Orden y Raíces Primitivas

Alan Reyes-Figueroa

Teoría de Números (Aula 17) 27.septiembre.2022

Definición

*Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, definimos el **orden** de $\bar{a}$, denotado $\operatorname{ord}(\bar{a})$ como el menor entero positivo $t > 0$ tal que $\bar{a}^t \equiv 1 \pmod{n}$.*

*Si $a, n \in \mathbb{Z}$, $(a, n) = 1$, definimos el **orden** de a módulo n, denotado por $\operatorname{ord}_n(a)$ como el orden de $\bar{a}$ en $(\mathbb{Z}/n\mathbb{Z})^*$.*

Definición

*Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, definimos el **orden** de $\bar{a}$, denotado $\text{ord}(\bar{a})$ como el menor entero positivo $t > 0$ tal que $\bar{a}^t \equiv 1 \pmod{n}$.*

*Si $a, n \in \mathbb{Z}$, $(a, n) = 1$, definimos el **orden** de a módulo n, denotado por $\text{ord}_n(a)$ como el orden de $\bar{a}$ en $(\mathbb{Z}/n\mathbb{Z})^*$.*

Obs! Por el Teorema de Euler-Fermat, sabemos que $\text{ord}_n(a) \leq \varphi(n)$, para todo $a \in \mathbb{Z}$, $(a, n) = 1$.

Orden y Raíces Primitivas

Definición

Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, definimos el ***orden*** *de $\bar{a}$, denotado $\mathrm{ord}(\bar{a})$ como el menor entero positivo $t > 0$ tal que $\bar{a}^t \equiv 1 \pmod{n}$.*

Si $a, n \in \mathbb{Z}$, $(a, n) = 1$, definimos el ***orden*** *de a módulo n, denotado por $\mathrm{ord}_n(a)$ como el orden de $\bar{a}$ en $(\mathbb{Z}/n\mathbb{Z})^*$.*

Obs! Por el Teorema de Euler-Fermat, sabemos que $\mathrm{ord}_n(a) \leq \varphi(n)$, para todo $a \in \mathbb{Z}$, $(a, n) = 1$.

Definición

Cuando $\mathrm{ord}_n\, a = \varphi(n)$, decimos que a es una ***raíz primitiva*** *módulo n.*

Definición

Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, definimos el ***orden*** *de $\bar{a}$, denotado $\text{ord}(\bar{a})$ como el menor entero positivo $t > 0$ tal que $\bar{a}^t \equiv 1 \pmod{n}$.*

Si $a, n \in \mathbb{Z}$, $(a, n) = 1$, definimos el ***orden*** *de a módulo n, denotado por $\text{ord}_n(a)$ como el orden de $\bar{a}$ en $(\mathbb{Z}/n\mathbb{Z})^*$.*

Obs! Por el Teorema de Euler-Fermat, sabemos que $\text{ord}_n(a) \leq \varphi(n)$, para todo $a \in \mathbb{Z}$, $(a, n) = 1$.

Definición

Cuando $\text{ord}_n\, a = \varphi(n)$, decimos que a es una ***raíz primitiva*** *módulo n.*

Ejemplo:
2 es raíz primitiva módulo 5, pues $2 \not\equiv 1 \pmod{5}$, $2^2 \equiv 4 \not\equiv 1 \pmod{5}$, $2^3 \equiv 3 \not\equiv 1 \pmod{5}$, y $2^4 \equiv 1 \pmod{5}$; y $\varphi(5) = 4$.

Ejemplo: ¿Cuáles son las raíces primitivas módulo 15?

Orden y Raíces Primitivas

Ejemplo: ¿Cuáles son las raíces primitivas módulo 15? El grupo de unidades módulo 15, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ tiene la estructura

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{14}$	$\overline{1}$	$\overline{7}$	$\overline{11}$	$\overline{13}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{13}$	$\overline{2}$	$\overline{14}$	$\overline{7}$	$\overline{11}$
$\overline{7}$	$\overline{7}$	$\overline{14}$	$\overline{13}$	$\overline{4}$	$\overline{11}$	$\overline{2}$	$\overline{1}$	$\overline{8}$
$\overline{8}$	$\overline{8}$	$\overline{1}$	$\overline{2}$	$\overline{11}$	$\overline{4}$	$\overline{13}$	$\overline{14}$	$\overline{7}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{14}$	$\overline{2}$	$\overline{13}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{7}$	$\overline{1}$	$\overline{14}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\overline{8}$	$\overline{7}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

Ejemplo: ¿Cuáles son las raíces primitivas módulo 15? El grupo de unidades módulo 15, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ tiene la estructura

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{14}$	$\bar{1}$	$\bar{7}$	$\bar{11}$	$\bar{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{13}$	$\bar{2}$	$\bar{14}$	$\bar{7}$	$\bar{11}$
$\bar{7}$	$\bar{7}$	$\bar{14}$	$\bar{13}$	$\bar{4}$	$\bar{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\bar{11}$	$\bar{4}$	$\bar{13}$	$\bar{14}$	$\bar{7}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{14}$	$\bar{2}$	$\bar{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{7}$	$\bar{1}$	$\bar{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{14}$	$\bar{14}$	$\bar{13}$	$\bar{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Observe que $1^1 \equiv 2^4 \equiv 4^2 \equiv 7^4 \equiv 8^4 \equiv 11^2 \equiv 13^4 \equiv 14^2 \equiv 1 \pmod{15}$.

Orden y Raíces Primitivas

Ejemplo: ¿Cuáles son las raíces primitivas módulo 15? El grupo de unidades módulo 15, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ tiene la estructura

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{14}$	$\bar{1}$	$\bar{7}$	$\bar{11}$	$\bar{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{13}$	$\bar{2}$	$\bar{14}$	$\bar{7}$	$\bar{11}$
$\bar{7}$	$\bar{7}$	$\bar{14}$	$\bar{13}$	$\bar{4}$	$\bar{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\bar{11}$	$\bar{4}$	$\bar{13}$	$\bar{14}$	$\bar{7}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{14}$	$\bar{2}$	$\bar{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{7}$	$\bar{1}$	$\bar{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{14}$	$\bar{14}$	$\bar{13}$	$\bar{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Observe que $1^1 \equiv 2^4 \equiv 4^2 \equiv 7^4 \equiv 8^4 \equiv 11^2 \equiv 13^4 \equiv 14^2 \equiv 1 \pmod{15}$.
Luego $\text{ord}(1) = 1$, $\text{ord}(4) = \text{ord}(11) = \text{ord}(14) = 2$, $\text{ord}(2) = \text{ord}(7) = \text{ord}(8) = \text{ord}(13) = 4$.

