Teorema de la Raíz Primitiva

En base a apuntes de Mauricio Guillermo de 2018

MD2 Cenur Noreste, sede Tacuarembó, Udelar

Junio de 2026

1. Notación

- $\overline{x}$ representa la clase de equivalencia de x módulo n.
- $U(n)$ representa el grupo de clases invertibles módulo n.
- $o(\overline{x})$ representa el orden de la clase $\overline{x}$ en el grupo $U(n)$.
- $\text{mcd}(x, n)$ representa el máximo común divisor entre x y n.

2. Definiciones y Resultados Preliminares

Definición 2.1. Sea $n \in \mathbb{Z}^+$.

1. El **grupo multiplicativo** (o grupo de unidades) módulo n se define como:
$$U(n) := \{\overline{x} \in \mathbb{Z}_n \mid \overline{x} \text{ es invertible en } \mathbb{Z}_n\} = \{\overline{x} \in \mathbb{Z}_n \mid \text{mcd}(x, n) = 1\}.$$
2. Una **raíz primitiva** módulo n es un entero $g \in \{1, \ldots, n\}$ cuya clase genera el grupo $U(n)$:
$$\langle \overline{g} \rangle = U(n).$$

2.1. Propiedades Fundamentales

- Si p es un número primo, entonces todos los elementos no nulos son invertibles:
$$U(p) = \{\overline{1}, \ldots, \overline{p-1}\}.$$
- Como consecuencia, si p es primo, vale:
$$x \cdot y \equiv 0 \pmod{p} \Rightarrow x \equiv 0 \pmod{p} \quad \text{o} \quad y \equiv 0 \pmod{p}.$$
Esto no es válido si el módulo no es primo (por ejemplo, $2 \cdot 2 \equiv 0 \pmod 4$, pero $2 \not\equiv 0 \pmod 4$).
- $(U(n), \cdot, \overline{1})$ es un grupo finito cuyo orden viene dado por la función de Euler: $|U(n)| = \varphi(n)$.
- Si g es una raíz primitiva módulo n, entonces: $U(n) = \langle \overline{g} \rangle = \{\overline{g}^0, \overline{g}^1, \ldots, \overline{g}^{\varphi(n)-1}\}$.
- Toda raíz primitiva g módulo n define un isomorfismo Ψ_g entre el grupo aditivo $(\mathbb{Z}_{\varphi(n)}, +, \overline{0})$ y el grupo multiplicativo $(U(n), \cdot, \overline{1})$, dado por:
$$\Psi_g(m) := \overline{g}^m.$$

Lema 2.2 (Lema 4.1.7 de las notas del curso)**.** *En un grupo G, si $x, y \in G$ son elementos que conmutan: $xy = yx$, y sus órdenes son coprimos:* $\text{mcd}(o(x), o(y)) = 1$*, entonces:*
$$o(xy) = o(x)o(y).$$

3. Estructura General de la Prueba

El **Teorema de la Raíz Primitiva** establece las condiciones necesarias y suficientes sobre n para la existencia de generadores de $U(n)$.

Teorema 3.1 (Teorema 4.1.15 de las notas)**.** *Sea $n \in \mathbb{Z}^+$. Existe una raíz primitiva módulo n si y sólo si n cumple una de las siguientes condiciones:*

1. $n = 1, 2, 4$
2. $n = p^k$*, con p primo impar y* $k \in \mathbb{Z}^+$.
3. $n = 2p^k$*, con p primo impar y* $k \in \mathbb{Z}^+$.

3.1. Plan de Demostración (El Recíproco por Casos)

- **Casos $n = 2$ y $n = 4$:** Son inmediatos observando que $\overline{1}$ genera $U(2) = \{\overline{1}\}$ y $\overline{3}$ genera $U(4) = \{\overline{1}, \overline{3}\}$.
- **Caso $n = p$ (con p primo impar):** Buscamos un elemento g con $o(\overline{g}) = p - 1$. Descomponemos el orden en factores primos $p - 1 = \prod_{i=1}^{k} p_i^{d_i}$ y encontramos elementos con órdenes locales máximos $p_i^{d_i}$ para luego multiplicarlos usando el Lema 2.2.
- **Caso $n = p^k$ ($k > 1$):** Construimos la raíz a partir de la raíz primitiva g de módulo p. Si $g^{p-1} \not\equiv 1 \pmod{p^2}$, entonces g sirve para todo p^k. Si no, el elemento corregido $g + p$ será la raíz primitiva válida.
- **Caso $n = 2p^k$:** A partir de una raíz primitiva g módulo p^k, si g es impar, sirve directamente. Si g es par, la solución es el elemento impar $g + p^k$.

