Números Primos

Todo numero entero positivo es divisible por 1 y por si mismo
Un entero positivo $p > 1$ se llama primo si los únicos divisores positivos de p sin 1 y p
Si un entero positivo no es primo se llama compuesto

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...\}$

Ejemplo: Determine si un numero dado es primo o compuesto

- 121. Compuesto porque $11|121$
- 53. Primo porque $\forall n(n \in \mathbb{Z} \land n|53 \Longrightarrow n = 1 \lor n = 53)$
- 259. Compuesto porque $7|259$
- 641. Primo porque $\forall n(n \in \mathbb{Z} \land n|641 \Longrightarrow n = 1 \lor n = 641)$

Teorema Fundamental de la Aritmética FTA

Todo entero positivo mayor que 1 se puede escribir de forma única como un primo o como el producto de dos o mas primos, en el que los factores primos se escriben de forma no decreciente.

Ejemplo: Descomponga en primos

- $89 = 89$
- $256 = 2^8$
- $525 = 3 \cdot 5^2 \cdot 7$
- $1000 = 2^3 \cdot 5^3$

Teoremas

- **Teorema:** Si n es un entero compuesto entonces n tiene un divisor primo menor o igual $\sqrt{n}$

  Demostración:

  Supongamos que n es un entero compuesto.

  Es decir $\exists k \in \mathbb{Z} \land k \neq 1 \land k \neq n$ tal que $k|n$ de modo que $n = k \cdot l$ donde $l \in \mathbb{Z}$.

  Observemos que $k \leq \sqrt{n} \land l \leq \sqrt{n}$, dado que si no fuera así, es decir si $k > \sqrt{n} \lor l > \sqrt{n}$ entonces $k \cdot l > \sqrt{n} \cdot \sqrt{n} \Longrightarrow k \cdot l > n$ lo cual es falso

  Si k es primo entonces queda probado que n tiene un divisor primo menor o igual que $\sqrt{n}$

  Si k y l no son primos entonces por el Teorema Fundamental de la Aritmética poseen al menos un divisor primo, y como k o l son menores o iguales que $\sqrt{n}$ este divisor también lo sera.

  Ejemplo:

  Para saber si 817 es primo o compuesto buscamos si es divisible por un entero menor o igual que $\sqrt{817} \approx 28.58$

  Buscamos los $\mathbb{P} < 28 = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$

  Encontramos que $817 = 19 \cdot 43$ por lo que 817 es compuesto

  Observe:

  Por el teorema anterior, si un entero positivo n no tiene divisores primos menores o iguales que $\sqrt{n}$ entonces n es primo.

- **Teorema:** Existen infinitos números primos

  Demostración: *(por reducción al absurdo)*

  Supongamos que existen un numero finito de primos $\{P_1, P_2, ..., P_n\}$.
  Sea $Q = P_1 \cdot P_2 \cdot ... \cdot P_n + 1$

  Observe que $P_1, P_2, ..., P_n$ no son divisores de Q

  Ademas Q puede ser primo o compuesto y por Teorema Fundamental de la Aritmética si Q es compuesto se puede descomponer en factores primos

  - Si Q fuera primo entonces Q seria otro primo fuera de $\{P_1, P_2, ..., P_n\}$ lo cual no puede ocurrir.
  - Si Q fuera compuesto debe existir algún $P_i \in \{P_1, P_2, ..., P_n\}$ tal que $P_i|Q$
    Pero también $P_i|P_1 \cdot P_2 \cdot ... \cdot P_n$
    Luego $P_i|Q - P_1 \cdot P_2 \cdot ... \cdot P_n$ Es decir $P_i|1$

Primos Relativos

Los enteros positivos a y b se llaman primos relativos si su mínimo común divisor $\text{mcd}(a, b) = 1$

Los enteros $a_1, a_2, ..., a_n$ son primos relativos dos a dos si $\text{mcd}(a_i, a_j) = 1$ para $i = 1, 2, ..., n$ y $j = 1, 2, ..., n$ con $i \neq j$

Ejemplo: $5, 7, 68, 99$ son primos relativos dos a dos porque:

$$\begin{aligned}
\text{mcd}(5,7) &= 1 \\
\text{mcd}(5,68) &= 1 \\
\text{mcd}(5,99) &= 1 \\
\text{mcd}(7,68) &= 1 \\
\text{mcd}(7,99) &= 1 \\
\text{mcd}(68,99) &= 1
\end{aligned}$$