Ejemplo: ¿Cuáles son las raíces primitivas módulo 15? El grupo de unidades módulo 15, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ tiene la estructura

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\overline{14}$	$\bar{1}$	$\bar{7}$	$\overline{11}$	$\overline{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\overline{13}$	$\bar{2}$	$\overline{14}$	$\bar{7}$	$\overline{11}$
$\bar{7}$	$\bar{7}$	$\overline{14}$	$\overline{13}$	$\bar{4}$	$\overline{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\overline{11}$	$\bar{4}$	$\overline{13}$	$\overline{14}$	$\bar{7}$
$\overline{11}$	$\overline{11}$	$\bar{7}$	$\overline{14}$	$\bar{2}$	$\overline{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\bar{7}$	$\bar{1}$	$\overline{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\overline{14}$	$\overline{14}$	$\overline{13}$	$\overline{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Observe que $1^1 \equiv 2^4 \equiv 4^2 \equiv 7^4 \equiv 8^4 \equiv 11^2 \equiv 13^4 \equiv 14^2 \equiv 1 \pmod{15}$.
Luego $\operatorname{ord}(1) = 1$, $\operatorname{ord}(4) = \operatorname{ord}(11) = \operatorname{ord}(14) = 2$, $\operatorname{ord}(2) = \operatorname{ord}(7) = \operatorname{ord}(8) = \operatorname{ord}(13) = 4$. No hay raíces primitivas módulo 15.

Orden y Raíces Primitivas

Otra forma de verlo: En el grupo de unidades módulo 15:

a	a^1	a^2	a^3	a^4	$\pmod{15}$
1	1				
2	2	4	8	1	
4	4	1			
7	7	4	13	1	
8	8	4	2	1	
11	11	1			
13	13	4	7	1	
14	14	1			

Orden y Raíces Primitivas

Otra forma de verlo: En el grupo de unidades módulo 15:

a	a^1	a^2	a^3	a^4	$\pmod{15}$
1	1				
2	2	4	8	1	
4	4	1			
7	7	4	13	1	
8	8	4	2	1	
11	11	1			
13	13	4	7	1	
14	14	1			

Como todas las potencias alcanzan el 1 antes de llegar a la potencia $\varphi(15) = 8$, no hay raíces primitivas módulo 15.

Ejemplo: Módulo 14

a	a^1	a^2	a^3	a^4	a^5	a^6	$\pmod{14}$
1	1						
3	3	9	13	11	5	1	
5	5	11	13	9	3	1	
9	9	11	1				
11	11	9	1				
13	13	1					

Ejemplo: Módulo 14

a	a^1	a^2	a^3	a^4	a^5	a^6	$\pmod{14}$
1	1						
3	3	9	13	11	5	1	
5	5	11	13	9	3	1	
9	9	11	1				
11	11	9	1				
13	13	1					

Así, 3 y 5 son raíces primitivas módulo 14.

Ejemplo: Módulo 14

a	a^1	a^2	a^3	a^4	a^5	a^6	$\pmod{14}$
1	1						
3	3	9	13	11	5	1	
5	5	11	13	9	3	1	
9	9	11	1				
11	11	9	1				
13	13	1					

Así, 3 y 5 son raíces primitivas módulo 14.

Una definición alternativa para una raíz primitiva es la siguiente

Orden y Raíces Primitivas

Ejemplo: Módulo 14

a	a^1	a^2	a^3	a^4	a^5	a^6	$\pmod{14}$
1	1						
3	3	9	13	11	5	1	
5	5	11	13	9	3	1	
9	9	11	1				
11	11	9	1				
13	13	1					

Así, 3 y 5 son raíces primitivas módulo 14.

Una definición alternativa para una raíz primitiva es la siguiente

Definición

*Dados $a, n \in \mathbb{Z}$, $n > 1$ y $(a, n) = 1$, decimos que a es una **raíz primitiva** módulo n si $U(n)$ es cíclico, y a es un generador para el grupo $U(n)$.*

Proposición

$$a^t \equiv 1 \pmod{n} \quad \Longleftrightarrow \quad \mathrm{ord}_n(a) \mid t.$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Proposición

$a^t \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid t.$

Prueba: $(\Leftarrow)$ Sea $t = q\,\mathrm{ord}_n(a)$. Como $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$,

UNIVERSIDAD DEL VALLE DE GUATEMALA

Proposición

$a^t \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid t.$

Prueba: $(\Leftarrow)$ Sea $t = q\,\mathrm{ord}_n(a)$. Como $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$, entonces para todo $k \in \mathbb{N}$ vale

$$a^{k\,\mathrm{ord}_n(a)} \equiv 1 \pmod{n}.$$

Proposición

$a^t \equiv 1 \pmod{n} \iff \text{ord}_n(a) \mid t.$

Prueba: ($\Leftarrow$) Sea $t = q\,\text{ord}_n(a)$. Como $a^{\text{ord}_n(a)} \equiv 1 \pmod{n}$, entonces para todo $k \in \mathbb{N}$ vale

$$a^{k\,\text{ord}_n(a)} \equiv 1 \pmod{n}.$$

En particular, $a^t \equiv a^{q\,\text{ord}_n(a)} \equiv 1 \pmod{n}$.

Proposición

$a^t \equiv 1 \pmod{n} \iff \operatorname{ord}_n(a) \mid t.$

Prueba: $(\Leftarrow)$ Sea $t = q \operatorname{ord}_n(a)$. Como $a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n}$, entonces para todo $k \in \mathbb{N}$ vale

$$a^{k \operatorname{ord}_n(a)} \equiv 1 \pmod{n}.$$

En particular, $a^t \equiv a^{q \operatorname{ord}_n(a)} \equiv 1 \pmod{n}$.

$(\Rightarrow)$ Por otro lado, si $a^t \equiv 1 \pmod{n}$, por el Algoritmo de la División, existen enteros $q, r \in \mathbb{Z}$, $0 \leq r < \operatorname{ord}_n(a)$ tales que $t = q \operatorname{ord}_n(a) + r$.

Luego, $r = t - q \operatorname{ord}_n(a)$ y

$$a^r \equiv a^{t - q \operatorname{ord}_n(a)} \equiv a^t \cdot (a^{\operatorname{ord}_n(a)})^{-q} \equiv 1 \cdot (1)^{-q} \equiv 1 \pmod{n}.$$

Proposición

$a^t \equiv 1 \pmod{n} \quad \Longleftrightarrow \quad \mathrm{ord}_n(a) \mid t.$

<u>Prueba</u>: $(\Leftarrow)$ Sea $t = q\,\mathrm{ord}_n(a)$. Como $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$, entonces para todo $k \in \mathbb{N}$ vale

$$a^{k\,\mathrm{ord}_n(a)} \equiv 1 \pmod{n}.$$

En particular, $a^t \equiv a^{q\,\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$.

$(\Rightarrow)$ Por otro lado, si $a^t \equiv 1 \pmod{n}$, por el Algoritmo de la División, existen enteros $q, r \in \mathbb{Z}$, $0 \leq r < \mathrm{ord}_n(a)$ tales que $t = q\,\mathrm{ord}_n(a) + r$.

Luego, $r = t - q\,\mathrm{ord}_n(a)$ y

$$a^r \equiv a^{t-q\,\mathrm{ord}_n(a)} \equiv a^t \cdot (a^{\mathrm{ord}_n(a)})^{-q} \equiv 1 \cdot (1)^{-q} \equiv 1 \pmod{n}.$$

Por la minimalidad de $\mathrm{ord}_n(a)$, se tiene que $r = 0$, y portanto $t = q\,\mathrm{ord}_n(a)$

Proposición

$a^t \equiv 1 \pmod{n} \iff \operatorname{ord}_n(a) \mid t.$

Prueba: ($\Leftarrow$) Sea $t = q\operatorname{ord}_n(a)$. Como $a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n}$, entonces para todo $k \in \mathbb{N}$ vale

$$a^{k\operatorname{ord}_n(a)} \equiv 1 \pmod{n}.$$

En particular, $a^t \equiv a^{q\operatorname{ord}_n(a)} \equiv 1 \pmod{n}$.

