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

FAMAF / UNC

6 de mayo de 2021

## Proposición

*Existen infinitos números primos.*

## Proposición

*Existen infinitos números primos.*

Demostración. Por el absurdo.

Supongamos que existen finitos primos $p_1, \dots, p_n$. Sea $a = 1 + p_1 \cdots p_n$.

$a = p_1^{e_1} \cdots p_n^{e_n}$ con $0 \leq e_i$ (por TFA)

Como $a \neq 1 \Rightarrow$ algún $e_i > 0 \Rightarrow p_i \mid a$

Como $p_i \mid p_1 \cdots p_n$ ($p_i$ (sin)) $\Rightarrow p \mid a - p_1 \cdots p_n = 1$ abs.

## 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.

□

## Ejemplo

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

obs Esto implica que $\sqrt{2}$ no es racional.

Que un número sea racional significa que es de la forma $\frac{m}{n}$ $(m, n \in \mathbb{Z})$

$\sqrt{2}$ racional $\iff$ $\sqrt{2} = \frac{m}{n} \iff (\sqrt{2})^2 = \left(\frac{m}{n}\right)^2$

$\iff 2 = \frac{m^2}{n^2} \iff 2n^2 = m^2$.

Luego $\sqrt{2}$ no es racional $\iff \forall m, n \in \mathbb{Z}$

$m^2 \neq 2n^2$

## 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

## 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

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

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

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

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

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

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.*

# 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 $m = 2^3 \cdot 7^2 \cdot 11$

$n = 3^2 \cdot 5 \cdot 7^4 \cdot 13$

$m = 2^3 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^1 \cdot 13^0$

$n = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^4 \cdot 11^0 \cdot 13^1$

# 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.

# 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).

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 $i$.*

Ej $p^1 q^2 \mid p^2 q^3$ $\wedge$ $p^2 q \nmid p^1 q^2$

$p^1 \mid p^3$

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

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 $p^{e_i}|m$. Como $m|n$ entonces $p^{e_i}|n$. Es decir $n = p^{e_i}u$. Es claro por TFA entonces que $e_i \leq f_i$.

($\Leftarrow$) Como $e_i \leq f_i$, tenemos que $p^{e_i}|p^{f_i}$, 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 $f_i$.*

Ej $\mathrm{mcd}(2^3 \cdot 3^2, 2^1 \cdot 3^2) = 2^1 \cdot 3^2$

$\mathrm{mcd}(2^3 \cdot 3^2 \cdot 7, 3 \cdot 5^2 \cdot 11) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3$

## Demostración

(a) Es claro que $d = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ 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 $p_1, \dots, p_r$ y por lo tanto

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

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 $c|p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = d$.

(b) Se deja como ejercicio.

□

## Ejemplo

Encontremos el mcd y el mcm de 168 y 495.

Ya habíamos visto que

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

Luego

- $\text{mcd}(168, 495) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3.$
- $\text{mcm}(168, 495) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^1.$

# 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 $m$.

Observar que

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

y que

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

## Proposición

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

## Demostración

Si $a = mh + r$ y $b = mk + s$, con $0 \leq r, s < m$, podemos suponer, sin perdida de generalidad, que $r \leq s$, luego

$$b - a = m(k - h) + (s - r) \qquad \text{con } 0 \leq s - r < m.$$

Se sigue que $s - r$ es el resto de dividir $b - a$ por $m$.
Luego si $a \equiv b$ (mód $m$), el resto de dividir $b - a$ por $m$ es 0, y por lo tanto $s - r = 0$ y $s = r$.
Si $a$ y $b$ tienen el mismo resto en la división por $m$, entonces $a = mh + r$ y $b = mk + r$, luego $a - b = m(h - k)$ que es divisible por $m$. □

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

Es decir si $m \in \mathbb{Z}$

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

entonces dado $m \in \mathbb{N}$,

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

Ej: $\mathbb{Z}$ = multiplos de 3 $\mathbb{Z}_0$ $(m=3)$

" " $+1$ $\mathbb{Z}_1$

" " $+2$ $\mathbb{Z}_2$

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

$m \mid x-y \quad \wedge \quad m \mid y-z$

$\Rightarrow m \mid (x-y)+(y-z) = x-z$

$\Rightarrow x \equiv z \pmod{m}$

Demostración

a) $x - x = 0$ y por lo tanto divisible por $m$.

b) $x - y = km$, entonces $y - x = (-k)m$.

c) $x - y = km$ y $y - z = lm$, $\Rightarrow x - z = (x - y) + (y - z) = (k + l)m$. $\square$

La utilidad de las congruencias reside principalmente en el hecho de que son compatibles con las operaciones aritméticas. Específicamente, tenemos el siguiente teorema.

**Teorema**

*Sea $m$ un entero positivo y sean $x_1$, $x_2$, $y_1$, $y_2$ enteros tales que*

$$x_1 \equiv x_2 \pmod{m}, \qquad y_1 \equiv y_2 \pmod{m}.$$

*Entonces*

*a)* $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

*b)* $x_1 y_1 \equiv x_2 y_2 \pmod{m}$,

*c) Si* $x \equiv y \pmod{m}$ *y* $j \in \mathbb{N}$, *entonces* $x^j \equiv y^j \pmod{m}$.

## Demostración

(a) Por hipótesis $\exists x, y$ tq $x_1 - x_2 = mx$ e $y_1 - y_2 = my$. Luego,

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= mx + my \\ &= m(x + y),\end{aligned}$$

y por consiguiente el lado izquierdo es divisible por $m$.

(b) Aquí tenemos

$$\begin{aligned}x_1 y_1 - x_2 y_2 &= x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2 \\ &= (x_1 - x_2) y_1 + x_2 (y_1 - y_2) \\ &= mxy_1 + x_2 my \\ &= m(xy_1 + x_2 y),\end{aligned}$$

y de nuevo el lado izquierdo es divisible por $m$.

(c) Lo haremos por inducción sobre $j$.

Es claro que si $j = 1$ el resultado es verdadero.

Supongamos ahora que el resultado vale para $j - 1$, es decir

$$x^{j-1} \equiv y^{j-1} \pmod{m}.$$

Como $x \equiv y \pmod{m}$, por (b) tenemos que

$$x^{j-1}x \equiv y^{j-1}y \pmod{m},$$

es decir

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

□