2019-10-09

Cálculo de inversos multiplicativos módulo n

Def: neutro multiplicativo: dado un elemento $\hat{e} \in \mathbb{Z}_n$, este se llama neutro multiplicativo si cumple:

$$a \cdot \hat{e} = a$$ para todo $a \in \mathbb{Z}_n$

! Siempre en $\mathbb{Z}_n$, el neutro es 1.

Observación = existe un "neutro aditivo que es el 0.

Por ejemplo, redefinimos ü:

! Filosofía

$a \ddot{u} b \to a^b$

$2 \ddot{u} 3 \to 2^3 \to 8$

$a \ddot{u} b \to a^1 \to a$

en neutro es 1

$a \Delta b \to b - a$

$2 \Delta 3 \to 3 - 2 \to 1$

$a \Delta \hat{e} \to \hat{e} - a \to a$

$a \Diamond b \to a^2 - 2ab + b^2$

$a \Diamond b \equiv a^2 - 2a\hat{e} + \hat{e}^2 \equiv a$

el Δ & ü son operaciones inventadas

Def de "inverso multiplicativo", Un elemento $b \in \mathbb{Z}_n$, se llama inverso multiplicativo de $a \in \mathbb{Z}$ si se cumple:

$$a \cdot b \equiv_n \underbrace{1}_{\text{el neutro multiplicativo}}$$

! En este caso a & b son inversos multiplicativos entre sí.

! Notación: $b \equiv a^{-1}$

Observación:

$$2x \equiv 7 \pmod{11} \equiv$$

$$2x \equiv 7 + 11 \equiv 18$$

$$\hookrightarrow 9 \hookleftarrow$$

$E(x) = x + d$ $\qquad x = 9$

$E(x) = m \cdot x + d$

Ej: Encuentre el inverso de a módulo n.

a) $n = 5$ & $a = 2$

$a^{-1} \equiv 3$ ya que:

$a \cdot a^{-1} = 2 \cdot 3 \equiv_5 1$

---

b) $n = 7$ & $a = 6$

$a^{-1} \equiv 6$ ya que:

$a \cdot a^{-1} = 6 \cdot 6 \equiv_7 1$

---

c) $n = 23$ & $a = 17$

$a^{-1} \equiv_{23} 19 \pmod{23}$

$a \cdot a^{-1} \equiv 17 \cdot 19 = 323 \equiv_{23} 1$

Un número va a tener inverso si son primos relativos.

---

[1] El 0 & el uno no son respuesta.

[1] A veces la inversa multiplicativa no existe.

- Si elijo mal "m" no puedo desencriptar.

[1] $6x = 5 \rightarrow x = \frac{5}{6}$

"pasas a dividir el 6"

$\frac{1}{6} 6x = 5 \cdot \frac{1}{6}$

$x = \frac{5}{6}$

"multiplicamos por el inverso multiplicativo de 6"