

Conferencia 7 - Raíces Primitivas

December 15, 2024

Definición. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$, el menor entero positivo tal que $a^k \equiv 1 (n)$ se denomina **orden** de a módulo de n y se denota $\text{ord}_n a$

Note que $\text{ord}_n a \leq \varphi(n)$

Teorema. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$, y $\text{ord}_n a = e$ entonces $a^t \equiv 1 (n)$ si y solo si $e|t$

Demostración

Si $e|t$ entonces $t = eq$, además $a^e \equiv 1 (n)$, por definición de orden luego $(a^e)^q \equiv 1 (n)$ y, por tanto, $a^{eq} \equiv a^t \equiv 1 (n)$

En el otro sentido, asumamos que $t = eq + r$ donde si $r \neq 0$ entonces $0 < r < e$ entonces $a^t = a^{eq+r} = a^{eq}a^r$ pero como $a^t \equiv 1 (n)$ se tendría que $a^{eq} \equiv 1 (n)$ y $a^r \equiv 1 (n)$ y cómo $r < e$ esto sería una contradicción por la definición de orden luego $r = 0$ y $t = eq$ por lo que $e|t$

Corolario. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$ entonces $\text{ord}_n a | \varphi(n)$

Teorema. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$, y $\text{ord}_n a = e$ entonces $a^i \equiv a^j (n)$ si y solo si $i \equiv j (e)$

Demostración

Si $a^i \equiv a^j (n)$ entonces $a^{i-j} \equiv 1 (n)$ luego, por definición de orden, $e|i-j$ y, por tanto, $i \equiv j (e)$

En el otro sentido, como $i \equiv j (e)$ se tiene que $e|i-j$ luego, por definición de orden, $a^{i-j} \equiv 1 (n)$, entonces $a^{i-j}a^j \equiv a^j (n)$, por tanto $a^i \equiv a^j (n)$

Definición. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$, a es **raíz primitiva** módulo n si $\text{ord}_n a = \varphi(n)$

Teorema. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$ y $\text{ord}_n a = e$ entonces $\text{ord}_n a^k = \frac{e}{(e, k)}$

Demostración

Sea $m = \text{ord}_n a^k$ y $d = (e, k)$ entonces $k = dk_1$ y $e = de_1$ tal que $(k_1, e_1) = 1$ luego $a^e \equiv 1 (n)$ y $(a^k)^m \equiv (a^{dk_1})^m \equiv a^{dk_1 m} \equiv 1 (n)$ entonces $e|dk_1 m$ luego $e_1 d | dk_1 m$ por lo que $e_1 | k_1 m$ como $(e_1, k_1) = 1$ entonces $e_1 | m$ Por otra parte, $(a^k)^{e_1} \equiv a^{dk_1 e_1} \equiv (a^e)^{k_1} \equiv 1 (n)$ por lo que $m|e_1$ y como $m|e_1$ y $e_1|m$ entonces $m = e_1$ por tanto $m = e_1 = \frac{e}{(e, k)}$

Teorema. Sean $a, n \in \mathbb{Z}_+$, $(a, n) = 1$ y a raíz primitiva módulo n entonces $\{a, a^2, a^3, \dots, a^{\varphi(n)}\}$ es un $SRR(n)$

Demostración

Para todo a^i , $1 \leq i \leq \varphi(n)$, se tiene que $(a^i, n) = 1$

Supongamos que existen $i \neq j$ tales que $a^i \equiv a^j (n)$

pero también se tiene que $\text{ord}_n a = \varphi(n)$, pues es a raíz primitiva

y como $a^i \equiv a^j (n)$ entonces $i \equiv j (\varphi(n))$ luego $\varphi(n) | i - j$

pero como $i - j < \varphi(n)$ entonces $i - j = 0$ por lo que $i = j$

entonces $\{a, a^2, a^3, \dots, a^{\varphi(n)}\}$ es un $SRR(n)$

Teorema. Sea $n \in \mathbb{Z}_+$, si n tiene raíces primitivas entonces n tiene $\varphi(\varphi(n))$ raíces primitivas

Demostración

Si n tiene raíces primitivas, y sea a una de esas raíces

entonces $\{a, a^2, a^3, \dots, a^{\varphi(n)}\}$ es un $SRR(n)$

Supongamos que b es otra raíz primitiva de n , luego $(b, n) = 1$

por tanto existe un i entero, $1 \leq i \leq \varphi(n)$ tal que $b \equiv a^i (n)$

por lo que $\text{ord}_n b = \text{ord}_n a^i$

luego $\varphi(n) = \text{ord}_n b = \text{ord}_n a^i = \frac{\text{ord}_n a}{(\text{ord}_n a, i)} = \frac{\varphi(n)}{(\varphi(n), i)}$

entonces $(\varphi(n), i) = 1$

Por tanto, para toda raíz primitiva b de n existe i tal que $b \equiv a^i (n)$

pero como $(\varphi(n), i) = 1$, por consiguiente, hay $\varphi(\varphi(n))$ elementos en

$\{a, a^2, a^3, \dots, a^{\varphi(n)}\}$ que son primos relativos con $\varphi(n)$

por tanto, hay $\varphi(\varphi(n))$ raíces primitivas de n