} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

luego,

$$N_{3a} = 28 \Longrightarrow (3+1)(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 28 \Longrightarrow (\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 7$$

y como 7 es primo, el producto anterior tiene un sólo factor resultando, en consecuencia,

$$\alpha_2 + 2 = 7 \Longrightarrow \alpha_2 = 5$$

es decir el número pedido es

$$a = 2^3 \cdot 3^5 = 8 \cdot 243 = 1944.$$

Veamos cuales son los divisores de este número.

| | 1 | 2 | 4 | 8 |
|---|---|---|---|---|
| $\times\ 3$ | 3 | 6 | 12 | 24 |
| $\times\ 3^2$ | 9 | 18 | 36 | 72 |
| $\times\ 3^3$ | 27 | 54 | 108 | 216 |
| $\times\ 3^4$ | 81 | 162 | 324 | 648 |
| $\times\ 3^5$ | 243 | 486 | 972 | 1944 |

Los divisores de 1944 son todos los números que aparecen en la tabla.

## 11.5 Método para el Cálculo del Máximo Común Divisor y el Mínimo Común Múltiplo

En este apartado estableceremos un método alternativo al algoritmo de Euclides para el cálculo del máximo común divisor de dos números. Está basado en el Teorema fundamental de la aritmética.

### 11.5.1 Lema

*Dados dos números enteros $a$ y $b$, pueden encontrarse $k$ números primos $p_1, p_2, \ldots, p_k$ y enteros $\alpha_i \geqslant 0$ y $\beta_i \geqslant 0$, $1 \leqslant i \leqslant k$ tales que*

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$y$$
$$b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

*siendo $p_1 < p_2 < \cdots < p_k$.*

Demostración

La descomposición de $a$ y $b$ se sigue directamente del corolario 11.3.5.

Si hay algún factor primo de $a$ que no lo sea de $b$ se introduce en la factorización de éste con exponente cero y análogamente se hace con los factores de $b$ que no lo sean de $a$.

**Ejemplo 11.22** Descomponer $a = 270$ y $b = 368$ en factores primos según el lema anterior.

Solución

| | |
|---|---|
| 270 | 2 |
| 135 | 3 |
| 45 | 3 |
| 15 | 3 |
| 5 | 5 |
| 1 | |

$\Longrightarrow \quad 270 = 2 \cdot 3^3 \cdot 5$

| | |
|---|---|
| 368 | 2 |
| 184 | 2 |
| 92 | 2 |
| 46 | 2 |
| 23 | 23 |
| 1 | |

$\Longrightarrow \quad 368 = 2^4 \cdot 23$

Ahora bastaría escribir,

$$270 = 2^2 \cdot 3^2 \cdot 5 \cdot 23^0$$
$$368 = 2^4 \cdot 3^0 \cdot 5^0 \cdot 23$$

para tener los números en la forma descrita en el lema.

### 11.5.2 Teorema

*Sean $a$ y $b$ dos enteros positivos. $d$ es el máximo común divisor de $a$ y $b$ si, y sólo si $d$ es igual al producto de los factores primos de ambos elevados a los menores exponentes con que aparezcan en la descomposición.*

Demostración

Por el lema anterior, pueden encontrarse números primos $p_i$ y enteros $\alpha_i \geqslant 0,\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k$ tales

que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
y
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

*"Sólo si".* En efecto, supongamos que $d$ es el máximo común de $a$ y $b$. Entonces, $d$ tendrá que ser un divisor de $a$ y $b$ luego por el criterio general de divisibilidad (11.4.1) tendrá todos los factores primos de $a$ y de $b$ con exponentes iguales o menores, es decir, será de la forma:

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

siendo $\gamma_i \leqslant \alpha_i$ y $\gamma_i \leqslant \beta_i$, para $1 \leqslant i \leqslant k$, es decir,

$$\gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k$$

y como $d$ ha de ser el máximo de los divisores comunes de $a$ y de $b$,

$$\gamma_i = \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k$$

*"Si".* Supongamos ahora que

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

con $\gamma_i = \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k$. Entonces,

