Apuntes sobre el teorema de la raíz primitiva

Mauricio GUILLERMO

02.06.2018

Notación 0.1. *En este tema, adoptaremos las siguientes notaciones:*

- $[x]_n$ *es la clase de equivalencia de* x *módulo* n*.*
- $|x|_n$ *es el orden de* $[x]_n$ *(con* $[x]_n \in \mathbb{Z}_n^*$*).*

Recordamos algunas definiciones y resultados relacionados:

Definición 0.2. *Sea* $n \in \mathbb{N}$*,* $n \neq 0$*.*

1. *El* grupo multiplicativo *módulo* n *es* $\mathbb{Z}_n^* := \{h \in \mathbb{Z}_n \mid h \text{ es invertible en } \mathbb{Z}_n\}$[1].
2. *Una* raíz primitiva *módulo* n *es un elemento* $r \in \mathbb{Z}_n$ *que es un generador de* $\mathbb{Z}_n^*$*; esto es:* $\langle r \rangle = \mathbb{Z}_n^*$*. Dado un entero* $g \in \mathbb{Z}$*, diremos que es* raíz primitiva módulo n *si* $r := [g]_n \in \mathbb{Z}_n^*$ *lo es.*

- Los elementos invertibles de $\mathbb{Z}_n$ son las clases módulo n de los enteros coprimos con n. Esto es: $\mathbb{Z}_n^* = \{[x]_n \mid \gcd(x, n) = 1\}$.
- Si p es un primo, entonces $\mathbb{Z}_p^* = \{[1]_p, \ldots, [p-1]_p\}$. Como todos los elementos no nulos de $\mathbb{Z}_p$ son invertibles, entonces $(\mathbb{Z}_p, +, \cdot, [0]_p, [1]_p)$ es un cuerpo.
- Por lo anterior, si p es primo y $x \cdot y \equiv_p 0$, entonces $x \equiv_p 0$ o $y \equiv_p 0$. Esto no es cierto si el módulo no es primo: $2 \cdot 2 \equiv_4 0$, pero $2 \not\equiv_4 0$.
- $(\mathbb{Z}_n^*, \cdot, [1]_n)$ es un grupo. De ahí el llamarlo *grupo multiplicativo*: es un grupo con la multiplicación.
- El orden de $\mathbb{Z}_n^*$ es $|\mathbb{Z}_n^*| = \varphi(n)$, donde φ es la *función de Euler*.
- Si g es una raíz primitiva módulo n, entonces $\mathbb{Z}_n^* = \langle g \rangle = \{g^0, \ldots, g^{\varphi(n)-1}\}$.
- Si g es raíz primitiva módulo n, entonces $\Psi_g(m) := g^m$ define un isomorfismo Ψ_g entre $(\mathbb{Z}_{\varphi(n)}, +, [0]_{\varphi(n)})$ y $(\mathbb{Z}_n^*, \cdot, [1]_n)$.
- Sea $(G, \cdot, e)$ un grupo, sean $a, b \in G$ de respectivos órdenes finitos $o(a)$ y $o(b)$. Si además a y b conmutan (esto es, si $a \cdot b = b \cdot a$) y $o(a)$ y $o(b)$ son coprimos; entonces $a \cdot b$ tiene orden $o(a)o(b)$.

[1] En las notas de Pereira, Qureshi & Rama se lo denota $U(n)$

1 Estructura general de la prueba

El teorema de la raíz primitiva establece una condición necesaria y suficiente para que un módulo admita raíz primitiva:

Teorema 1.1. *$\mathbb{Z}_n$ admite una raíz primitiva si y sólo si n satisface una de las siguientes:*

1. *$n = 2$ o $n = 4$.*
2. *Existen un primo impar p y un natural positivo k tales que $n = p^k$.*
3. *Existen un primo impar p y un natural positivo k tales que $n = 2.p^k$.*

Para demostrar este teorema procedemos siguiendo el siguiente plan:

1. El directo es el ejercicio 7c del práctico 8.
2. El recíproco es una prueba por casos:
   (a) Los casos $n = 2$ y $n = 4$ del item 1. son inmediatos. Basta con observar que:
      - $[1]_2$ es un generador de $\mathbb{Z}_2^* = \{[1]_2\}$.
      - $[3]_4$ es un generador de $\mathbb{Z}_4^* = \{[1]_4, [3]_4\}$.

