PRACTICO 3

Teorema Fundamental de la Aritmetica

1) $\exists$ primos $p_1, \dots, p_k$ con $k \geq 1$ t.q $n = p_1 \cdot \dots \cdot p_k$
(Todo entero > 1 es prod. de primos)

2) Hay unicidad en la factorización, a menos del orden de los factores

Proposición: Sean a y $b \in \mathbb{Z}^+$ tq $a = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \dots$ y $b = 2^{b_2} \cdot 3^{b_3} \cdot 5^{b_5} \dots$
Entonces:

1) $a | b \leftrightarrow a_p \leq b_p \ \forall p$

2) $mcd(a,b) = 2^{d_2} \cdot 3^{d_3} \cdot 5^{d_5} \dots$
siendo $d_p = \min\{a_p, b_p\}$ $\forall$ primo p

3) $mcm(a,b) = 2^{m_2} \cdot 3^{m_3} \cdot 5^{m_5} \dots$
siendo $m_p = \max\{a_p, b_p\}$ $\forall$ primo p

Corolario: Existen infinitos primos

Obs: Si en la descomposición de un entero positivo a, tomamos primos distintos, entonces estos pueden aparecer con exponentes, por lo que $a > 1$ es: $a = p_1^{e_1} \cdot p_2^{e_2} \dots p_k^{e_k}$ con $e_i \in \mathbb{Z}^+$

Corolario: Sea $n = p_1^{e_1} \dots p_k^{e_k}$ con p_i primos distintos y $e_i \in \mathbb{Z}^+$
Entonces:

1) $Div_+(n) = \{p_1^{c_1} \cdot p_2^{c_2} \dots p_k^{c_k} : c_i \in \mathbb{N}$ y $c_i \leq e_i, \ \forall i = 1 \dots k\}$

2) La cantidad de divisores posit. de n es: $\#Div_+(n) = (e_1 + 1) \dots (e_k + 1)$

3) El entero n es un cuadrado perfecto ($\exists m \in \mathbb{Z} : n = m^2$) $\leftrightarrow 2 | e_i \ \forall i = 1 \dots k$

4) $\exists m \in \mathbb{Z}^+$ y $k \in \mathbb{Z}^+ : n = m^k \leftrightarrow$ todos los e_i son multiplos de k

Propiedades practico:

- Sea (p_n) la sucesión de numeros primos $\Rightarrow \forall n \in \mathbb{N}$ $p_1 \cdot p_2 \dots p_n + 1 \geq p_{n+1}$.
- $n \in \mathbb{N}$ es un cuadrado perfecto $\leftrightarrow$ n tiene un numero impar de divisores positivos
- Si $p > 2$ es primo $\Rightarrow p = 4k \pm 1$ para algun $k \in \mathbb{Z}$
- Si $p > 3$ es primo $\Rightarrow p = 6k \pm 1$ para algun $k \in \mathbb{Z}$
- $\exists$ infinitos primos de la forma $4k-1$
- (x_1, x_2, x_3) son coprimos $\leftrightarrow \nexists$ p primo que divida a x_i $\forall i = 1,2,3$
- Si p es primo y $p^2 | ab$ y $mcd(a,b) = 1$ $\Rightarrow p^2 | a$ o $p^2 | b$
- $mcd(a^n, b^n) = mcd(a,b)^n$ con $n \geq 1$
- Si p es primo $\Rightarrow p | \binom{p}{i}$ $\forall\, 0 < i < p$ siendo $\binom{p}{i}$ las combinaciones de p en i