3.2. Existencia de una Raíz Primitiva Módulo p (p Primo Impar)

A diferencia de la aritmética usual, en aritmética modular un polinomio de grado m puede tener más de m raíces. Por ejemplo, la ecuación de grado uno $2x \equiv 0 \pmod 4$ tiene dos raíces en $\mathbb{Z}_4$ ($\overline{0}$ y $\overline{2}$). Sin embargo, si el módulo es un número primo, recuperamos la propiedad clásica.

Lema 3.2 (Lema 4.1.8 de las notas)**.** *Sea p* ***primo*** *y sea $f(x) = \sum_{i=0}^{m} a_i x^i$ un polinomio con coeficientes en $\mathbb{Z}$. Si el coeficiente principal cumple $a_m \not\equiv 0 \pmod p$, entonces la ecuación $f(x) \equiv 0 \pmod p$ tiene* ***a lo sumo*** *m soluciones en $\mathbb{Z}_p$.*

Demostración. Lo probamos por inducción en el grado m:

- **Base inductiva ($m = 0$):** $f(x) = a_0$ con $a_0 \not\equiv 0 \pmod p$. Al ser una constante no nula módulo p, tiene 0 raíces.
- **Paso inductivo:** Supongamos válido el resultado para polinomios de grado menor que m. Sea $f(x)$ de grado m con al menos m raíces distintas $z_1, \ldots, z_m$. Construimos el polinomio auxiliar

$$g(x) = a_m \prod_{i=1}^{m} (x - z_i),$$

que comparte grado y coeficiente principal con $f(x)$. Definimos $h(x) = f(x) - g(x)$, cuyo grado es estrictamente menor que m. Como $f(x) \equiv 0 \pmod p$ y $g(x) \equiv 0 \pmod p$ comparten las m raíces, $h(x) \equiv 0 \pmod p$ también debe admitirlas. Por hipótesis inductiva, la única forma de que un polinomio de grado menor que m tenga m raíces es que sea el polinomio nulo módulo p (todos sus coeficientes son múltiplos de p). Por lo tanto, $f(x) \equiv g(x) \pmod p$. Como p es primo, la condición $a_m \prod_{i=1}^{m}(x - z_i) \equiv 0 \pmod p$ exige que obligatoriamente alguna de las componentes $(x - z_i) \equiv 0 \pmod p$. Así, las únicas raíces son exactamente $z_1, \ldots, z_m$.

□

Lema 3.3 (Lema 4.1.9 de las notas)**.** *Sea p primo y d un divisor de $p-1$. Entonces la ecuación $x^d \equiv 1 \pmod{p}$ tiene **exactamente** d raíces distintas en $U(p)$.*

Demostración. Si $p-1 = de$, podemos utilizar la identidad algebraica para factorizar la diferencia de potencias:

$$x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1)$$

Llamemos n a la cantidad de soluciones de $x^d - 1 \equiv 0 \pmod{p}$ y m a las soluciones de la componente larga de grado $d(e-1)$. Por el **Pequeño Teorema de Fermat**, sabemos que $x^{p-1} - 1 \equiv 0 \pmod{p}$ tiene **exactamente** $p-1$ soluciones. Utilizando el Lema 3.2:

$$p - 1 \leq n + m \leq d + d(e-1) = de = p - 1$$

Para que se preserve la cadena de desigualdades, todos los términos intermedios deben ser igualdades, obligando a que $n = d$, como queríamos. □

Corolario 3.4. *Sean p y p_i primos tales que $p_i^{\alpha_i} \mid (p-1)$, con $\alpha_i \neq 0$. Entonces existe un entero g_i tal que su orden en $U(p)$ es exactamente $o(\overline{g}_i) = p_i^{\alpha_i}$.*

Demostración. Por el Lema 3.3, la ecuación $x^{p_i^{\alpha_i}} \equiv 1 \pmod{p}$ tiene exactamente $p_i^{\alpha_i}$ soluciones, mientras que $x^{p_i^{\alpha_i - 1}} \equiv 1 \pmod{p}$ tiene exactamente $p_i^{\alpha_i - 1}$ soluciones. Al haber estrictamente más soluciones en el primer conjunto, podemos elegir un elemento g_i que cumpla la primera ecuación pero no la segunda:

$$(1)\ \ g_i^{p_i^{\alpha_i}} \equiv 1 \pmod{p}, \quad (2)\ \ g_i^{p_i^{\alpha_i - 1}} \not\equiv 1 \pmod{p}.$$

