Hoja 6: Raíces primitivas mód p

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Un resultado importante sobre los residuos módulo p es el siguiente.

> Para todo primo p existe un elemento $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ con $\operatorname{ord}(x) = p-1 = \phi(p) = \#(\mathbb{Z}/p\mathbb{Z})^\times$. En otras palabras,
> $$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, x, x^2, \ldots, x^{p-2}\}.$$
> Este x se llama una **raíz primitiva** mód p.

Ejemplo. Para $p = 13$ como una raíz primitiva funciona $x = [2]_{13}$:

$$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10,\ 2^{11} \equiv 7.$$

Ejemplo. Módulo 15 hay 8 elementos invertibles, y sus ordenes son los siguientes:

a	1	2	4	7	8	11	13	14
$\operatorname{ord}[a]_{15}$	1	4	2	4	4	2	4	2

Entonces, no hay elemento x tal que $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, x, x^2, \ldots, x^7\}$. Esto sucede porque 15 es compuesto.

En estas notas **no** vamos a probar la existencia de raíz primitiva. No es muy difícil, pero el argumento es un poco técnico y nos llevaría un poco lejos. Lo que pasa es que la prueba no es constructiva, y en general no existe una fórmula sencilla que para un primo p dé una raíz primitiva mód p. He aquí una pequeña lista de raíces primitivas módulo los primeros diez primos:

$$\begin{aligned}
p = 2&: 1,\\
p = 3&: 2,\\
p = 5&: 2, 3,\\
p = 7&: 3, 5,\\
p = 11&: 2, 6, 7, 8,\\
p = 13&: 2, 6, 7, 11,\\
p = 17&: 3, 5, 6, 7, 10, 11, 12, 14,\\
p = 19&: 2, 3, 10, 13, 14, 15,\\
p = 23&: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21,\\
p = 29&: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27,\\
&\ldots
\end{aligned}$$

En el resto de problemas, p es un número primo, y se puede asumir existencia de una raíz primitiva $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Problema 6.1. Demuestre que para cada $d \mid (p-1)$, en $(\mathbb{Z}/p\mathbb{Z})^\times$ hay exactamente $\phi(d)$ elementos de orden d.

Comentario. En particular, el problema anterior nos dice que hay $\phi(p-1)$ diferentes raíces primitivas mód p. El número $\phi(p-1)$ no es tan pequeño respecto a $p-1$, así que en práctica, para encontrar una raíz primitiva mód p, se puede escoger un número $1 < a < p-1$ al azar, y luego comprobar si $\operatorname{ord}[a]_p = p-1$.

Ejemplo. He aquí los ordenes de los residuos mód $p = 13$:

a:	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ord}[a]_{13}$:	1	12	3	6	4	12	12	4	3	6	12	2

Problema 6.2.

a) Demuestre que si x, x' son dos raíces primitivas mód p, entonces xx' no es una raíz primitiva mód p.

b) Demuestre que si x es una raíz primitiva mód p, entonces x^{-1} es también una raíz primitiva mód p.

Problema 6.3. Sea p un primo impar. Demuestre que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod{p}$ si y solamente si $p \equiv 1 \pmod{4}$.

Problema 6.4 (Euler)**.** Sea p un primo impar. Demuestre que para $p \nmid a$ se tiene la congruencia mód p

$$a^{\frac{p-1}{2}} \equiv \begin{cases} +1, & a \text{ es cuadrado mód } p, \\ -1, & a \text{ no es cuadrado mód } p. \end{cases}$$

Problema 6.5. Investigue para cuáles primos p existe $x \in \mathbb{Z}/p\mathbb{Z}$, tal que $x^3 = 1$ y $x \neq 1$.

Problema 6.6. Sea p un número primo.

a) Si $p \equiv 1 \pmod{4}$, demuestre que a es una raíz primitiva módulo p si y solamente si $-a$ lo es.

b) Si $p \equiv 3 \pmod{4}$, demuestre que a es una raíz primitiva módulo p si y solamente si $-a$ tiene orden $\frac{p-1}{2}$.

Problema 6.7. Demuestre que

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

si $p-1 \nmid k$. Por ejemplo,

$$1^3 + 2^3 + 3^3 + 4^3 = 100 \equiv 0 \pmod{5}.$$

Problema 6.8 (Gauss)**.** Demuestre que si $a_1, \ldots, a_s$ son diferentes raíces primitivas módulo p, entonces

$$a_1 \cdots a_s \equiv 1 \pmod{p}.$$

Problema 6.9 (Teorema de Wilson-3)**.** Use la existencia de una raíz primitiva para probar que $(p-1)! \equiv -1 \pmod{p}$.

Problema 6.10. Sea p un primo impar.

a) Demuestre que en $(\mathbb{Z}/p\mathbb{Z})^\times$ hay exactamente $\frac{p-1}{2}$ cuadrados (elementos de la forma x^2 para $x \in (\mathbb{Z}/p\mathbb{Z})^\times$).

b) Demuestre que los conjuntos $X = \{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$ e $Y = \{-1 - y^2 \mid y \in \mathbb{Z}/p\mathbb{Z}\}$ tienen intersección no vacía.

c) Deduzca que siempre existen $m, n \in \mathbb{Z}$ tales que $m^2 + n^2 + 1 \equiv 0 \pmod{p}$.