($\Rightarrow$) Por otro lado, si $a^t \equiv 1 \pmod{n}$, por el Algoritmo de la División, existen enteros $q, r \in \mathbb{Z}$, $0 \leq r < \operatorname{ord}_n(a)$ tales que $t = q\operatorname{ord}_n(a) + r$.

Luego, $r = t - q\operatorname{ord}_n(a)$ y

$$a^r \equiv a^{t-q\operatorname{ord}_n(a)} \equiv a^t \cdot (a^{\operatorname{ord}_n(a)})^{-q} \equiv 1 \cdot (1)^{-q} \equiv 1 \pmod{n}.$$

Por la minimalidad de $\operatorname{ord}_n(a)$, se tiene que $r = 0$, y portanto $t = q\operatorname{ord}_n(a)$ $\operatorname{ord}_n(a) \mid t$. $\square$

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

Solución: Observe que $(a, a^n - 1) = 1$.

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

<u>Solución</u>: Observe que $(a, a^n - 1) = 1$. Por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(a^n - 1)} \equiv 1 \pmod{a^n - 1}.$$

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

Solución: Observe que $(a, a^n - 1) = 1$. Por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(a^n - 1)} \equiv 1 \pmod{a^n - 1}.$$

Por otro lado, n es el orden de a módulo $a^n - 1$,

Corolario

Para todo $a \in U(n)$*, vale* $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

Solución: Observe que $(a, a^n - 1) = 1$. Por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}.$$

Por otro lado, n es el orden de a módulo $a^n - 1$, ya que $a^n \equiv 1 \pmod{a^n - 1}$,

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

<u>Solución</u>: Observe que $(a, a^n - 1) = 1$. Por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}.$$

Por otro lado, n es el orden de a módulo $a^n - 1$, ya que $a^n \equiv 1 \pmod{a^n - 1}$, y si $0 < t < n$, entonces

$$0 < t < n \quad \Longrightarrow \quad 0 < a^t - 1 < a^n - 1 \quad \Longrightarrow \quad a^n - 1 \nmid a^t - 1.$$

Corolario

Para todo $a \in U(n)$, vale $\text{ord}_n(a) \mid \varphi(n)$. $\square$

Ejemplo: Mostrar que $n \mid \varphi(a^n - 1)$ para todo entero positivo $a > 1$.

Solución: Observe que $(a, a^n - 1) = 1$. Por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}.$$

Por otro lado, n es el orden de a módulo $a^n - 1$, ya que $a^n \equiv 1 \pmod{a^n - 1}$, y si $0 < t < n$, entonces

$$0 < t < n \quad \Longrightarrow \quad 0 < a^t - 1 < a^n - 1 \quad \Longrightarrow \quad a^n - 1 \nmid a^t - 1.$$

Por el corolario anterior, $n = \text{ord}_{a^n-1}(a) \mid \varphi(a^n - 1)$. $\square$

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Solución: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Orden y Raíces Primitivas

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Solución: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Sabemos que $2^n \equiv 1 \pmod{p}$.

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

<u>Solución</u>: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Sabemos que $2^n \equiv 1 \pmod{p}$. Además, por el Teorema de Euler-Fermat, tenemos que $2^{p-1} \equiv 1 \pmod{p}$.

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Solución: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Sabemos que $2^n \equiv 1 \pmod{p}$. Además, por el Teorema de Euler-Fermat, tenemos que $2^{p-1} \equiv 1 \pmod{p}$.

Portanto, $r \mid n$ y $r \mid p - 1$, lo que implica que $r \mid (n, p - 1)$.

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Solución: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Sabemos que $2^n \equiv 1 \pmod{p}$. Además, por el Teorema de Euler-Fermat, tenemos que $2^{p-1} \equiv 1 \pmod{p}$.

Portanto, $r \mid n$ y $r \mid p - 1$, lo que implica que $r \mid (n, p-1)$. Pero, $(n, p-1) = 1$, ya que p es el menor divisor primo de n, y así, los divisores primos de $p - 1$ son menores que los divisores primos de n.

Ejemplo: Mostrar que no existe un entero $n > 1$ tal que $n \mid 2^n - 1$.

Solución: Supongamos lo contario, y tome p el menor divisor primo de n, y $r = \text{ord}_p(2)$.

Sabemos que $2^n \equiv 1 \pmod{p}$. Además, por el Teorema de Euler-Fermat, tenemos que $2^{p-1} \equiv 1 \pmod{p}$.

Portanto, $r \mid n$ y $r \mid p-1$, lo que implica que $r \mid (n, p-1)$. Pero, $(n, p-1) = 1$, ya que p es el menor divisor primo de n, y así, los divisores primos de $p-1$ son menores que los divisores primos de n.

Esto muestra que $r = 1$, y portanto $2^1 \equiv 1 \pmod{p} \;\Rightarrow\; p \mid 1$, lo cual es una contradicción.

$\square$

Orden y Raíces Primitivas

Una otra caracterización de las raíces primitivas es la siguiente.

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ *es raíz primitiva módulo* n *si, y sólo si,* $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ es raíz primitiva módulo n si, y sólo si, $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

<u>Prueba</u>: Para todo $a \in \mathbb{Z}$ con $(a, n) = 1$, se tiene que $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} \subseteq U(n)$.

Orden y Raíces Primitivas

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ es raíz primitiva módulo n si, y sólo si, $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

Prueba: Para todo $a \in \mathbb{Z}$ con $(a, n) = 1$, se tiene que $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} \subseteq U(n)$. Observe que $\langle \bar{a} \rangle = \{1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\mathrm{ord}_n(a)-1}\}$ es un conjunto con $\mathrm{ord}_n(a)$ elementos.

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ es raíz primitiva módulo n si, y sólo si, $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

Prueba: Para todo $a \in \mathbb{Z}$ con $(a, n) = 1$, se tiene que $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} \subseteq U(n)$. Observe que $\langle \bar{a} \rangle = \{1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\text{ord}_n(a)-1}\}$ es un conjunto con $\text{ord}_n(a)$ elementos. Todas las otras potencias $\bar{a}^t$ corresponden a alguna de las potencias $\bar{a}^r$, con $0 \leq r < \text{ord}_n(a)$ el residuo de la división módulo $\text{ord}_n(a)$.

Orden y Raíces Primitivas

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ es raíz primitiva módulo n si, y sólo si, $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

<u>Prueba</u>: Para todo $a \in \mathbb{Z}$ con $(a, n) = 1$, se tiene que $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} \subseteq U(n)$. Observe que $\langle \bar{a} \rangle = \{1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\text{ord}_n(a)-1}\}$ es un conjunto con $\text{ord}_n(a)$ elementos. Todas las otras potencias $\bar{a}^t$ corresponden a alguna de las potencias $\bar{a}^r$, con $0 \leq r < \text{ord}_n(a)$ el residuo de la división módulo $\text{ord}_n(a)$.

