UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Residuos Cuadráticos. Orden y Raíces.

Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 15) 28.septiembre.2021

Raíces Módulo n

En los enteros módulo n, sabemos cómo resolver ecuaciones lineales:

Si $ax + b \equiv 0 \pmod{n}$, con $(a, n) = 1$, $\implies$ $x \equiv -ba^{-1} \pmod{n}$.

Pregunta: ¿Qué ocurre si queremos resolver ecuaciones de mayor grado?
Respues: problema difícil.

Por ejemplo: $x^2 - c \equiv 0 \pmod{n}$, $x^3 - c \equiv \pmod{n}$, $x^{43} \equiv c \pmod{n}$.

Definición

*Sean $c, k, n \in \mathbb{Z}$, $k, n > 1$. Diremos que x es una **raíz k-ésima módulo** n de c si*

$$x^k \equiv c \pmod{n}.$$

Ejemplos: 6 es una raíz cúbica de 8 módulo 13, pues

$$6^3 \equiv 6 \cdot 6^2 \equiv 6 \cdot 36 \equiv 6 \cdot 10 \equiv 60 \equiv 8 \pmod{13}.$$

¿Cuál es la raíz cuadrada de 3 módulo 11? Respuesta: 5. $5^2 \equiv 25 \equiv 3 \pmod{11}$.

Raíces Módulo n

Observaciones:

- No todos los números tiene raíces k-ésimas módulo n.
- Cuando existe la raíz k-ésima, no siempre es eficiente calcularla.

Casos fáciles:

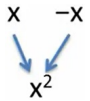
- Cuando $(k, \varphi(n)) = 1$.
  En este caso, tomamos $d = k^{-1} \pmod{\varphi(n)}$. Afirmamos que la raíz k-ésima de c es $x = c^d$.

  De hecho, como $d \cdot k \equiv 1 \pmod{\varphi(n)}$, esto significa que $d \cdot k = q\varphi(n) + 1$. Usando el Teorema de Euler-Fermat, resulta
  $$(c^d)^k = c^{dk} = c^{q\varphi(n)+1} = (c^{\varphi}(n))^q \cdot c \equiv (1)^q \cdot c \equiv c \pmod{n}.$$

- Si p es primo $\varphi(p) = p - 1$. Supongamos que $(k, p-1) = 1$.
  En este caso, si $d = k^{-1} \pmod{p-1}$, entonces la raíz k-ésima de c es $x = c^d$, pues
  $$(c^d)^k = c^{dk} = c^{q(p-1)+1} = (c^{p-1})^q \cdot c \equiv (1)^q \cdot c \equiv c \pmod{n}.$$

Raíces Módulo n

Raíces cuadradas: Vamos a trabajar módulo primo n.
En general, la función definida en $\mathbb{Z}/n\mathbb{Z}$ dada por $\mathbf{x} \mapsto \mathbf{x}^2$ es 2 a 1:



Obs!

- Lo anterior implica que si un número $c \pmod n$ tiene raíz cuadrada x, entonces tiene dos raíces cuadradas: x y $-x \pmod n$ (excepto cuando $x \equiv -x \pmod n$).
- $c = 0$ sólo tiene una raíz cuadrado, en todo módulo n.
- En módulo $n = 2$, 0 y 1 sólo tienen una raíz cuadrada.

Ejemplo: Módulo $n = 11$:

Residuos Cuadráticos

Estamos interesados en encontrar criterios simples que nos permitas saber si un número $d \pmod p$ posee raíz cuadrada. Esto es, si existen soluciones de la ecuación

$$x^2 \equiv d \pmod p. \tag{1}$$

Definición

Si la ecuación (1) tiene solución, esto es, $\bar{d}$ es un cuadrado perfecto en $\mathbb{Z}/p\mathbb{Z}$, diremos que d es un ***residuo cuadrático*** *módulo p.*

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \left(\pm \frac{p-1}{2}\right)^2 \pmod p,$$

ya que $i^2 \equiv (-i)^2 \pmod p$.

Así, si x es residuo cuadrático módulo p, debe ser congruente a alguno de estos números.

Residuos Cuadráticos

Ahora, aunque conozcamos la lista completa de residuos cuadráticos módulo p, en la práctica es difícil reconocer si un número d es o no residuo cuadrático módulo p.

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Ejemplo: ¿Es 53 resíduo cuadrático módulo 101? No.

Precisamos de una forma eficiente para determinar si un entero a cualquiera es residuo cuadrático módulo p.

