Logaritmo Discreto

Ronald Mas,
Angel Ramirez

26 de agosto de 2020

Contenido

Índices

Índice

Sea m raíz primitiva módulo n y $b \in \mathbb{N}$ con $MCD(b, n) = 1$. Entonces para exactamente uno de los valores $e \in \{0, 1, \cdots, \phi(n) - 1\}$ se tiene que $b \equiv m^e \, (mod \, n)$. Este único valor e módulo $\phi(n)$ es el índice de b en la base m módulo n, denotado por $ind_m(b)$.

Observaciones:

- Para el caso $n = p$ (número primo), el índice $ind_m(b)$ también es conocido como el **logaritmo discreto** de b en base m módulo p, es decir cumple propiedades similares a la función logaritmo que conocemos.
- El índice de b en la base m módulo n permite resolver ecuaciones diofánticas como lo veremos más adelante.

Ejemplo:

Si $n = 11$ entonces 2 es una raíz primitiva módulo 11 y

$$\begin{array}{lll} 2^1 \equiv 2\,(mod\,11) & , & 2^2 \equiv 4\,(mod\,11) \\ 2^3 \equiv 8\,(mod\,11) & , & 2^4 \equiv 5\,(mod\,11) \\ 2^5 \equiv 10\,(mod\,11) & , & 2^6 \equiv 9\,(mod\,11) \\ 2^7 \equiv 7\,(mod\,11) & , & 2^8 \equiv 3\,(mod\,11) \\ 2^9 \equiv 6\,(mod\,11) & , & 2^{10} \equiv 1\,(mod\,11). \end{array}$$

Por lo tanto,

$$\begin{array}{lllll} ind_2(1) = 0, & ind_2(2) = 1, & ind_2(3) = 8 & ind_2(4) = 2, & ind_2(5) = 4, \\ ind_2(6) = 9, & ind_2(7) = 7, & ind_2(8) = 3 & ind_2(9) = 6, & ind_2(10) = 5. \end{array}$$

Teorema

Si m una raíz primitiva módulo n entonces para todo $c, d \in \mathbb{Z}$ se cumple:

1) $ind_m(1) \equiv 0 \,(mod\, \phi(n))$.
2) $ind_m(cd) \equiv ind_m(c) + ind_m(d) \,(mod\, \phi(n))$.
3) *Para todo* $t \in \mathbb{N}$, $ind_m(c^t) \equiv t \cdot ind_m(c) \,(mod\, \phi(n))$.

Prueba:

1) Sea $ind_m(1) = w$ entonces $1 \equiv m^w \,(mod\, n)$. Como m es un raíz primitiva módulo n entonces $w \equiv 0 \,(mod\, \phi(n))$. Por tanto $ind_m(1) \equiv 0 \,(mod\, \phi(n))$.

Continuación de la prueba

2) Sean $x \equiv ind_m(cd), y \equiv ind_m(c)$ y $z \equiv ind_m(d)$. Como $cd \equiv m^x (mod\ n)$, $c \equiv m^y (mod\ n)$ y $d \equiv m^z (mod\ n)$ entonces

$$m^{y+z} \equiv cd \equiv m^x\ (mod\ n).$$

Por lo tanto

$$m^{y+z-x} \equiv 1\ (mod\ n),$$

y como m es una raíz primitiva módulo n se tiene que:

$$y + z - x \equiv 0\ (mod\ \phi(n)).$$

3) De la parte 2), como $c \equiv m^y\ (mod\ n)$ entonces

$$c^t \equiv m^{yt}\ (mod\ n).$$

Por lo tanto $ind_m(c^t) \equiv yt \equiv t \cdot ind_m(c)\ (mod\ \phi(n))$.

Ejemplo:

Resolver la ecuación diofántica:

$$3x^3 \equiv 7\,(mod\,11).$$

Al tomar el índice en base 2 a ambos lados se tiene:

$$ind_2(3x^3) \equiv ind_2(7)\,(mod\,10).$$

Luego

$$ind_2(3) + 3ind_2(x) \equiv 7\,(mod\,10),$$

como $ind_2(3) = 8$ entonces

$$ind_2(x) \equiv 3^{-1}(7-8) \equiv -7 \equiv 3\,(mod\,10).$$

Por lo tanto $x \equiv 2^3 \equiv 8(mod\,11)$.