Por otro lado, los elementos $1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\text{ord}_n(a)-1}$ son todos distintos, pues si $\bar{a}^i = \bar{a}^j$ con $0 \leq i < j < \text{ord}_n(a)$, entonces $a^{j-i} \equiv 1 \pmod{n}$, y $\bar{a}^{j-i} = \bar{1}$, lo cual contradice la definición de $\text{ord}_n(a)$ como la menor potencia de $\bar{a}$ que es 1.

Una otra caracterización de las raíces primitivas es la siguiente.

Teorema

El número $a \in \mathbb{Z}$ es raíz primitiva módulo n si, y sólo si, $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n)$.

<u>Prueba</u>: Para todo $a \in \mathbb{Z}$ con $(a, n) = 1$, se tiene que $\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} \subseteq U(n)$. Observe que $\langle \bar{a} \rangle = \{1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\mathrm{ord}_n(a)-1}\}$ es un conjunto con $\mathrm{ord}_n(a)$ elementos. Todas las otras potencias $\bar{a}^t$ corresponden a alguna de las potencias $\bar{a}^r$, con $0 \leq r < \mathrm{ord}_n(a)$ el residuo de la división módulo $\mathrm{ord}_n(a)$.

Por otro lado, los elementos $1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{\mathrm{ord}_n(a)-1}$ son todos distintos, pues si $\bar{a}^i = \bar{a}^j$ con $0 \leq i < j < \mathrm{ord}_n(a)$, entonces $a^{j-i} \equiv 1 \pmod{n}$, y $\bar{a}^{j-i} = \bar{1}$, lo cual contradice la definición de $\mathrm{ord}_n(a)$ como la menor potencia de $\bar{a}$ que es 1.

Así, $\langle \bar{a} \rangle = U(n)$ si, y sólo si, $(a, n) = 1$ y $\mathrm{ord}_n(a) = \varphi(n)$. Esto es, si y sólo si, a es una raíz primitiva módulo n. $\square$

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod{n}$ en $z \pmod{m}$ es sobrejectivo.

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod{n}$ en $z \pmod{m}$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle \bar{a} \rangle = (\mathbb{Z}/n\mathbb{Z})^*$.

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

<u>Prueba</u>: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod{n}$ en $z \pmod{m}$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle \bar{a} \rangle = (\mathbb{Z}/n\mathbb{Z})^*$. En particular, la imagen $f(\langle \bar{a} \rangle) = \{a^t \pmod{m} : \ t \in \mathbb{N}\}$ cubre a todo $(\mathbb{Z}/m\mathbb{Z})^*$, y tenemos que $\langle \bar{a} \rangle = (\mathbb{Z}/m\mathbb{Z})^*$

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f:(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod n$ en $z \pmod m$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle\bar{a}\rangle = (\mathbb{Z}/n\mathbb{Z})^*$. En particular, la imagen $f(\langle\bar{a}\rangle) = \{a^t \pmod m : t \in \mathbb{N}\}$ cubre a todo $(\mathbb{Z}/m\mathbb{Z})^*$, y tenemos que $\langle\bar{a}\rangle = (\mathbb{Z}/m\mathbb{Z})^*$
Esto muestra que a es raíz primitiva módulo m. $\square$

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod n$ en $z \pmod m$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle \bar{a} \rangle = (\mathbb{Z}/n\mathbb{Z})^*$. En particular, la imagen $f(\langle \bar{a} \rangle) = \{a^t \pmod m) : t \in \mathbb{N}\}$ cubre a todo $(\mathbb{Z}/m\mathbb{Z})^*$, y tenemos que $\langle \bar{a} \rangle = (\mathbb{Z}/m\mathbb{Z})^*$
Esto muestra que a es raíz primitiva módulo m. $\square$

Las raíces primitivas son importantes en varios aspectos de la teoría de números. Ya vimos que no todo módulo posee raíces primitivas.

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod{n}$ en $z \pmod{m}$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle \bar{a} \rangle = (\mathbb{Z}/n\mathbb{Z})^*$. En particular, la imagen $f(\langle \bar{a} \rangle) = \{a^t \pmod{m} : \ t \in \mathbb{N}\}$ cubre a todo $(\mathbb{Z}/m\mathbb{Z})^*$, y tenemos que $\langle \bar{a} \rangle = (\mathbb{Z}/m\mathbb{Z})^*$
Esto muestra que a es raíz primitiva módulo m. $\square$

Las raíces primitivas son importantes en varios aspectos de la teoría de números. Ya vimos que no todo módulo posee raíces primitivas. Nos gustaría una caracterización de aquellos módulos que poseen raíces primitivas.

Corolario

Si $m \mid n$ y a es raíz primitiva módulo n, entonces a es raíz parimitiva módulo m.

Prueba: El mapa natural $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ que lleva $x \pmod{n}$ en $z \pmod{m}$ es sobrejectivo.
Como a es raíz primitiva módulo n, entonces $\langle \bar{a} \rangle = (\mathbb{Z}/n\mathbb{Z})^*$. En particular, la imagen $f(\langle \bar{a} \rangle) = \{a^t \pmod{m} : t \in \mathbb{N}\}$ cubre a todo $(\mathbb{Z}/m\mathbb{Z})^*$, y tenemos que $\langle \bar{a} \rangle = (\mathbb{Z}/m\mathbb{Z})^*$
Esto muestra que a es raíz primitiva módulo m. $\square$

Las raíces primitivas son importantes en varios aspectos de la teoría de números. Ya vimos que no todo módulo posee raíces primitivas. Nos gustaría una caracterización de aquellos módulos que poseen raíces primitivas.

Teorema

Existe alguna raíz primitiva módulo n si, y sólo si, $n = 2$, $n = 4$, $n = p^k$ ó $n = 2p^k$, para algún primo impar p.

La prueba de este teorema es extensa y requerirá varios pasos.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Orden y Raíces Primitivas

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Orden y Raíces Primitivas

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r + 1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r + 1) + 1 \pmod 8$.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r + 1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r + 1) + 1 \pmod 8$.
Pero $r(r + 1)$ es par,

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

<u>Prueba</u>: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r+1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r+1) + 1 \pmod 8$.
Pero $r(r+1)$ es par, de modo que $4r(r+1) \equiv 0 \pmod 8$

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r+1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r+1) + 1 \pmod 8$.
Pero $r(r+1)$ es par, de modo que $4r(r+1) \equiv 0 \pmod 8$ y se tiene que $a^2 \equiv 1 \pmod 8$.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r+1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r+1) + 1 \pmod 8$.
Pero $r(r+1)$ es par, de modo que $4r(r+1) \equiv 0 \pmod 8$ y se tiene que $a^2 \equiv 1 \pmod 8$.

Así, todo elemento en $U(8)$ es de orden 2, y no hay elemento de orden $\varphi(8) = 4$.

La prueba de este teorema es extensa y requerirá varios pasos.

