RAÍCES PRIMITIVAS.

Profesores del curso:

Ronald Mass [1]

Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

19 de agosto de 2020

Tabla de contenidos

Orden modular de un entero

Definición 1

Sea $m \in \mathbb{Z}$, $n \in \mathbb{N}$ y $mcd(m, n) = 1$. Entonces el **orden** *de m módulo n es el menor número $e \in \mathbb{N}$ tal que $m^e \equiv 1 \, (mod \, n)$, el cual es denotado por $e = ord_n(m)$.*

Ejemplos:

1. $$2^3 \equiv 1 \, (mod \, 7)$$

   pero $2^j \not\equiv 1 \, (mod \, 7)$ para $j = 1, 2$, entonces $ord_7(2) = 3$.
2. Por el pequeño teorema de Fermat $2^{10} \equiv 1 \, (mod \, 11)$ y además $2^d \not\equiv 1 \, (mod \, 11)$ para todo $d < 10$, luego $ord_{11}(2) = 10$.

Tabla de contenidos

Definición 2

Si $m \in \mathbb{Z}$, $n \in \mathbb{N}$ y:

$$ord_n(m) = \phi(n),$$

entonces m es llamado una **raíz primitiva** *módulo n.*

Ejemplos:

1. 2 es una raíz primitiva módulo 11 pues $ord_{11}(2) = 10 = \phi(11)$.
2. $2962 = 2 \times 1481$ donde 1481 es primo, entonces $\phi(2962) = 1480$ y además $ord_{2962}(3) = 1480 = \phi(2962)$, entonces 3 es raíz primitiva de 2962.
3. 35 no tiene raíz primitiva.

Proposición 1

Si $m \in \mathbb{Z}$, $d, n \in \mathbb{N}$ tal que $mcd(m, n) = 1$, entonces $m^d \equiv 1\,(mod\ n)$ si y sólo si $ord_n(m)|d$.

Demostración:

- ($\Leftarrow$) Si $ord_n(m)|d$ entonces existe $k \in \mathbb{N}$ tal que $d = k\, ord_n(m)$. Luego:

$$m^d = m^{k\, ord_n(m)} = (m^{ord_n(m)})^k \equiv 1(mod\ n).$$

- ($\Rightarrow$) Si $m^d \equiv 1(mod\ n)$ entonces $d \geq ord_n(m)$. Luego, existen únicos enteros q, r tal que $d = q\, ord_n(m) + r$ donde $0 \geq r < ord_n(m)$. Luego:

$$1 \equiv_n m^d \equiv_n m^{q\, ord_n(m)+r} \equiv_n (m^{ord_n(m)})qm^r \equiv m^r\,(mod\ n)$$

de donde por la minimalidad del orden, se tiene que $r = 0$. Es decir, $ord_n(m)|d$.

Corolario 1

Si $mcd(m, n) = 1$, *donde* $m \in \mathbb{Z}$ *y* $n \in \mathbb{N}$, *entonces:*

$$ord_n(m)|\phi(n).$$

Demostración:

Como $mcd(m, n) = 1$, el teorema de Euler establece que $m^{\phi(n)} \equiv 1(mod\, n)$, y así por la Proposición 1, se tiene que $ord_n(m)|\phi(n)$.

Ejemplo:

Por el Corolario 1 se tiene que todos los posibles órdenes son divisores de $\phi(n)$, esto permite reducir la búsqueda. Por ejemplo, para determinar el orden de 3 módulo 2962, sólo necesitamos buscar en los divisores de $\phi(2962) = 1480$, los cuales son: $1, 2, 4, 5, 8, 10, 20, 37, 40, 74, 148, 185, 296, 370, 740, 1480$. De donde concluimos que 3 es raíz primitiva módulo 2962, sin la necesidad de probar con todos los exponentes $1 \leq j \leq 1480$.

Corolario 2

Si $d, n \in \mathbb{N}$ *y* $m \in \mathbb{Z}$ *tal que* $mcd(m, n) = 1$, *entonces:*

$$ord_n(m^d) = \frac{ord_n(m)}{mcd(d, ord_n(m))}.$$

Demostración:
Ejercicio.

Corolario 3

Sean $e, n \in \mathbb{N}$ y $m \in \mathbb{Z}$ tal que $mcd(m, n) = 1$, entonces:

$$ord_n(m^e) = ord_n(m).$$

si y sólo si:

$$mcd(e, ord_n(m)) = 1.$$

Demostración:

Por el Corolario 2:

$$ord_n(m^e) = \frac{ord_n(m)}{mcd(e, ord_n(m))}$$

$$\Rightarrow ord_n(m) = \frac{ord_n(m)}{mcd(e, ord_n(m))} \Rightarrow mcd(e, ord_n(m)) = 1.$$

Corolario 4

Si m es una raíz primitiva módulo n, entonces m^e es una raíz primitiva módulo n si y sólo si $mcd(e, \phi(n)) = 1$.

Demostración:
Ejercicio.