   (b) El caso $n = p$ con p primo impar corresponde al item 2. con $k = 1$. Procedemos según el siguiente plan:
      - Observamos que $\varphi(p) = p - 1$, de modo que buscamos $g \in \mathbb{Z}$ de orden $|g|_n = p - 1$. Descomponemos $p - 1$ en factores primos, obteniendo: $p - 1 = \Pi_{i=1}^{k} p_i^{\alpha_i}$.
      - Mediante dos lemas técnicos, probamos que para cada i existe un elemento $g_i \in \mathbb{Z}$ de orden $|g_i|_n = p_i^{\alpha_i}$.
      - Como los órdenes de estos elementos son dos a dos coprimos y el grupo es conmutativo, $g := \Pi_{i=1}^{k} g_i$ tiene orden $|g|_n = \Pi_{i=1}^{k} p_i^{\alpha_i} = p - 1$, lo cual concluye la prueba.

   (c) El caso $n = p^k$ con $k \neq 1$. La prueba da explícitamente una raíz primitiva módulo p^k a partir de $g \in \mathbb{Z}$ raíz primitiva módulo p:
      i. Si $g^{p-1} \not\equiv_{p^2} 1$, entonces g es raíz primitiva módulo p^k para todo k natural positivo.
      ii. Si $g^{p-1} \equiv_{p^2} 1$, entonces $g+p$ es raíz primitiva módulo p y además –se prueba– satisface $(g + p)^{p-1} \not\equiv_{p^2} 1$. Entonces, aplicando el caso anterior, $g + p$ es raíz primitiva módulo p^k para todo k natural positivo.

   (d) Sea ahora $n = 2.p^k$ con p primo impar y k un natural positivo. La prueba da explícitamente una raíz primitiva módulo $2.p^k$ a partir de $g \in \mathbb{Z}$ raíz primitiva módulo p^k:
      i. Si g es impar, entonces g es raíz primitiva módulo $2.p^k$.
      ii. Si g es par, entonces $g+p^k$ es impar y es raíz primitiva módulo p^k, de modo que, aplicando el caso anterior, $g + p^k$ es raíz primitiva módulo $2.p^k$.

1.1 Existencia de una raíz primitiva módulo p con p primo impar.

Observación 1.2. Todo polinomio $f(x) = \Sigma_{i=0}^{m} a_i \cdot x^i$ de coeficientes enteros define un polinomio de coeficientes en $\mathbb{Z}_n$, que es $\widehat{f}(x) := \Sigma_{i=0}^{m}[a_i]_n \cdot x^i$. Como las operaciones de suma y producto en $\mathbb{Z}$ son compatibles con la relación de equivalencia $\equiv_n$, entonces para todo entero $x \in \mathbb{Z}$ tenemos:

$$\widehat{f}([x]_n) = \Sigma_{i=0}^{m}[a_i]_n \cdot [x]_n^i = [\Sigma_{i=0}^{m} a_i \cdot x^i]_n = [f(x)]_n$$

Recíprocamente, un polinomio con coeficientes en $\mathbb{Z}_n$ es de la forma $\widehat{f}$ para algún polinomio f a coeficientes enteros (de hecho, para infinitos f).

En $\mathbb{R}$ sabemos que un polinomio de grado m tiene a lo sumo m raíces reales. En $\mathbb{Z}_n$ esto puede no ser cierto: $\widehat{f}(x) = [2]_4 \cdot x$ es un polinomio de grado 1 en $\mathbb{Z}_4$, que admite raíces $[0]_4$ y $[2]_4$. A continuación veremos que esto no puede suceder si el módulo es primo:

Lema 1.3. *Sea p primo. Sea $f(x) = \Sigma_{i=0}^{m} a_i \cdot x^i$ un polinomio con coeficientes en $\mathbb{Z}$. Entonces, si $a_m \not\equiv_p 0$, $\widehat{f}$ tiene a lo sumo m raíces en $\mathbb{Z}_p$.*

Demostración: Observación: La tesis también dice que si $\widehat{f}$ admite más de m raíces, entonces es el polinomio nulo de $\mathbb{Z}_p$, es decir, todos sus coeficientes son nulos (en $\mathbb{Z}_p$).

Probamos el resultado por inducción en m:

- Si $m = 0$, entonces $f(x) = a_0$ con $a_0 \not\equiv_p 0$. Entonces, $\widehat{f}$ tiene cero raíces en $\mathbb{Z}_p$ porque es una constante no nula.