Proposición

Si $k \geq 3$, entonces no existe ninguna raíz primitiva módulo 2^k.

Prueba: Por el coroloario anterior, basta probar que no existe raíz primitiva módulo 8 (esto mostraría que no hay raíces primitivas para ningún módulo de la forma 2^k, $k \geq 3$).

Esto se sigue del hecho que si $(a, 8) = 1$, entonces $a = 1, 3, 5, 7$. y $a \equiv 2r + 1 \pmod 8$, con $r \in \mathbb{N}$. Luego, $a^2 \equiv (2r+1)^2 \equiv 4r^2 + 4r + 1 \equiv 4r(r+1) + 1 \pmod 8$.
Pero $r(r+1)$ es par, de modo que $4r(r+1) \equiv 0 \pmod 8$ y se tiene que $a^2 \equiv 1 \pmod 8$.

Así, todo elemento en $U(8)$ es de orden 2, y no hay elemento de orden $\varphi(8) = 4$. Esto muestra que no hay raíces primitivas módulo 8, y en consecuencia, no existen raíces rimitivas módulo 2^k, $k \geq 3$. $\square$

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$

Proposición

Si $n = ab$*, con* $a \geq 3$*,* $b \geq 3$*, enteros tales que* $(a, b) = 1$*, entonces no existen raíces primitivas módulo* n*.*

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares.

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares. Si $(k, n) = 1$, entonces por Euler-Fermat

$$k^{\varphi(n)/2} \equiv (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a},$$

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares. Si $(k, n) = 1$, entonces por Euler-Fermat

$$\begin{aligned} k^{\varphi(n)/2} &\equiv (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a}, \\ k^{\varphi(n)/2} &\equiv (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares. Si $(k, n) = 1$, entonces por Euler-Fermat

$$\begin{aligned} k^{\varphi(n)/2} &\equiv (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a}, \\ k^{\varphi(n)/2} &\equiv (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

De ahí que $(a, b) = 1$ implica que $k^{\varphi(n)/2} \equiv 1 \pmod{n}$,

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares. Si $(k, n) = 1$, entonces por Euler-Fermat

$$\begin{aligned} k^{\varphi(n)/2} &\equiv (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a}, \\ k^{\varphi(n)/2} &\equiv (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

De ahí que $(a, b) = 1$ implica que $k^{\varphi(n)/2} \equiv 1 \pmod{n}$, y portanto $\text{ord}_n(k) \leq \frac{\varphi(n)}{2} < \varphi(n)$, para todo $(k, n) = 1$. $\square$

Proposición

Si $n = ab$, con $a \geq 3$, $b \geq 3$, enteros tales que $(a, b) = 1$, entonces no existen raíces primitivas módulo n.

Prueba: Como $\varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$, y $a, b \geq 3$ entonces $\varphi(a)$ y $\varphi(b)$ son pares. Si $(k, n) = 1$, entonces por Euler-Fermat

$$\begin{aligned} k^{\varphi(n)/2} &\equiv (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \pmod{a}, \\ k^{\varphi(n)/2} &\equiv (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \pmod{b}. \end{aligned}$$

De ahí que $(a, b) = 1$ implica que $k^{\varphi(n)/2} \equiv 1 \pmod{n}$, y portanto $\mathrm{ord}_n(k) \leq \frac{\varphi(n)}{2} < \varphi(n)$, para todo $(k, n) = 1$. $\square$

Proposición

Si p es primo y $a \in \mathbb{Z}$ es una raíz primitiva módulo p, entonces a ó $a + p$ es una raíz primitiva módulo p^2.

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$.

Orden y Raíces Primitivas

<u>Prueba</u>: Por hipótesis, $\mathrm{ord}_p(a) = \mathrm{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$,

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\mathrm{ord}_p(a) = \mathrm{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \mathrm{ord}_{p^2}(a)$.

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$,

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\text{ord}_{p^2}(a+p) = p-1$ ó $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$.

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\mathrm{ord}_p(a) = \mathrm{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \mathrm{ord}_{p^2}(a)$.
Además, como $\mathrm{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\mathrm{ord}_{p^2}(a) = p-1$ ó $\mathrm{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\mathrm{ord}_{p^2}(a+p) = p-1$ ó $\mathrm{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta mostrar entonces que $\mathrm{ord}_{p^2}(a) \neq p-1$ ó $\mathrm{ord}_{p^2}(a+p) \neq p-1$.

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\text{ord}_{p^2}(a+p) = p-1$ ó $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta mostrar entonces que $\text{ord}_{p^2}(a) \neq p-1$ ó $\text{ord}_{p^2}(a+p) \neq p-1$.

Suponga que $\text{ord}_{p^2}(a) = p-1$.

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\text{ord}_{p^2}(a+p) = p-1$ ó $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta mostrar entonces que $\text{ord}_{p^2}(a) \neq p-1$ ó $\text{ord}_{p^2}(a+p) \neq p-1$.

Suponga que $\text{ord}_{p^2}(a) = p-1$. Entonces $a^{p-1} \equiv 1 \pmod{p^2}$ y

$$(a+p)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2}p + \binom{p-1}{2} a^{p-3}p^2 + \ldots + p^{p-1} \equiv a^{p-1} - pa^{p-2} \pmod{p^2}.$$

Orden y Raíces Primitivas

Prueba: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\text{ord}_{p^2}(a+p) = p-1$ ó $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta mostrar entonces que $\text{ord}_{p^2}(a) \neq p-1$ ó $\text{ord}_{p^2}(a+p) \neq p-1$.

Suponga que $\text{ord}_{p^2}(a) = p-1$. Entonces $a^{p-1} \equiv 1 \pmod{p^2}$ y

$$(a+p)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2}p + \binom{p-1}{2} a^{p-3}p^2 + \ldots + p^{p-1} \equiv a^{p-1} - pa^{p-2} \pmod{p^2}.$$

Portanto, $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, ya que p^2 no divide a pa^{p-2} (recordar que $(a,p) = 1$).

<u>Prueba</u>: Por hipótesis, $\text{ord}_p(a) = \text{ord}_p(a+p) = p-1$. Como $a^t \equiv 1 \pmod{p^2}$ implica que $a^t \equiv 1 \pmod{p}$, entonces $p-1 \mid \text{ord}_{p^2}(a)$.
Además, como $\text{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$, entonces $\text{ord}_{p^2}(a) = p-1$ ó $\text{ord}_{p^2}(a) = p(p-1) = \varphi(p^2)$.

De la misma forma, $\text{ord}_{p^2}(a+p) = p-1$ ó $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$. Basta mostrar entonces que $\text{ord}_{p^2}(a) \neq p-1$ ó $\text{ord}_{p^2}(a+p) \neq p-1$.

Suponga que $\text{ord}_{p^2}(a) = p-1$. Entonces $a^{p-1} \equiv 1 \pmod{p^2}$ y

$$(a+p)^{p-1} = a^{p-1} + \binom{p-1}{1} a^{p-2} p + \binom{p-1}{2} a^{p-3} p^2 + \ldots + p^{p-1} \equiv a^{p-1} - pa^{p-2} \pmod{p^2}.$$

Portanto, $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, ya que p^2 no divide a pa^{p-2} (recordar que $(a,p) = 1$). Esto muestra que $\text{ord}_{p^2}(a+p) = p(p-1) = \varphi(p^2)$, y que $a+p$ es raíz primitiva módulo p^2. $\square$

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2),

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

<u>Prueba</u>: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$.

