# Cálculo de inversos multiplicativos de módulo n

Dado $a \in \mathbb{Z}$, $n \geq 2$, buscamos un entero $a^{-1} \in \mathbb{Z}_n$ que satisface:

$$a \cdot a^{-1} \equiv_n 1$$

Consideremos nuevamente el ejemplo

$$a = 17 \quad \& \quad n = 23$$

$$a \cdot a^{-1} = q_1 \cdot n + 1$$

$$\underbrace{a}_{\text{conocido}} \cdot a^{-1} - q_1 \cdot \underbrace{n}_{\text{conocido}} = 1$$

en términos conocidos:

$$a^{-1} \equiv x \qquad q_1 \equiv y$$

$$\underbrace{a \cdot x - y n = 1}_{\text{identidad de Bézout.}}$$

① Primero calculamos $mcd(23, 17)$:

$$23 = 1 \cdot 17 + 6$$
$$17 = 2 \cdot 6 + 5$$
$$6 = 1 \cdot 5 + 1$$
$$5 = 5 \cdot 1 + 0$$
$$mcd(23, 17) = 1$$

coprimos

Observación: para que la inversa exista se tiene que trabajar con co-primos.

② Luego resolvemos Bézout:

$$\boxed{6 - 5 = 1}$$
$$17 - 2 \cdot 6 = 5$$
$$\boxed{6 - (17 - 2 \cdot 6) = 1}$$
$$\boxed{3 \cdot 6 - 17 = 1}$$
$$3(23 - 17) - 17 = 1$$
$$3 \cdot 23 - 4 \cdot 17 = 1$$

Entonces...

$$3 \cdot 23 - 4 \cdot 17 = 1$$

$\mathbb{Z}_{23}$

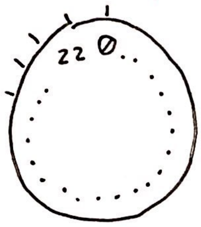
$$3 \cdot 23 - 4 \cdot 17 = 1$$

$\mathbb{Z}_{23}$

traducir todo a $mod_{23}$.

$$\cancel{3 \cdot 0}\;{}^{0} - 19 \cdot 17 = 1$$

$$19 \cdot 17 \equiv_{23} 1$$




En conclusión, el inverso multiplicativo de 17 en $\mathbb{Z}_{23}$ = 19.

---

<u>Ej</u>: $n = 28$ & $a = 5$

$mcd(28, 5)$

$28 = 5 \cdot 5 + 3$

$mcd(5, 3)$

$5 = 3 \cdot 1 + 2$

$mcd(3, 2)$

$3 = 2 \cdot 1 + 1$

$mcd(2, 1)$

$2 = 2 \cdot 1 + 0$

$3 - 2 \cdot 1 = 1$

$5 - 3 \cdot 1 = 2$ ; $28 - 5 \cdot 5 = 3$

$3 - (5 - 3) \cdot 1 = 1$

$3 - 5 + 3 = 1$

$2 \cdot 3 - 5 = 1$

$2(28 - 5 \cdot 5) - 5 = 1$

$2 \cdot 28 - 10 \cdot 5 - 5 = 1$

$2 \cdot 28 - 11 \cdot 5 = 1$

$\mathbb{Z}_{28}$

$$2 \cdot 28 - 11 \cdot 5 = 1$$

$$\mathbb{Z}_{28}$$

$$\cancel{2 \cdot 0}^{\,0} \quad 17 \cdot 5 \equiv_3 1$$

El inverso multiplicativo de 5 en $\mathbb{Z}_{28}$ es 17.

---

Vimos que en ambos casos, a & n son primos relativos:

$$mcd(n, a) = 1$$

Entonces podemos concluir que:

$\boxed{!}$ $a \in \mathbb{Z}_n$ tiene inverso módulo n, si y solo si, el máximo común divisor de a y n es 1.

---

Ej: Cifrado Cesar ponderado:

Def: Definimos un diccionario:

$$\begin{array}{cccccccc} A, & B, & C, & D \ldots, & X, & Y, & Z \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 3 & 23 & 24 & 25 \end{array}$$

mod 26 ya que estamos trabajando con 26 caracteres.

Función de encriptación:

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

Por ejemplo $K = 3$ & $d = 5$

$$
\begin{array}{c}
m = \text{A T T A C K} \\
\downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\
\boxed{\quad E(x) \quad} \\
5\ \ 10\ \ 10\ \ 5\ \ 11\ \ 9 \\
\downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow \\
c = \text{F K K F L J}
\end{array}
$$

Función de derencriptación:

$$D(x) = (x - d) \cdot K^{-1}$$