- Supongamos que el resultado es válido para los polinomios en de grado menor que m y probemos que es válido para los polinomios de grado m. Sea $f(x) = \Sigma_{i=0}^{m} a_i \cdot x^i$ con $a_m \not\equiv_p 0$.

  Si f tiene menos de m raíces, entonces el resultado está probado. Supongamos que tiene al menos m raíces distintas $z_1, \ldots, z_m$ y probemos que no tiene más.

  Sea $g(x) = a_m(x-z_1)\cdots(x-z_m) = a_m \cdot \Pi_{i=0}^{m}(x-z_i)$. Este polinomio tiene grado m y su coeficiente de grado m es a_m. Definimos $h(x) = f(x) - g(x)$, que es un polinomio de grado menor que m. Como $\widehat{g}$ admite al menos las m raíces en $\mathbb{Z}_p$ que admite $\widehat{f}$, entonces $\widehat{h}$ también. Por ser de grado menor que m, por la hipótesis de inducción y la observación, $\widehat{h}$ es el polinomio nulo (en $\mathbb{Z}_p$). Concluimos que $\widehat{f} = \widehat{g} + \widehat{h} = \widehat{g}$ (igualdad de polinomios en $\mathbb{Z}_p$).

  Como p es primo, $g(x) = a_m(x-z_1)\cdots(x-z_m) \equiv_p 0$ si y sólo si $x - z_i \equiv_p 0$ para algún i. En definitiva, las únicas raíces de $\widehat{f}$ en $\mathbb{Z}_p$ son las de $\widehat{g}$ (porque $\widehat{f} = \widehat{g}$), que son $z_1, \ldots, z_m$.

□

Lema 1.4. *Sean p primo, $d \mid (p-1)$ y $f(x) = x^d - 1$. Entonces $\widehat{f}$ tiene exactamente d raíces en $\mathbb{Z}_p$.*

Demostración: Sea $k \in \mathbb{Z}$ tal que $p - 1 = dk$. Mediante la fórmula

$$y^k - 1 = (y-1)(1 + \cdots + y^{k-1}) = (y-1)\Sigma_{i=0}^{k-1} y^i$$

substituyendo $y := x^d$ expresamos:

$$\underbrace{x^{p-1} - 1}_{g(x)} = \underbrace{(x^d - 1)}_{f(x)} \underbrace{\Sigma_{i=0}^{k-1} x^{di}}_{h(x)}$$

Sean F, G y H respectivamente los conjuntos de raíces de $\widehat{f}$, $\widehat{g}$ y $\widehat{h}$ (en $\mathbb{Z}_p$). Por ser p primo y $g(x) = f(x) \cdot h(x)$, entonces $G = F \cup H$.

Por el teorema de Euler, $\#G = p - 1$. Por el Lema 1.3, $\#F \leq d$ y $\#H \leq d(k-1)$. Entonces:

$$p - 1 = \#G \leq \#F + \#H \leq d + (k-1)d = dk = p - 1$$

Entonces, los $\leq$ son igualdades y debe ser $\#F = d$. □

Corolario 1.5. *Sean p y p_i primos tales que $p_i^{\alpha_i} \mid (p-1)$, con $\alpha_i \neq 0$. Entonces existe $g_i \in \mathbb{Z}$ tal que $|g_i|_p = p_i^{\alpha_i}$.*

Demostración: Sean R y S respectivamente los conjuntos de raíces de $x^{(p_i^{\alpha_i})} - 1$ y $x^{(p_i^{\alpha_i - 1})} - 1$ en $\mathbb{Z}_p$. Por el Lema 1.4, $\#R = p_i^{\alpha_i}$ y $\#S = p_i^{\alpha_i - 1}$. Entonces, $R \setminus S \neq \emptyset$ y concluimos que existe g_i tal que:

1. $g_i^{(p_i^{\alpha_i})} \equiv_p 1$
2. $g_i^{(p_i^{\alpha_i - 1})} \not\equiv_p 1$

Por 1., $|g_i|_p \mid p_i^{\alpha_i}$. Entonces $|g_i|_p = p_i^{\beta_i}$ para algún $\beta_i \leq \alpha_i$. Por 2. $\beta_i > \alpha_i - 1$ y entonces $|g_i|_p = p_i^{\alpha_i}$. □

Aplicando el plan del item (b) del Teorema 1.1, se resuelve este caso.

1.2 Construcción de una raíz primitiva módulo p^k con $k > 1$ a partir de una raíz primitiva módulo p; siendo p un primo impar.

