

Introducción a Python – Sesión 1

Cesar Garcia

2025

Definition $x \pmod n$

- remainder of $\frac{x}{n}$

$$\begin{array}{lll} 0 \bmod 4 = 0 & 4 \bmod 4 = 0 & 8 \bmod 4 = 0 \\ 1 \bmod 4 = 1 & 5 \bmod 4 = 1 & 9 \bmod 4 = 1 \\ 2 \bmod 4 = 2 & 6 \bmod 4 = 2 & 10 \bmod 4 = 2 \\ 3 \bmod 4 = 3 & 7 \bmod 4 = 3 & 11 \bmod 4 = 3 \end{array}$$

Modular Math

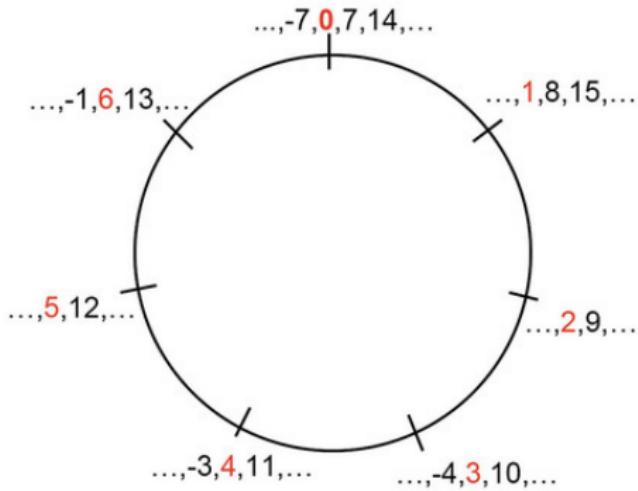


Figura 1: Modular Clock

Modular Math

Modular equivalence: $x \equiv y \pmod{n}$

$$1 \equiv 5 \pmod{4}$$

$$x^2 \equiv y \pmod{4}$$

$$(m^e)^d \equiv m \pmod{n}$$