Símbolo de Legendre

Definición

Sea $p > 2$ un número primo y $a \in \mathbb{Z}$ un entero cualquiera. Definimos el ***símbolo de Legendre*** *como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } p \nmid a \text{ y } a \text{ es residuo cuadrático módulo } p; \\ 0, & \text{si } p \mid a; \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Proposición (Criterio de Euler)

Sea $p > 2$ un primo impar, y sea $a \in \mathbb{Z}$. Entonces

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

Ejemplo: Para $p = 11$

a	0	1	2	3	4	5	6	7	8	9	10
$a^{\frac{p-1}{2}}$	1	1	-1	1	1	1	-1	-1	-1	1	-1

Corolario (Euler)

Sea $p > 2$ primo. Entonces $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ si, y sólo si, $p \equiv 1 \pmod{4}$.

Prueba: Como p es impar, sólo puede ser de la forma $p = 4k+1$ o de la forma $p = 4k+3$.

- Si $p = 4k+1 \Rightarrow \frac{p-1}{2} = \frac{4k}{2} = 2k$. Luego, $(-1)^{(p-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p}$.
- Si $p = 4k+3 \Rightarrow \frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$. Luego, $(-1)^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$.

Corolario

El símbolo de Legendre satisface las siguientes propiedades:

1. *Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a^2}{p}\right) = 1$, *si $p \nmid a$.*
3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. *Esto es, -1 es residuo cuadrático módulo $p \Leftrightarrow p \equiv 1 \pmod{4}$.*
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Símbolo de Legendre

Prueba: (1) y (2) son inmediatos a partir de la definición, o si lo prefieren, también se deducen a partir de Criterio de Euler:

$$a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) \pmod{p} \Rightarrow , \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

$$\left(\frac{1}{p}\right) \equiv (1)^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow \left(\frac{1}{p}\right) = 1.$$

(3) Del Criterio de Euler, junto con el corolario anterior, tenemos

$$\left(\frac{-1}{p}\right) \equiv 1 \pmod{p} \iff (-1)^{(p-1)/2} \equiv 1 \pmod{p}$$

$$\iff p = 4k + 1 \iff p \equiv 1 \pmod{4}.$$

(4) Finalmente, del Criterio de Euler tenemos que

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}\, b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

lo que muestra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pues ambos lados son iguales a ± 1. □

Símbolo de Legendre

El Criterio de Euler ya produce un mecanismo para identificar residuos cuadráticos. Vamos a enunciar ahora un resultado más general.

Teorema (Ley de Reciprocidad Cuadrática)

1. *Sea p un primo impar. Entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & si\ p \equiv \pm 1 \pmod 8; \\ -1, & si\ p \equiv \pm 3 \pmod 8. \end{cases}$$

2. *Sean p, q primos impares distintos. Entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

- La parte 1 sirve sólo para saber si 2 es residuo cuadrático módulo p.
- La parte 2 sirve para intercambiar de $(\frac{p}{q})$ a $(\frac{q}{p})$, cuando p, q son primos impares.

Corolario

Si p y q son primos impares distintos, entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 4, \text{ó } q \equiv 1 \pmod 4; \\ -1, & \text{si } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Prueba: Basta ver que si $p = 4k + 1$, el exponente $\frac{p-1}{2} = 2k$ es par. Similarmente para el caso $q = 4k + 1$. Por el contrario, si $p = 4k + 3$ y $q = 4j + 3$, ambos exponentes son impares. □

Corolario

Si p y q son primos impares distintos, entonces

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{si } p \equiv 1 \pmod 4, \text{ó } q \equiv 1 \pmod 4; \\ -\left(\frac{q}{p}\right), & \text{si } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Residuos Cuadráticos

Ejemplo: Calcular $\left(\frac{29}{53}\right)$.

De la Ley de Reciprocidad Cuadrática, tenemos -0.1cm

$$\begin{aligned}
\left(\frac{29}{53}\right) &= \left(\frac{53}{29}\right)(-1)^{\frac{29-1}{2}\cdot\frac{53-1}{2}} = \left(\frac{53}{29}\right)(-1)^{14\cdot 26} = \left(\frac{53}{29}\right) \\
&= \left(\frac{24}{29}\right) = \left(\frac{2^3\cdot 3}{29}\right) = \left(\frac{2}{29}\right)^3\left(\frac{3}{29}\right) = \underbrace{\left(\frac{2}{29}\right)^2}_{=1}\left(\frac{2}{29}\right)\left(\frac{3}{29}\right) \\
&= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{29}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{29-1}{2}} = \left(\frac{2}{29}\right)\left(\frac{29}{3}\right)(-1)^{1\cdot 14} \\
&= \left(\frac{2}{29}\right)\left(\frac{29}{3}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{3}\right) = (-1)^{\frac{29^2-1}{8}}(-1)^{\frac{3^2-1}{2}} \\
&= (-1)^{105}(-1)^1 = (-1)^{106} = 1.
\end{aligned}$$

Esto muestra que 29 es residuo cuadrático módulo 53.