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde $p \nmid b_k$, para todo $k \geq 1$.

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde $p \nmid b_k$, para todo $k \geq 1$.

De hecho, para $k \geq 1$ y p primo, se tiene que

$$a^{p^k(p-1)} \;=\; (1 + b_k p^k)^p \;=\; 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \ldots + \binom{p}{p} b_k^p p^{pk}$$

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde $p \nmid b_k$, para todo $k \geq 1$.

De hecho, para $k \geq 1$ y p primo, se tiene que

$$\begin{aligned} a^{p^k(p-1)} &= (1 + b_k p^k)^p = 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \ldots + \binom{p}{p} b_k^p p^{pk} \\ &= 1 + p^{k+1}(b_k + pt), \end{aligned}$$

para algún $t \in \mathbb{Z}$;

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde $p \nmid b_k$, para todo $k \geq 1$.

De hecho, para $k \geq 1$ y p primo, se tiene que

$$\begin{aligned} a^{p^k(p-1)} &= (1 + b_k p^k)^p = 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \ldots + \binom{p}{p} b_k^p p^{pk} \\ &= 1 + p^{k+1}(b_k + pt), \end{aligned}$$

para algún $t \in \mathbb{Z}$; y como $p \nmid b_k$, entonces también $p \nmid (b_k + pt) = b_{k+1}$.

Proposición

Si p es un primo impar y a es raíz primitiva módulo p^2, entonces a es raíz primitiva módulo p^k, para todo $k \in \mathbb{N}$.

Prueba: Como $a^{p-1} \equiv 1 \pmod{p}$, pero $a^{p-1} \not\equiv 1 \pmod{p^2}$, (ya que a es raíz primitiva módulo p^2), tenemos que $a^{p-1} = 1 + b_1 p$, donde $p \nmid b_1$. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde $p \nmid b_k$, para todo $k \geq 1$.

De hecho, para $k \geq 1$ y p primo, se tiene que

$$\begin{aligned} a^{p^k(p-1)} &= (1 + b_k p^k)^p = 1 + \binom{p}{1} b_k p^k + \binom{p}{2} b_k^2 p^{2k} + \ldots + \binom{p}{p} b_k^p p^{pk} \\ &= 1 + p^{k+1}(b_k + pt), \end{aligned}$$

para algún $t \in \mathbb{Z}$; y como $p \nmid b_k$, entonces también $p \nmid (b_k + pt) = b_{k+1}$.

Mostramos ahora por inducción que a es raíz primitiva módulo p^k, para todo $k \geq 2$.

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k.

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow$ $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$.

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow$ $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\mathrm{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow a^{\mathrm{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \mathrm{ord}_{p^k}(a) \mid \mathrm{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto, $\mathrm{ord}_{p^{k+1}}(a) = p^{k-1}(p-1)$ ó $\mathrm{ord}_{p^{k+1}}(a) = p^k(p-1) = \varphi(p^{k+1})$.

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto, $\text{ord}_{p^{k+1}}(a) = p^{k-1}(p-1)$ ó $\text{ord}_{p^{k+1}}(a) = p^k(p-1) = \varphi(p^{k+1})$. Sin embargo, el primer caso es imposible, ya que $a^{p^{k+1}} = 1 + b_k p^k$, con $p \nmid b_k$.

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto, $\text{ord}_{p^{k+1}}(a) = p^{k-1}(p-1)$ ó $\text{ord}_{p^{k+1}}(a) = p^k(p-1) = \varphi(p^{k+1})$. Sin embargo, el primer caso es imposible, ya que $a^{p^{k+1}} = 1 + b_k p^k$, con $p \nmid b_k$.

De ahí que $\text{ord}_{p^{k+1}}(a) = \varphi(p^{k+1})$, y a es una raíz primitiva módulo p^{k+1}, lo que conluye la inducción. $\square$

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow$ $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto, $\text{ord}_{p^{k+1}}(a) = p^{k-1}(p-1)$ ó $\text{ord}_{p^{k+1}}(a) = p^k(p-1) = \varphi(p^{k+1})$. Sin embargo, el primer caso es imposible, ya que $a^{p^{k+1}} = 1 + b_k p^k$, con $p \nmid b_k$.

De ahí que $\text{ord}_{p^{k+1}}(a) = \varphi(p^{k+1})$, y a es una raíz primitiva módulo p^{k+1}, lo que conluye la inducción. $\square$

Ejemplo: 2 es raíz primitiva módulo 5^k para todo $k \geq 1$.

Orden y Raíces Primitivas

Suponga que a es raíz primitiva módulo p^k. Como $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^{k+1}} \Rightarrow$ $a^{\text{ord}_{p^{k+1}}(a)} \equiv 1 \pmod{p^k}$. Luego

$$p^{k-1}(p-1) = \varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p^k(p-1).$$

Portanto, $\text{ord}_{p^{k+1}}(a) = p^{k-1}(p-1)$ ó $\text{ord}_{p^{k+1}}(a) = p^k(p-1) = \varphi(p^{k+1})$. Sin embargo, el primer caso es imposible, ya que $a^{p^{k+1}} = 1 + b_k p^k$, con $p \nmid b_k$.

De ahí que $\text{ord}_{p^{k+1}}(a) = \varphi(p^{k+1})$, y a es una raíz primitiva módulo p^{k+1}, lo que conluye la inducción. $\square$

Ejemplo: 2 es raíz primitiva módulo 5^k para todo $k \geq 1$. De hecho, 2 es raíz primitiva módulo 5 (Ejemplo 1 de hoy); y como $2^4 \equiv 16 \not\equiv 1 \pmod{5^2}$, entonces 2 es raíz primitiva módulo 25 también.
De la proposición anterior se conluye que 2 es raíz primitiva módulo 5^k, para todo $k \geq 1$.

Proposición

Si p es primo impar y $a \in \mathbb{Z}$ es un entero impar tal que a es raíz primitiva módulo p^k, entonces a es raíz primitiva módulo $2p^k$.
En particular, si a es raíz primitiva módulo p^k, entonces a ó $a + p^k$ es una raíz primitiva módulo $2p^k$.

Proposición

Si p es primo impar y $a \in \mathbb{Z}$ es un entero impar tal que a es raíz primitiva módulo p^k, entonces a es raíz primitiva módulo $2p^k$.
En particular, si a es raíz primitiva módulo p^k, entonces a ó $a + p^k$ es una raíz primitiva módulo $2p^k$.

Prueba: Al igual que en las pruebas anteriores, tenemos que

$$\varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{2p^k}(a) \mid \varphi(2p^k) = \varphi(p^k).$$

Proposición

Si p es primo impar y $a \in \mathbb{Z}$ es un entero impar tal que a es raíz primitiva módulo p^k, entonces a es raíz primitiva módulo $2p^k$.
En particular, si a es raíz primitiva módulo p^k, entonces a ó $a + p^k$ es una raíz primitiva módulo $2p^k$.