Por la condición (1), el orden de nuestro elemento debe dividir a la potencia: $o(\overline{g}_i) = p_i^{\beta_i}$ con $\beta_i \leq \alpha_i$. Por la condición (2), el exponente no puede ser menor o igual a $\alpha_i - 1$. Por descarte, concluimos que $o(\overline{g}_i) = p_i^{\alpha_i}$. □

Observación 3.5. Multiplicando los elementos correspondientes a cada factor primo de $p-1$ mediante el Lema 2.2, queda demostrada la existencia de la raíz primitiva módulo p.

3.3. Construcción de una Raíz Primitiva Módulo p^k $(k > 1)$

En esta sección veremos que si p es primo impar, y g es una raíz primitiva módulo p, entonces g o $g+p$ son una raíz primitiva módulo p^k, para todo $k \geq 1$. Notar que la existencia de una raíz primitiva módulo p está garantizada por el resultado de la sección anterior.

Lema 3.6. *Sea p primo impar y sea $g \in \mathbb{Z}$ una raíz primitiva módulo p. Supongamos que se cumple que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Entonces, se cumple:*

$$g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}, \quad \forall\ k \in \mathbb{Z}^+,\ k \geq 1.$$

Demostración. Procedemos por inducción sobre el exponente k:

- **Base inductiva ($k = 1$):** Se cumple de manera directa por la hipótesis del enunciado, ya que $\varphi(p) = p - 1$.

- **Paso inductivo:** Supongamos que se cumple para k. Por el **Teorema de Euler** clásico, sabemos que $g^{\varphi(p^k)} \equiv 1 \pmod{p^k}$. Es decir:

$$g^{\varphi(p^k)} = 1 + m \cdot p^k, \quad \text{para algún } m \in \mathbb{Z}.$$

Como p es primo, se cumple:

$$\varphi(p^{k+1}) = p^{k+1} - p^k = p\left(p^k - p^{k-1}\right) = p \cdot \varphi(p^k).$$

Esto permite escribir:

$$g^{\varphi(p^{k+1})} = g^{p\varphi(p^k)} = (g^{\varphi(p^k)})^p = (1 + m \cdot p^k)^p.$$

Aplicando el binomio de Newton:

$$(1 + m \cdot p^k)^p = 1 + p(m \cdot p^k) + \sum_{i=2}^{p} \binom{p}{i} m^i p^{ki} = 1 + m \cdot p^{k+1} + \sum_{i=2}^{p} \binom{p}{i} m^i p^{ki}.$$

Todos los sumandos de la sumatoria para $i \geq 2$ contienen factores de potencia lo suficientemente altos como para ser múltiplos de p^{k+2} (puesto que para $i = p$, $kp \geq 3k \geq k + 2$). Por lo tanto, reduciendo módulo p^{k+2}:

$$g^{\varphi(p^{k+1})} \equiv 1 + m \cdot p^{k+1} \pmod{p^{k+2}}.$$

Finalmente, gracias a nuestra hipótesis de inducción ($g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$), tenemos la certeza de que $p \nmid m$. Esto implica:

$$m \cdot p^{k+1} \not\equiv 0 \pmod{p^{k+2}}.$$

Por lo tanto:

$$g^{\varphi(p^{k+1})} \equiv 1 + m \cdot p^{k+1} \not\equiv 1 \pmod{p^{k+2}}.$$

□

Teorema 3.7 (Lemas 4.1.11 y 4.1.12 de las notas)**.** *Sea p primo impar y sea g una raíz primitiva módulo p.*

1. *Si $g^{p-1} \not\equiv 1 \pmod{p^2}$, entonces g es raíz primitiva módulo p^k, para todo $k \in \mathbb{Z}^+$.*
2. *Si $g^{p-1} \equiv 1 \pmod{p^2}$, entonces $g + p$ es raíz primitiva módulo p^k, para todo $k \in \mathbb{Z}^+$.*

Demostración. **Caso 1:** Queremos probar que el orden de $\overline{g}$ en $U(p^k)$ es exactamente $\varphi(p^k)$. Lo hacemos por inducción en k.