Lemma 1

Si $m \in \mathbb{Z}$ y $n \in \mathbb{N}$ tal que $mcd(m, n) = 1$, entonces $m^i \equiv m^j \, (mod\ n)$ para enteros no negativos i, j si y sólo si $i \equiv j \, (mod\ ord_n(m))$.

Demostración:

- ($\Rightarrow$) Si $m^i \equiv m^j (mod\ n)$ para $0 \leq i \leq j \leq \phi(n)$, como $mcd(m, n) = 1$, por la ley de cancelación se tiene que $m^{j-i} \equiv 1 (mod\ n)$ y por la Proposición 1 se tiene que $ord_n(m) | (j - i)$, es decir: $i \equiv j (mod\ ord_n(m))$.
- ($\Leftarrow$) Si $i \equiv j (mod\ ord_n(m))$ para $0 \leq i \leq j$, entonces $j = i + q\, ord_n(m)$ donde $q \geq 0$. Por tanto:

$$m^j \equiv m^{i+q\, ord_n(m)} \equiv m^i (m^{ord_n(m)})^q \equiv m^i 1^q \equiv m^i (mod\ n)$$

Teorema 1 (Raíces primitivas y residuos reducidos)

Sean $m \in \mathbb{Z}$ y $n \in \mathbb{N}$ relativamente primo con m. Si m es una raíz primitiva módulo n, entonces $\{m^j\}_{j=1}^{\phi(n)}$ es un conjunto completo de residuos reducidos módulo n.

Demostración:

Ejercicio.

Ejemplo:

Sabemos que 2 es raíz primitiva módulo 11, luego:

$$\{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\}$$

es un sistema completo de residuos reducidos módulo 11.

Teorema 2 (Número de raíces primitivas)

Si $n \in \mathbb{N}$ tiene una raíz primitiva, entonces este tiene $\phi(\phi)$ raíces primitivas incongruentes.

Demostración:

Sea m una raíz primitiva módulo n. Por el Teorema 1, otra raíz primitiva debe ser de la forma m^e donde $1 \leq e \leq \phi(n)$. Por el Corolario 1, se sabe que: $ord_n(m) = ord_n(m^e)$ si y sólo si $mcd(e, \phi(n)) = 1$, y así son precisamente $\phi(\phi(n))$ de tales enteros e.

Ejemplo:

How many primitive roots are there modulo the prime 257?

Solution:

There are $\phi(\phi(257)) = \phi(256) = \phi(2^8) = 2^7 = 128$ primitive roots.

Ejemplo:

Calcule el orden de 3 módulo 301.

Resolución:

Note que $301 = 7 \times 43$. Si h_1 es el orden de 3 módulo 7 y h_2 es el orden de 3 módulo 43, entonces el orden de 3 módulo 301 será el mínimo común múltiplo de h_1 y h_2 (**Ejercicio: Demostrar esta afirmación**). Por el Teorema de Fermat: $3^6 \equiv 1(mod\, 7)$ Observe que 3^2 y 3^3 no son congruentes 1 módulo 7, por tanto $h_1 = 6$. También $3^{42} \equiv 1(mod\, 43)$, desde que el orden divide a 42, luego, o es igual a 42 o $42|p$ donde p es uno dels primos que divide a 42: 2, 3 o 7. Ahora, observe que $3^{21}, 3^14$ y 3^6 no son $1(mod\, 43)$. Así $h_2 = 42$. Entonces, el orden de 3 módulo 301 es $mcm(6, 42) = 42$.

Ejemplo:

Suponga que x es un entero que satisface $19^x \equiv 2(mod\, 29)$. Dado que 19 es una raíz primitiva de 29, ¿x es par o impar?.

Resolución:

Observe que si α es una raíz primitiva módulo un primo p, entonces una solución x a $\alpha^x \equiv b(mod\, p)$ será par si $b^{(p-1)/2} \equiv 1(mod\, p)$ e impar si $b^{(p-1)/2} \equiv -1(mod\, p)$. Ahora, calculamos:

$$\begin{aligned} 2^{(29-1)/2} &\equiv 2^{14}(mod\, 29) \\ &\equiv 2^8 \times 2^4 \times 2^2(mod\, 29) \\ &\equiv (256)(16)(4)(mod\, 29) \\ &\equiv (24)(16)(4)(mod\, 29) \\ &\equiv 1536(mod\, 29) \\ &\equiv 28(mod\, 29) \\ &\equiv -1(mod\, 29) \end{aligned}$$

por tanto, concluimos que x debe ser impar.

Example:

Suppose that $a, b, n \in \mathbb{N}$, the order of a modulo n es h, and the order of b modulo n is k. Prove that the order of ab modulo n divides hk.

Solution:

We have a theorem which states that, if the order of a modulo n is t, then $a^s \equiv 1 (mod\, n)$ if and only if $t|s$. So it is enough to show that $(ab)^{hk} \equiv 1 (mod\, n)$. Note that
$(ab)^{hk} = a^{hk} b^{hk} = (a^h)^k (b^k)^h \equiv 1^k 1^h = 1 (mod\, p)$.