1. $d|a$ y $d|b$. En efecto, bastaría observar que $a$ y $b$ tienen todos los factores primos de $d$ con exponentes iguales o mayores y aplicar el criterio general de divisibilidad (11.4.1).
2. $d$ es el máximo. En efecto, si $c$ es otro divisor de $a$ y $b$, entonces por 11.4.1, tendrá todos los factores primos de $a$ y $b$ con exponentes iguales o menores, es decir $c$ tendrá la forma:

   $$c = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$$

   con $\delta_i \leqslant \alpha_i$ y $\delta_i \leqslant \beta_i$, $1 \leqslant i \leqslant k$, luego $\delta_i \leqslant \min\{\alpha_i, \beta_i\}$, o sea $\delta_i \leqslant \gamma_i$. Por lo tanto, $c|d$ y, consecuentemente, $d$ es el máximo.

### 11.5.3 Teorema

*Sean $a$ y $b$ dos enteros positivos. $m$ es el mínimo común múltiplo de $a$ y $b$ si, y sólo si $m$ es igual al producto de los factores primos de ambos elevados a los mayores exponentes con que aparezcan en la descomposición.*

Demostración

De acuerdo con el lema 11.5.1, podremos encontrar números primos $p_i$ y enteros $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$, $1 \leqslant i \leqslant k$ tales que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
y
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

*"Sólo si".* En efecto, si $m$ es el mínimo común múltiplo de $a$ y $b$, entonces será múltiplo de $a$ y múltiplo de $b$ luego por el criterio general de divisibilidad (11.4.1) tendrá todos los factores primos de $a$ y de $b$ con exponentes iguales o mayores, es decir, será de la forma:

$$m = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

siendo $\gamma_i \geqslant \alpha_i$ y $\gamma_i \geqslant \beta_i$ para $1 \leqslant i \leqslant k$, o sea,

$$\gamma_i \leqslant \max\{\alpha_i, \beta_i\}\,,\ 1 \leqslant i \leqslant k$$

y como $m$ ha de ser el mínimo de los múltiplos comunes de $a$ y de $b$,

$$\gamma_i = \max\{\alpha_i, \beta_i\}\,,\ 1 \leqslant i \leqslant k$$

*"Si"*. Recíprocamente, sea

$$m = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

con $\gamma_i = \max\{\alpha_i, \beta_i\}\,,\ 1 \leqslant i \leqslant k$. Entonces,

1. $a|m$ y $b|m$. En efecto, bastaría observar que $a$ y $b$ tienen todos los factores primos de $m$ con exponentes iguales o menores y aplicar el criterio general de divisibilidad (11.4.1).
2. $m$ es el mínimo. En efecto, si $c$ es otro múltiplo de $a$ y $b$, entonces por 11.4.1, tendrá todos los factores primos de $a$ y $b$ con exponentes iguales o mayores, es decir $c$ tendrá la forma:

   $$c = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$$

   con $\delta_i \geqslant \alpha_i$ y $\delta_i \geqslant \beta_i$, $1 \leqslant i \leqslant k$, luego $\delta_i \geqslant \max\{\alpha_i, \beta_i\}$, o sea $\delta_i \geqslant \gamma_i$. Por lo tanto, $m|c$ y, consecuentemente, $m$ es el mínimo.

**Ejemplo 11.23** Calcular el máximo común divisor de 2340 y 8248.

Solución

Descomponemos ambos números en factores primos

| | |
|---|---|
| 8428 | 2 |
| 4214 | 2 |
| 2107 | 7 |
| 301 | 7 |
| 43 | 43 |
| 1 | |

$$\Longrightarrow \quad 8428 = 2^2 \cdot 7^2 \cdot 43$$

| | |
|---|---|
| 2340 | 2 |
| 1170 | 2 |
| 585 | 3 |
| 195 | 3 |
| 65 | 5 |
| 13 | 13 |
| 1 | |

$$\Longrightarrow \quad 2340 = 2^2 \cdot 3^2 \cdot 5 \cdot 13$$

o lo que es igual

$$2340 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 13 \cdot 43^0$$
$$8428 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 13^0 \cdot 43$$

y por el teorema anterior,

$$\text{m.c.d.}\,(8428, 2340) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 13^0 \cdot 43^0 = 4$$