El caso base $k = 1$ es inmediato. Para el paso inductivo, fijemos $k \geq 1$ y supongamos que la propiedad se cumple para este k. Definamos $m := o(\overline{g})$, el orden de $\overline{g}$ en $U(p^{k+1})$. Como $g^m \equiv 1 \pmod{p^{k+1}}$, entonces $g^m \equiv 1 \pmod{p^k}$. Por hipótesis de inducción, esto nos fuerza a que $\varphi(p^k) \mid m$. Por otra parte, el **Teorema de Euler** nos asegura que $m \mid \varphi(p^{k+1})$. Entonces:

$$\varphi(p^k) \leq m \leq \varphi(p^{k+1}) = p \cdot \varphi(p^k).$$

Como $m \mid \varphi(p^{k+1})$, y no existen divisores de $\varphi(p^{k+1})$ en el intervalo $\left(\varphi(p^k), \varphi(p^{k+1})\right)$, solo restan dos alternativas para el valor de m:

1. $m = \varphi(p^k)$, lo cual implicaría que $g^{\varphi(p^k)} \equiv 1 \pmod{p^{k+1}}$, entrando en contradicción directa con lo demostrado en el Lema 3.6, o
2. $m = \varphi(p^{k+1})$, validando que $\overline{g}$ es un generador del grupo $U(p^{k+1})$.

Caso 2: La idea es ver que $g+p$ cumple las condiciones del Caso 1.

Vemos que $g+p \equiv g \pmod{p}$. Es decir que $\overline{g+p} = \overline{g}$ en $U(p)$, y entonces $g+p$ es raíz primitiva módulo p al igual que g. Expandiendo mediante binomio de Newton, se obtiene:

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)p \cdot g^{p-2} \pmod{p^2}.$$

Sustituyendo nuestra condición de Caso 2 ($g^{p-1} \equiv 1 \pmod{p^2}$):

$$(g+p)^{p-1} \equiv 1 + p^2 g^{p-2} - p \cdot g^{p-2} \equiv 1 - p \cdot g^{p-2} \pmod{p^2}.$$

Dado que $\overline{g} \in U(p)$, sabemos que $p \nmid g$. Esto implica que $p \cdot g^{p-2} \not\equiv 0 \pmod{p^2}$, demostrando que $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$. Es decir que $g+p$ cumple las hipótesis del Caso 1, con lo cual $g+p$ es raíz primitiva módulo p^k. □

3.4. Construcción de una Raíz Primitiva Módulo $2p^k$

En esta sección veremos que si p es primo impar, y g es raíz primitiva módulo p^k, entonces g o $g+p^k$ son raíz primitiva módulo $2p^k$. Notar que la existencia de raíz primitiva módulo p^k está garantizada por el resultado de la sección anterior.

Teorema 3.8 (Lema 4.1.13 de las notas)**.** *Sea p un primo impar, $k \in \mathbb{Z}^+$ y sea g una raíz primitiva módulo p^k. Entonces:*

1. *Si g es impar, g es raíz primitiva módulo $2p^k$.*
2. *Si g es par, $g+p^k$ es raíz primitiva módulo $2p^k$.*

Demostración. Como las bases $\text{mcd}(2, p^k) = 1$ son coprimas, el **Teorema Chino del Resto** nos permite asegurar que para cualquier exponente de control m, la congruencia en el grupo extendido se parte de forma bicondicional:

$$g^m \equiv 1 \pmod{2p^k} \iff \begin{cases} g^m \equiv 1 \pmod{p^k} \\ g^m \equiv 1 \pmod{2} \end{cases}$$

Por las propiedades de la función multiplicativa de Euler, el tamaño de los grupos coincide:

$$\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k).$$

1. **Si g es impar:** La condición de frontera $g^m \equiv 1 \pmod{2}$ es una identidad trivial que siempre se cumple para cualquier m. Por lo tanto, resolver la ecuación en el módulo compuesto equivale únicamente a resolver $g^m \equiv 1 \pmod{p^k}$. Esto conserva intacto el orden original del elemento, logrando que $o(\overline{g}) = \varphi(p^k) = \varphi(2p^k)$.
2. **Si g es par:** Evaluamos el cambio de fase lineal $g+p^k$. Módulo p^k, se anula el término de traslación ($g+p^k \equiv g \pmod{p^k}$), reteniendo su naturaleza de raíz primitiva. Adicionalmente, la suma de un número par (g) y un número impar (p^k) da como resultado un número impar. Al caer nuevamente en las condiciones del caso (1), queda demostrado el enunciado.

□