Definición

Si $m, n \in \mathbb{N}$, $b \in \mathbb{Z}$, $MCD(b, n) = 1$ entonces b es llamado una m-ésima potencia residual módulo n si $x^m \equiv b(mod\ n)$ para algún $x \in \mathbb{Z}$ y x es la llamado una m-ésima raíz módulo n.

Observaciones:

- Para el caso $m = 2$ decimos que x es una ráiz cuadrada módulo n y b es una potencia cuadrática módulo n.
- Para el caso $m = 3$ decimos que x es una ráiz cúbica módulo n y b es una potencia cúbica módulo n y así sucesivamente.

Teorema

Sean $e, n \in \mathbb{N}$ tal que n tiene una raíz primitiva, sea $b \in \mathbb{Z}$ tal que $MCD(b, n) = 1$ y sea $g = MCD(e, \phi(n))$. Entonces la congruencia

$$x^e \equiv b (mod\ n) \tag{1}$$

es soluble (posee solución) si y sólo si $b^{\phi(n)/g} \equiv 1 (mod\ n)$.
Es más, si existen soluciones en (1), entonces existen exactamente g soluciones incongruentes x módulo n.

Prueba:

Sea a una raíz primitiva módulo n. Resolver la ecuación (1) es equivalente a resolver la ecuación

$$e \cdot ind_a(x) \equiv ind_a(b)\,(mod\ \phi(n)) \tag{2}$$

Continuación de la prueba

Esta última ecuación posee solución si y sólo si $g \mid ind_a(b)$. Si $g \mid ind_a(b)$ entonces existen exactamente g soluciones incongruentes módulo $\phi(n)$ tal que satisfacen la ecuación (2) y así se tendrá exactamente g enteros x incongruentes módulo n tal que se satisface la ecuación (1). Luego, $g \mid ind_a(b)$ si y sólo si

$$ind_a(b)\phi(n)/g \equiv 0 \,(mod\, \phi(n)),$$

que es equivalente a decir que

$$(a^{ind_a b()})^{\phi(n)/g} \equiv b^{\phi(n)/g} \equiv 1 \equiv a^0 \,(mod\, n).$$

Corolario

Si p es un número primo impar, $c, e \in \mathbb{N}$ y $b \in \mathbb{Z}$ con $MCD(p, b) = 1$ entonces $x^e \equiv b \,(mod\ p^c)$ si y sólo si

$$b^{p^{c-1}(p-1)/g} \equiv 1 \,(mod p^c),$$

donde $g \equiv MCD(e, p^{c-1}(p-1))$.
Es más, si éste posee una solución entonces tiene exactamente g soluciones.

Ejemplo 1 Supongamos que buscamos soluciones para

$$x^5 \equiv 5 \,(mod\ 27). \tag{3}$$

Se tiene que $g = MCD(e, \phi(p^c)) = MCD(5, 18) = 1$. Como $5^{18} \equiv 1 \,(mod\ 27)$, por el teorema anterior la ecuación (1) posee solución y que existe sólo una solución ya que $g = 1$.

Continua el ejemplo

Al aplicar el índice en base 2 módulo 27 a la ecuación (3), se tiene que:

$$5 \cdot ind_2(x) \equiv ind_2(5) \equiv 5\,(mod\,18),$$

luego $m = 2$ es un raíz primitiva módulo 3^3. Por lo tanto

$$ind_2(x) \equiv 1\,(mod\,18),$$

entonces se tiene dos opciones, o $ind_2(x) \equiv 1\,(mod\,27)$ o $ind_2(x) \equiv 19\,(mod\,27)$. Al evaluar, se tiene como única solución que $x \equiv 2(mod\,27)$ y que $2^{19} \equiv 2(mod\,27)$.

Ejemplo 2

Resolver la ecuación

$$x^3 \equiv 4 (mod\, 27).$$

Como $4^6 \equiv 19\,(mod\, 27)$ donde $\phi(27)/MCD(\phi(27), 3) = 18/3 = 6$ entonces por el teorema anterior no existe solución.