# Matemática Discreta I
# Clase 15 - Factorización en primos 2 / Congruencia

FAMAF / UNC

6 de mayo de 2021

## Proposición

*Existen infinitos números primos.*

## Demostración

Haremos la demostración por el absurdo.

Sean $p_1, p_2, \ldots, p_r$ todos los números primos.

Sea $n = p_1 p_2 \ldots p_r + 1$.

Sea $p$ primo tal que $p|n \Rightarrow$ existe $i$ tal que $p = p_i$.

Ahora bien $p_i|n$ y $p_i|p_1 p_2 \ldots p_r$, luego $p_i|n - p_1 p_2 \ldots p_r = 1$. Absurdo.

$\square$

## Ejemplo

Probemos que si $m$ y $n$ son enteros tales que $m \geq 2$ y $n \geq 2$, entonces $m^2 \neq 2n^2$.

## Demostración

Recordemos que

$$(ab)^r = a^r b^r, \quad (a^r)^s = a^{rs}, \quad a \cdot a^r = a^{r+1}.$$

$$n = 2^x p_2^{e_2} \dots p_r^{e_r} \quad (x \geq 0,\ p_i \text{ todos primos diferentes a 2.})$$

$$n^2 = 2^{2x} p_2^{2e_2} \dots p_r^{2e_r}$$

$$\boxed{2n^2 = 2^{2x+1} p_2^{2e_2} \dots p_r^{2e_r}.} \qquad (*)$$

$$m = 2^y q_2^{f_2} \dots q_s^{f_s} \quad (y \geq 0,\ q_i \text{ todos primos diferentes a 2.})$$

$$\boxed{m^2 = 2^{2y} q_2^{2f_2} \dots q_s^{2f_s}} \qquad (**)$$

Como $2x + 1 \neq 2y$ (el primero es impar y el segundo par), por unicidad de la descomposición, (*) $\neq$ (**), es decir $m^2 \neq 2n^2$.

$\square$

### Observación

El ejemplo anterior nos dice que

$$m^2 \neq 2n^2 \quad \Rightarrow \quad \frac{m^2}{n^2} \neq 2 \quad \Rightarrow \quad \left(\frac{m}{n}\right)^2 \neq 2 \quad \Rightarrow \quad \frac{m}{n} \neq \sqrt{2}.$$

Es decir $\sqrt{2}$ *no es un número racional.*

### Ejercicio

Probar que $\sqrt{15}$ no es un número racional.

# Notación

Sean $m$ y $n$ dos enteros positivos, a veces es conveniente escribir la factorización prima de ambos números usando los mismos primos.
Los primos que usamos son los que se encuentran en la factorización prima de ambos:

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

con $e_i, f_i \geq 0$ para $i = 1, \dots, r$ y $e_i$ o $f_i$ distinto de cero.

**Ejemplo**

168 y 495. Tenemos que

$$168 = 2^3 \cdot 3^1 \cdot 7^1, \qquad 495 = 3^2 \cdot 5^1 \cdot 11^1$$

Luego

$$168 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0,$$
$$495 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^1$$

Veremos ahora un resultado que se puede deducir fácilmente del Teorema Fundamental de la Aritmética (TFA).

### Proposición

*Sean* $m, n \geq 2$ *con*

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

*donde* $p_i$ *primo y* $e_i, f_i \geq 0$ *para* $i = 1, \dots, r$.
*Entonces* $m|n$ *si y sólo si* $e_i \leq f_i$ *para todo* $i$.

### Demostración

($\Rightarrow$) Por la descomposición de $m$ es claro que $p_i^{e_i}|m$. Como $m|n$ entonces $p_i^{e_i}|n$. Es decir $n = p_i^{e_i}u$. Es claro por TFA entonces que $e_i \leq f_i$.

($\Leftarrow$) Como $e_i \leq f_i$, tenemos que $p_i^{e_i}|p_i^{f_i}$, para $1 \leq i \leq r$. Luego

$$p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} | p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

Es decir $m|n$.

Ahora veremos que es posible calcular el mcd y el mcm de un par de números sabiendo sus descomposiciones primas.

## Proposición

*Sean $m$ y $n$ enteros positivos cuyas factorizaciones primas son*

$$m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \qquad n = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}.$$

*a) El mcd de $m$ y $n$ es $d = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ donde, para cada $i$ en el rango $1 \leq i \leq r$, $k_i$ es el mínimo entre $e_i$ y $f_i$.*

*b) El mcm de $m$ y $n$ es $u = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ donde, para cada $i$ en el rango $1 \leq i \leq r$, $h_i$ es el máximo entre $e_i$ y $f_i$.*

## Demostración

(a) Es claro que $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ divide a $m$ y $n$.