Prueba: Al igual que en las pruebas anteriores, tenemos que

$$\varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{2p^k}(a) \mid \varphi(2p^k) = \varphi(p^k).$$

Portanto, $\text{ord}_{2p^k}(a) = \varphi(2p^k)$, y a es una raíz primitiva módulo $2p^k$. $\square$

Proposición

Si p es primo impar y $a \in \mathbb{Z}$ es un entero impar tal que a es raíz primitiva módulo p^k, entonces a es raíz primitiva módulo $2p^k$.
En particular, si a es raíz primitiva módulo p^k, entonces a ó $a + p^k$ es una raíz primitiva módulo $2p^k$.

Prueba: Al igual que en las pruebas anteriores, tenemos que

$$\varphi(p^k) = \text{ord}_{p^k}(a) \mid \text{ord}_{2p^k}(a) \mid \varphi(2p^k) = \varphi(p^k).$$

Portanto, $\text{ord}_{2p^k}(a) = \varphi(2p^k)$, y a es una raíz primitiva módulo $2p^k$. $\square$

Para completar la prueba del teorema de caracterización de módulos con raíces primitivas, falta mostrar que si p es primo impar, entonces hay raíz primitiva módulo p.

Proposición

Si p es primo impar y $a \in \mathbb{Z}$ es un entero impar tal que a es raíz primitiva módulo p^k, entonces a es raíz primitiva módulo $2p^k$.
En particular, si a es raíz primitiva módulo p^k, entonces a ó $a + p^k$ es una raíz primitiva módulo $2p^k$.

<u>Prueba</u>: Al igual que en las pruebas anteriores, tenemos que

$$\varphi(p^k) = \operatorname{ord}_{p^k}(a) \mid \operatorname{ord}_{2p^k}(a) \mid \varphi(2p^k) = \varphi(p^k).$$

Portanto, $\operatorname{ord}_{2p^k}(a) = \varphi(2p^k)$, y a es una raíz primitiva módulo $2p^k$. $\square$

Para completar la prueba del teorema de caracterización de módulos con raíces primitivas, falta mostrar que si p es primo impar, entonces hay raíz primitiva módulo p.

Para ello, necesitamos aún dos lemas.

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

<u>Prueba</u>: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

Prueba: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Obtenemos una nueva lista reduciendo cada uno de estos n números a su fracción más simple $\frac{k}{d}$, en donde el numerador k y el denominador d son primos relativos.

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

<u>Prueba</u>: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Obtenemos una nueva lista reduciendo cada uno de estos n números a su fracción más simple $\frac{k}{d}$, en donde el numerador k y el denominador d son primos relativos.
Los denominadores de los números de la nueva lista serán todos divisores de n.

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

Prueba: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Obtenemos una nueva lista reduciendo cada uno de estos n números a su fracción más simple $\frac{k}{d}$, en donde el numerador k y el denominador d son primos relativos.
Los denominadores de los números de la nueva lista serán todos divisores de n.

Si $d|n$, hay exactamente $\varphi(d)$ de estas fracciones con d como denominador.

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

<u>Prueba</u>: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Obtenemos una nueva lista reduciendo cada uno de estos n números a su fracción más simple $\frac{k}{d}$, en donde el numerador k y el denominador d son primos relativos.
Los denominadores de los números de la nueva lista serán todos divisores de n.

Si $d|n$, hay exactamente $\varphi(d)$ de estas fracciones con d como denominador. Así, tenemos que los n números se reparten en grupos de $\varphi(d)$, para cada uno de los denominadores d.

Lema (Gauss)

$$\sum_{d|n} \varphi(d) = n.$$

<u>Prueba</u>: Consideramos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n}{n}.$$

Obtenemos una nueva lista reduciendo cada uno de estos n números a su fracción más simple $\frac{k}{d}$, en donde el numerador k y el denominador d son primos relativos.
Los denominadores de los números de la nueva lista serán todos divisores de n.

Si $d|n$, hay exactamente $\varphi(d)$ de estas fracciones con d como denominador. Así, tenemos que los n números se reparten en grupos de $\varphi(d)$, para cada uno de los denominadores d. Esto es

$$\sum_{d|n} \varphi(d) = n. \qquad \square$$

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

Prueba: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$.

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

Prueba: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo),

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\operatorname{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\operatorname{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

Por otro lado, si $\operatorname{ord}_p(a^k) = d$, entonces $(k, d) = 1$,

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

Prueba: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

Por otro lado, si $\text{ord}_p(a^k) = d$, entonces $(k, d) = 1$, pues si fuese $(k, d) = r > 1$, tendríamos que $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$,

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\operatorname{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\operatorname{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

Por otro lado, si $\operatorname{ord}_p(a^k) = d$, entonces $(k,d) = 1$, pues si fuese $(k,d) = r > 1$, tendríamos que $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, luego $\operatorname{ord}_p(a^k) \leq \frac{d}{r} < d$.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

Por otro lado, si $\text{ord}_p(a^k) = d$, entonces $(k,d) = 1$, pues si fuese $(k,d) = r > 1$, tendríamos que $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, luego $\text{ord}_p(a^k) \leq \frac{d}{r} < d$. De esta forma

$$\{b \in (\mathbb{Z}/p\mathbb{Z}) : \ \text{ord}_d(b) = d\} \subseteq \{\bar{a}^k.\ 0 \leq k < d,\ \ (k,d) = 1\},$$

Lema

Sea p un número primo, y d un divisor de $p-1$. Defina $N(d)$ como la cantidad de elementos $\bar{a} \in U(p)$, con orden $\text{ord}(a) = d$. Entonces, $N(d) \leq \varphi(d)$.

<u>Prueba</u>: Podemos suponer que $N(d) > 0$, de modo que, existe $a \in U(p)$ tal que $\text{ord}_p(a) = d$. Luego, $a^d \equiv 1 \pmod{p}$, y para $0 \leq k < d$, las clases a^k son todas distintas módulo p.

Como $\bar{a}^d = \bar{1}$ y la ecuación $\bar{x}^d - 1$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$, (recordemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), entonces sus raíces son exactamente $\bar{a}^k$, con $0 \leq k < d$.

Por otro lado, si $\text{ord}_p(a^k) = d$, entonces $(k,d) = 1$, pues si fuese $(k,d) = r > 1$, tendríamos que $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1 \pmod{p}$, luego $\text{ord}_p(a^k) \leq \frac{d}{r} < d$. De esta forma

$$\{b \in (\mathbb{Z}/p\mathbb{Z}) : \ \text{ord}_d(b) = d\} \subseteq \{\bar{a}^k . \ 0 \leq k < d, \ (k,d) = 1\},$$

y portanto $N(d) \leq \varphi(d)$ (de hecho, los dos conjuntos arriba son iguales, como quedará claro en la siguiente proposición). $\square$

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

<u>Prueba</u>: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$.

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

Prueba: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$. Por otro lado, tenemos por los lemas anteriores

$$p-1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p-1,$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

<u>Prueba</u>: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$. Por otro lado, tenemos por los lemas anteriores

$$p-1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p-1,$$

y en consecuencia $N(d) = \varphi(d)$, para todo $p \mid p-1$.