Para hacer esta construcción, empezamos por enunciar y probar un lema técnico:

Lema 1.6. *Sea p primo impar y sea $g \in \mathbb{Z}$ una raíz primitiva módulo p. Supongamos que $g^{p-1} \not\equiv_{p^2} 1$. Entonces para todo $k \in \mathbb{N}$, $k > 1$, se tiene que $g^{\varphi(p^k)} \not\equiv_{p^{k+1}} 1$.*

Demostración: La prueba es por inducción en k.

Base inductiva: El caso $k = 1$ (base inductiva) es la hipótesis, ya que $\varphi(p) = p - 1$.

Paso inductivo: Supongamos que $g^{\varphi(p^k)} \not\equiv_{p^{k+1}} 1$. La función de Euler cumple que $\varphi(p^{k+1}) = p^{k+1} - p^k = p\ (p^k - p^{k-1}) = p\ \varphi(p^k)$. Entonces $g^{\varphi(p^{k+1})} = (g^{\varphi(p^k)})^p$.

Por el teorema de Euler, sabemos que $g^{\varphi(p^k)} \equiv_{p^k} 1$, de modo que $g^{\varphi(p^k)} = 1 + m.p^k$ para algún $m \in \mathbb{Z}$. Por la hipótesis de inducción, $1 + mp^k \not\equiv_{p^{k+1}} 1$, de donde deducimos que $p \nmid m$.

Aplicando la fórmula del binomio de Newton:

$$g^{\varphi(p^{k+1})} = (1 + mp^k)^p = \sum_{i=0}^{p} \binom{p}{i} 1^{p-i} (mp^k)^i = \sum_{i=0}^{p} \binom{p}{i} m^i p^{ki}$$

Donde $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$. En particular, $\binom{p}{0} = 1$ y $\binom{p}{1} = p$. Tenemos:

$$g^{\varphi(p^{k+1})} = \underbrace{1}_{i=0} + \underbrace{mp^{k+1}}_{i=1} + \underbrace{\sum_{i=2}^{p} \binom{p}{i} m^i p^{ki}}_{i \geq 2}$$

Probaremos que todos los sumandos con $i \geq 2$ son nulos módulo p^{k+2}:

- $\underline{2 \leq i < p}$: $ki \geq k.2 = k + k \geq k + 1$. Entonces, $p^{k+1} \mid p^{ki}$. Además, $p \mid \binom{p}{i}$ porque $0 < i < p$ (ejercicio 19 del práctico 3). Entonces, si $2 \leq i < p$, tenemos que $p^{k+2} \mid \binom{p}{i} m^i p^{ki}$.

- $\underline{\text{Para } i = p}$: $k.p \geq k.3 = k + k + k \geq k + 2$. Entonces $p^{k+2} \mid p^{k.p}$ y por lo tanto, $p^{k+2} \mid \binom{p}{p} m^p p^{k.p} = m^p p^{kp}$, que es el último sumando del desarrollo.

Concluimos que $g^{\varphi(p^{k+1})} \equiv_{p^{k+2}} 1 + mp^{k+1} \not\equiv_{p^{k+2}} 1$ porque vimos que $p \nmid m$. $\square$

Ahora, podemos probar el algoritmo de obtención de una raíz primitiva módulo p^k a partir de una raíz primitiva módulo p que enunciamos al principio:

Lema 1.7.

Sea p primo impar y sea g una raíz primitiva módulo p. Se tiene que:

1. Si $g^{p-1} \not\equiv_{p^2} 1$, entonces g es raíz primitiva módulo p^k, para todo $k \geq 1$.
2. Si $g^{p-1} \equiv_{p^2} 1$, entonces $g + p$ es raíz primitiva módulo p^k para todo $k \geq 1$.

Demostración:

1. Basta con probar $|g|_{p^k} = \varphi(p^k) = p^{k-1}(p-1)$ para todo $k \geq 1$ (recordar: $|g|_{p^k}$ es el orden de g como elemento de $\mathbb{Z}_{p^k}^*$).

   Base inductiva: Por hipótesis, esta afirmación es cierta para $k = 1$, ya que g es raíz primitiva módulo p.

   Paso inductivo: Supongamos que $|g|_{p^k} = \varphi(p^k)$ (hipótesis de inducción). Sea $m := |g|_{p^{k+1}}$. Basta con probar que $m = \varphi(p^{k+1})$.