Sea $c$ tal que $c|n$ y $c|m$, entonces los primos que intervienen en la factorización de $c$ son $p_1, \ldots, p_r$ y por lo tanto

$$c = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}.$$

Además, como $c|n$ y $c|m$ tenemos que $t_i \leq e_i, f_i$ y por lo tanto $t_i \leq k_i = \text{mín}(e_i, f_i)$.

De esto se deduce que $c|p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} = d$.

(b) Se deja como ejercicio.

$\square$

Ejemplo

Encontremos el mcd y el mcm de 168 y 495.

Ya habíamos visto que

$$\begin{aligned} 168 &= 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0, \\ 495 &= 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^1 \end{aligned}$$

Luego

$$\begin{aligned} \mathrm{mcd}(168, 495) &= 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3, \\ \mathrm{mcm}(168, 495) &= 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^1. \end{aligned}$$

# Congruencia - Definiciones y propiedades básicas

Definición

Sean $a$ y $b$ enteros y $m$ un entero positivo. Diremos que $a$ es *congruente* a $b$ *módulo* $m$, y escribimos

$$a \equiv b \pmod{m}$$

si $a - b$ es divisible or $m$, es decir si $m|a - b$.

Observar que

$$a \equiv 0 \pmod{m} \Leftrightarrow m|a$$

y que

$$a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m}.$$

## Notación

$a \equiv b \pmod{m}$ también lo denotamos $a \equiv b\ (m)$.

## Ejemplo

- $7 \equiv 3\ (2)$, pues $2 | 7 - 3 = 4$.
- $17 \equiv 8\ (3)$, pues $3 | 17 - 8 = 9$.
- $8 \equiv 17\ (3)$, pues $3 | 8 - 17 = -9$.
- $35 \equiv 13\ (11)$, pues $11 | 35 - 13 = 22 = 2 \cdot 11$.

**Proposición**

*Sean $a$ entero y $m$ un entero positivo. Sea $r$ el resto de dividir $a$ por $m$.*

$$a \equiv r \pmod{m}.$$

**Demostración**

$a = mq + r$ con $0 \leq r < m$.

Luego,

$$a - r = mq \quad \Rightarrow \quad m | a - r \quad \Rightarrow \quad a \equiv r \pmod{m}.$$

$\square$

Es fácil verificar que la congruencia módulo $m$ verifica las siguientes propiedades

a) Es *reflexiva* es decir $x \equiv x \pmod{m}$.

b) Es *simétrica*, es decir si $x \equiv y \pmod{m}$, entonces

$y \equiv x \pmod{m}$.

c) Es *transitiva*, es decir si $x \equiv y \pmod{m}$ e $y \equiv z \pmod{m}$, entonces $x \equiv z \pmod{m}$.

Demostración

a) $m | x - x = 0$ y por lo tanto $x \equiv x \pmod{m}$.

b) $x \equiv y \ (m) \Rightarrow m | x - y \Rightarrow m | -(x - y) \Rightarrow m | y - x \Rightarrow y \equiv x \ (m)$.

c) $x \equiv y \ (m) \wedge y \equiv z \ (m) \quad \Rightarrow \quad m | x - y \wedge m | y - z \quad \Rightarrow$

$m | (x - y) + (y - z) = x - z \quad \Rightarrow \quad x \equiv z \ (m)$.

$\square$

### Proposición

*Sean $a$ y $b$ enteros y $m$ un entero positivo. Entonces $a \equiv b \pmod{m}$ si y sólo si $a$ y $b$ tienen el mismo resto en la división por $m$.*

### Demostración

Se deduce por la proposición de la p. 12 y transitividad. $\square$

Así como separamos $\mathbb{Z}$ en los números pares e impares, la propiedad anterior nos permite expresar $\mathbb{Z}$ como una unión de $m$ subconjuntos.

Es decir si $\mathbb{Z}_{[r]} = \{x \in \mathbb{Z} : \text{el resto de dividir } x \text{ por } m \text{ es } r\}$,

entonces,

$$\mathbb{Z} = \mathbb{Z}_{[0]} \cup \mathbb{Z}_{[1]} \cup \cdots \cup \mathbb{Z}_{[m-1]}.$$