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

Prueba: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$. Por otro lado, tenemos por los lemas anteriores

$$p-1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p-1,$$

y en consecuencia $N(d) = \varphi(d)$, para todo $p \mid p-1$. En particular $N(p-1) = \varphi(p-1) > 0$, y existen elementos con orden $p-1$. Así, hay raíces primitivas módulo p. $\square$

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

Prueba: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$. Por otro lado, tenemos por los lemas anteriores

$$p-1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p-1,$$

y en consecuencia $N(d) = \varphi(d)$, para todo $p \mid p-1$. En particular $N(p-1) = \varphi(p-1) > 0$, y existen elementos con orden $p-1$. Así, hay raíces primitivas módulo p. $\square$

Corolario

Sea p primo. Para cada $d \mid p-1$, existen exactamente $\varphi(d)$ elementos en $U(p)$ con orden d. En particular, p posee exactamente $\varphi(p-1)$ raíces primitivas. $\square$

Proposición

Si p es primo, entonces existen raíces primitivas módulo p.

Prueba: Para cada $a \in U(n)$, se tiene que $\text{ord}_p(a) \mid p-1$, y portanto $p-1 = \sum_{d|p-1} N(d)$. Por otro lado, tenemos por los lemas anteriores

$$p-1 = \sum_{d|p-1} N(d) \leq \sum_{d|p-1} \varphi(d) = p-1,$$

y en consecuencia $N(d) = \varphi(d)$, para todo $p \mid p-1$. En particular $N(p-1) = \varphi(p-1) > 0$, y existen elementos con orden $p-1$. Así, hay raíces primitivas módulo p. $\square$

Corolario

Sea p primo. Para cada $d \mid p-1$, existen exactamente $\varphi(d)$ elementos en $U(p)$ con orden d. En particular, p posee exactamente $\varphi(p-1)$ raíces primitivas. $\square$

Esto completa la prueba del teorema de caractarización.

Orden y Raíces Primitivas

Observaciones:

- El último corolario afirma que para $n = p$, primo, el número de raíces primitivas módulo p es $\varphi(\varphi(p))$.

Orden y Raíces Primitivas

Observaciones:

- El último corolario afirma que para $n = p$, primo, el número de raíces primitivas módulo p es $\varphi(\varphi(p))$.
- La afirmación anterior vale en general. Dado $n > 1$, el número de raíces primitivas módulo n, si hay, es $\varphi(\varphi(n))$.

Orden y Raíces Primitivas

Observaciones:

- El último corolario afirma que para $n = p$, primo, el número de raíces primitivas módulo p es $\varphi(\varphi(p))$.
- La afirmación anterior vale en general. Dado $n > 1$, el número de raíces primitivas módulo n, si hay, es $\varphi(\varphi(n))$.
- Como ya se observó, para existan raíces primitivas módulo n, es neceario que $U(n)$ sea cíclico.

Orden y Raíces Primitivas

Observaciones:

- El último corolario afirma que para $n = p$, primo, el número de raíces primitivas módulo p es $\varphi(\varphi(p))$.
- La afirmación anterior vale en general. Dado $n > 1$, el número de raíces primitivas módulo n, si hay, es $\varphi(\varphi(n))$.
- Como ya se observó, para existan raíces primitivas módulo n, es neceario que $U(n)$ sea cíclico. El Teorema de Caracterización de módulos que admiten raíz primitiva, es equivalente a determinar todos los valores de n para los cuales el grupo abeliano $U(n) = (\mathbb{Z}/n\mathbb{Z})^*$ es cíclico.

Orden y Raíces Primitivas

Observaciones:

- El último corolario afirma que para $n = p$, primo, el número de raíces primitivas módulo p es $\varphi(\varphi(p))$.
- La afirmación anterior vale en general. Dado $n > 1$, el número de raíces primitivas módulo n, si hay, es $\varphi(\varphi(n))$.
- Como ya se observó, para existan raíces primitivas módulo n, es neceario que $U(n)$ sea cíclico. El Teorema de Caracterización de módulos que admiten raíz primitiva, es equivalente a determinar todos los valores de n para los cuales el grupo abeliano $U(n) = (\mathbb{Z}/n\mathbb{Z})^*$ es cíclico.

  Del Teorema Fundamental de grupos abelianos finitos, si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, se puede mostrar que
  $$U(n) \cong U(p_1^{k_1}) \times U(p_2^{k_2}) \times \cdots \times U(p_r^{k_r}).$$

  Los factores $U(p_i^{k_i})$ se descomponen a su vez en factores cíclicos, y se puede mostrar que, $U(n) \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$ es cíclico si, y sólo si, $n = 1, 2, 4, p^k$ ó $2p^k$, con p primo impar, y $k > 0$. Esto fue mostrado primero por Gauss.

Orden y Raíces Primitivas

La importancia de las raíces primitivas en teoría de números se deriva de este hecho:

Orden y Raíces Primitivas

La importancia de las raíces primitivas en teoría de números se deriva de este hecho: Si *a* es una raíz aprimitiva módulo *n*, entonces

$$\langle a\rangle = \{a^k : \; k = 0, 1, \ldots, \varphi(n)\} = U(n).$$

Orden y Raíces Primitivas

La importancia de las raíces primitivas en teoría de números se deriva de este hecho: Si a es una raíz aprimitiva módulo n, entonces

$$\langle a \rangle = \{a^k : \ k = 0, 1, \ldots, \varphi(n)\} = U(n).$$

Es decir, a es una raíz primitiva módulo n, si para cada entero x con $(x, n) = 1$ existe un entero k para el cual $a^k \equiv x \pmod{n}$.

La importancia de las raíces primitivas en teoría de números se deriva de este hecho: Si a es una raíz aprimitiva módulo n, entonces

$$\langle a\rangle = \{a^k: \ k = 0, 1, \ldots, \varphi(n)\} = U(n).$$

Es decir, a es una raíz primitiva módulo n, si para cada entero x con $(x, n) = 1$ existe un entero k para el cual $a^k \equiv x \pmod{n}$.

Tal valor k se llama **índice** o **logaritmo discreto** de x en base a módulo n.

Orden y Raíces Primitivas

La importancia de las raíces primitivas en teoría de números se deriva de este hecho: Si a es una raíz aprimitiva módulo n, entonces

$$\langle a\rangle = \{a^k : \ k = 0, 1, \ldots, \varphi(n)\} = U(n).$$

Es decir, a es una raíz primitiva módulo n, si para cada entero x con $(x, n) = 1$ existe un entero k para el cual $a^k \equiv x \pmod{n}$.

Tal valor k se llama **índice** o **logaritmo discreto** de x en base a módulo n.

Como ya hemos visto, calcular potencias (aún cuando k es grande) módulo n es un problema directo, y se resuelve de forma rápida y simple. Sin embargo, el problema de encontrar el logaritmo discreto de x en base a módulo n es un problema difícil. Actualmente, muchas herramientas criptográfica basan su fortaleza en la dificultad de calcular el logaritmo discreto.