Residuos Cuadráticos

Ejemplo: Determinar si 90 es residuo cuadrático módulo 1019.

Como $90 = 2 \cdot 3^2 \cdot 5$, tenemos que

$$\begin{aligned}
\left(\frac{90}{1019}\right) &= \left(\frac{2 \cdot 3^2 \cdot 5}{1019}\right) = \left(\frac{2}{1019}\right) \underbrace{\left(\frac{3^2}{1019}\right)}_{=1} \left(\frac{5}{1019}\right) \\
&= \left(\frac{2}{1019}\right)\left(\frac{5}{1019}\right) = \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right)(-1)^{\frac{5-1}{2} \cdot \frac{1019-1}{2}} \\
&= \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right)(-1)^{2 \cdot 509} = \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right) = \left(\frac{2}{1019}\right)\left(\frac{4}{5}\right) \\
&= \left(\frac{2}{1019}\right) \underbrace{\left(\frac{2^2}{5}\right)}_{=1} = \left(\frac{2}{1019}\right) = (-1)^{\frac{1019^2-1}{8}} = (-1)^{129,795} \\
&= -1.
\end{aligned}$$

Esto muestra que 90 no es residuo cuadrático módulo 1019.

Residuos Cuadráticos

¿Cómo calcular raíces cuadradas módulo p?

- Si $p \equiv 3 \pmod 4$: En este caso, si a es residuo cuadrático módulo p, tenemos que $\sqrt{a} = a^{\frac{p+1}{4}}$.

  Prueba: $p \equiv 3 \pmod 4 \Rightarrow p+1 \equiv 0 \pmod 4 \Rightarrow 4 \mid p+1$. Además, como a es residuo cuadrático, del criterio de Euler $a^{\frac{p-1}{2}} = 1$. Luego

  $$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv 1 \cdot a \equiv a \pmod p.$$

  Ejemplo: Hallar la raíz de 7 módulo 19: Como $p = 1019 \equiv 3 \pmod 4$, tenemos $\frac{p+1}{4} = \frac{19+1}{4} = 5$. Así

  $$\sqrt{7} = 7^5 = 7^2 \cdot 7^3 \equiv 11 \cdot 77 \equiv 11 \cdot 1 \equiv 11 \pmod{19},$$

  y las raíces de 7 son 11 y $8 = -11 \pmod{19}$.
- Si $p \equiv 1 \pmod 4$: En este caso no tenemos un algoritmo directo. Sin embargo existen algoritmos eficientes (aleatorios) de complejidad $O(log^3 p)$.

Orden y Raíces Primitivas

Definición

*Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* = U(n)$, 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 $\varphi(5) = 4$.

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 $\text{ord}(1) = 1$, $\text{ord}(4) = \text{ord}(11) = \text{ord}(14) = 2$, $\text{ord}(2) = \text{ord}(7) = \text{ord}(8) = \text{ord}(13) = 4$. 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	(mod 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.

Orden y Raíces Primitivas

Ejemplo: Módulo 14

a	a^1	a^2	a^3	a^4	a^5	a^6	(mod 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.

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 $U(n)$, esto es*

$$\langle \bar{a} \rangle = \{\bar{a}^t : t \in \mathbb{N}\} = U(n).$$

Orden y Raíces Primitivas

Las raíces primitivas son importantes en varios aspectos computacionales. 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.* □

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.

Importante: Actualmente muchas herramientas criptográfica basan su fortaleza en la dificultad de calcular el logaritmo discreto. Veremos más de este tema en la próxima clase.

Problemas Intratables

Problemas simples en aritmética modular:

- Dado un entero $n > 1$, y dado $a \in \mathbb{Z}$ con $(a, n) = 1$, hallar $a^{-1} \pmod{n}$.
  (Se puede calcular con el algoritmo de Euclides extendido).
- Dado un primo p y un polinomio $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, hallar un $a \in \mathbb{Z}/p\mathbb{Z}$ tal que $f(a) \equiv 0 \pmod{p}$ (si existe),
  (Hay algoritmos en tiempo $O(\deg f)$ para calcular raíces).

Ahora, no todos los problemas en aritmética modular son simples. Existen problemas para los cuales no hay algoritmos eficientes.

Problemas difíciles:

- Dado un entero $a, b \in \mathbb{Z}$, y enteros $k, n > 1$, hallar $b \in \mathbb{Z}$ tal que $b^k \equiv a \pmod{n}$.
  k se llama el **logaritmo discreto** de a con base b módulo n (No existen algoritmos simples para calcular k).