Factorización prima

Definicion

- Se dice que un entero positivo p es primo si
  - $p \geq 2$
  - Los unicos numeros que dividen a p son 1 y p
- El número 1 no es primo

Propiedades

- Todo entero positivo puede expresarse como producto de primos
- Existen infinitos números primos
- La factorización en primos de un entero positivo es única — Exceptuando permutaciones
- p es primo $\Leftrightarrow$ $p = m_1 m_2 \;\Rightarrow\; m_1 = 1,\; m_2 = p$
- $m \geq 2$ no es primo $\Leftrightarrow$ $\exists\; 1 < m_1,\; m_2 < m : m = m_1 m_2$
- $a \in \mathbb{Z}$ y p primo $\Rightarrow$
  - $p \nmid a \Rightarrow mcd(a, b) = 1$
  - p y p' son primos $\wedge\, p \mid p' \;\Rightarrow\; p = p'$
- $n > 0$ no es primo $\Rightarrow \exists\, m > 0 : m \mid n \;\wedge\; m < \sqrt{n}$
- $n \geq 2$ — $\forall m : 1 < m \leq \sqrt{n} : m \nmid n \Rightarrow$ n es primo
- $n \geq 2$ — $\forall p : 1 < p \leq \sqrt{n} : p \nmid n \Rightarrow$ n es primo — p es primo
- $p \mid xy \Rightarrow p \mid x \vee p \mid y$
- $p \mid x_1 x_2 \ldots x_n \Rightarrow p \mid x_i$ para algun x_i $(1 \leq i \leq n)$
- $n \in \mathbb{Z}^+$ — $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$
  - $p_1, p_2, \ldots, p_r$ — primos distintos
  - $e_1, e_2, \ldots, e_r$ — Enteros positivos
- $m, n \geq 2$
  - $m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $n = p_1^{f_1} p_2^{f_2} \ldots p_r^{f_r}$ $\Rightarrow$ $m \mid n \Leftrightarrow e_i \leq f_i\,, \forall i$
  - donde p_1 primo $\wedge\, e_i, f_i \geq 0$ para $i = 1, \ldots, r$

mcd y mcm

- El mcd de m y n es
  - $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ — donde para cada i en el rango — $1 \geq i \geq r, k_i$ es el mínimo entre $e_i \wedge f_i$
- El mcm de m y n es
  - $d = p_1^{h_1} p_2^{h_2} \ldots p_r^{h_r}$ — donde para cada i en el rango — $1 \geq i \geq r, h_i$ es el maximo entre $e_i \wedge f_i$