



TEOREMAS SOBRE NUMEROS ENTEROS

En esta hoja se enunciarán una serie de teoremas sobre números enteros que nos resultarán muy útiles en la resolución de problemas. Comenzaremos definiendo la función de Euler:

Función de Euler: Sea m un entero positivo. Se denota por $\Phi(m)$ el número de enteros k tal que $0 < k \leq m$ verificándose que $\text{m.c.d.}(k, m) = 1$. La función

$$\begin{aligned}\Phi: \mathbf{N} &\rightarrow \mathbf{N} \\ m &\rightarrow \Phi(m)\end{aligned}$$

se denomina *función de Euler*.

Cálculo de la función de Euler:

- 1) $\Phi(1) = 1, \Phi(2) = 1, \Phi(3) = 2, \Phi(4) = 2$
- 2) Si $m > 1$, $\Phi(m)$ es el número de unidades en \mathbf{Z}_m .
- 3) Si $p > 1$ primo \Rightarrow para todo $k < p$, $\text{m.c.d.}(p, k) = 1$

$$\Rightarrow \Phi(p) = p - 1, \quad \Phi(p^a) = p^a \left(1 - \frac{1}{p}\right)$$

- 4) Si $\Phi(p) = p - 1 \Rightarrow p$ es primo.

- 5) *Cálculo de $\Phi(m)$:* Si $m = p_1^{a_1} \cdots p_r^{a_r}$ (factorización) $\Rightarrow \Phi(m) = m \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$

Teorema de Euler:

Si $m > 1$ y k son números enteros primos entre sí ($\text{m.c.d.}(k, m) = 1$), entonces

$$k^{\Phi(m)} \equiv 1 \pmod{m}.$$

Teorema de Fermat:

Si p es primo, entonces para todo entero a tal que p no divide a a se verifica

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corolario: Si p es primo, entonces $a^p \equiv a \pmod{p}$.

Teorema de Wilson:

Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$.