   Por una parte, $g^m \equiv_{p^{k+1}} 1$, de donde, en particular, $g^m \equiv_{p^k} 1$. De aquí por la hipótesis de inducción, concluimos que $p^{k-1}(p-1) = \varphi(p^k) \Big| m$.

   Por otra parte, por el teorema de Euler $g^{\varphi(p^{k+1})} \equiv_{p^{k+1}} 1$. Entonces $m \Big| \varphi(p^{k+1}) = p^k(p-1)$.

   Deducimos que $p^{k-1}(p-1) \Big| m \Big| p^k(p-1)$. Existen dos posibilidades:

   - $m = p^{k-1}(p-1) = \varphi(p^k)$. Entonces, $g^{\varphi(p^k)} \equiv_{p^{k+1}} 1$. Esto contradice el lema 1.6.
   - $m = p^k(p-1) = \varphi(p^{k+1})$, que es lo que queríamos demostrar.

2. Consideramos $g+p \equiv_p g$ y, por lo tanto, es raíz primitiva módulo p. Basta entonces con probar que $(g+p)^{p-1} \not\equiv_{p^2} 1$ y aplicar el caso anterior a $g+p$. Para probar esto, aplicamos de nuevo la fórmula del binomio de Newton a $(g+p)^{p-1}$:

$$(g+p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} p^i g^{p-1-i} = \underbrace{g^{p-1}}_{i=0} + \underbrace{(p-1)pg^{p-2}}_{i=1} + \underbrace{+\sum_{i\geq 2}^{p-1} \binom{p-1}{i} p^i g^{p-1-i}}_{i\geq 2}$$

   Para todo $i \geq 2$ el término $\binom{p-1}{i} p^i g^{p-1-i}$ contiene un factor p^2, de modo que $\sum_{i\geq 2}^{p-1} \binom{p-1}{i} p^i g^{p-1-i} \equiv_{p^2} 0$.

   Deducimos que $(g+p)^{p-1} \equiv_{p^2} g^{p-1} + p(p-1)g^{p-2} = g^{p-1} + p^2 g^{p-2} - pg^{p-2} \equiv_{p^2} 1 - pg^{p-2}$ (puesto que $g^{p-1} \equiv_{p^2} 1$ y $p^2 g^{p-2} \equiv_{p^2} 0$). Como $p \not\Big| g$ (porque $[g]_p \in \mathbb{Z}_p^*$), entonces $(g+p)^{p-1} \not\equiv_{p^2} 1$.

□

1.3 construcción de una raíz primitiva módulo $2.p^k$ a partir de una raíz primitiva módulo p^k; siendo p un primo impar y k un entero positivo.

Lema 1.8. *Sea p un primo impar, k un entero positivo y sea $g \in \mathbb{Z}$ una raíz primitiva módulo p^k. Entonces:*

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

Demostración: Comenzamos por observar que, dado que 2 y p^k son coprimos, para todo entero positivo m, la ecuación $g^m \equiv_{2p^k} 1$ equivale al sistema de congruencias $\begin{cases} g^m \equiv_{p^k} & 1 \\ g^m \equiv_2 & 1 \end{cases}$. Por otra parte, $\varphi(2.p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$. Buscamos un elemento de $\mathbb{Z}_{2p^k}$ de orden $\varphi(p^k)$ pero en $2p^k$.

Sea g es raíz primitiva módulo p^k. Entonces se presentan dos casos:

1. Supongamos que g es impar. Entonces: $g^m \equiv_2 1$ para todo m entero positivo, de donde $g^m \equiv_{2p^k 1}$ si y sólo si $g^m \equiv_{p^k} 1$. concluimos entonces que $|g|_{2p^k} = |g|_{p^k} = \varphi(p^k) = \varphi(2p^k)$, lo que implica que g es raíz primitiva módulo $2p^k$.
2. Supongamos que g es par. En ese caso, $g + p^k \equiv_{p^k} g$, de modo que $g + p^k$ es una raíz primtiva módulo p^k. Además, $g + p^k$ es impar (puesto que p es impar), de modo que $g + p^k$ está en las condiciones del caso 1. y, por consecuencia, es raíz primitiva módulo $2p^k$.

□

Referencias

- *Notas De Matemática Discreta 2* de Mariana Pereira, Claudio Qureshi y Gustavo Rama, corregidas por Marcelo Lanzilotta (en el sitio EVA del curso).
- *The Primitive Root Theorem* Amin Witno. Universidad de Philadelphia. https://www.philadelphia.edu.jo/math/witno/notes/won5.pdf