Logaritmo Discreto

Ronald Mas,
Angel Ramirez

28 de agosto de 2020

Contenido

El símbolo de Legendre

Residuos cuadráticos

Sean $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ tal que $MCD(a, n) = 1$, decimos que a es un **residuo cuadrático** módulo n si existe un $x \in \mathbb{Z}$ tal que:

$$x^2 \equiv a \,(mod\, n),$$

caso contrario, decimos que a no es un residuo cuadrático módulo n.

Observación:

- Como siempre $0^2 \equiv 0 \,(mod\, n)$, nos interesa estudiar los residuos cuadráticos positivos.

Ejemplo:

Para calcular los residuos cuadráticos módulo 11, es necesario calcular todos los cuadrados de todos lo números menores que 11. es decir:

$$
\begin{aligned}
1^2 &\equiv 1\,(mod\,11) \\
2^2 &\equiv 4\,(mod\,11) \\
3^2 &\equiv 9\,(mod\,11) \\
4^2 &\equiv 5\,(mod\,11) \\
5^2 &\equiv 3\,(mod\,11)
\end{aligned}
\qquad \text{y} \qquad
\begin{aligned}
6^2 &\equiv 3\,(mod\,11) \\
7^2 &\equiv 5\,(mod\,11) \\
8^2 &\equiv 9\,(mod\,11) \\
9^2 &\equiv 4\,(mod\,11) \\
10^2 &\equiv 1\,(mod\,11)
\end{aligned}
$$

Por tanto, los números residuos cuadráticos módulo 11 son $1, 3, 4, 5$ y 9 y los números que no son números residuos cuadráticos módulo 7 son $2, 6, 7, 8$ y 10.

Número de residuos cuadráticos módulo n

Teorema

Si $p > 2$ un número primo entonces en el conjunto $S = \{1, 2, 3 \cdots, p-1\}$ existen exactamente $(p-1)/2$ residuos cuadráticos y $(p-1)/2$ no residuos cuadráticos módulo p.

Prueba:

Por el teorema de Fermat el conjunto S coincide con el conjunto de residuos positivos de los enteros:

$$a, a^2, a^3, \cdots, a^{p-1} \text{ modulo } p.$$

Luego, la ecuación $x^2 \equiv b \,(mod\, p)$ posee solución si y sólo si $2 \mid ind_a(b)$. Es decir, $x^2 \equiv b \,(mod\, p)$ posee solución si y sólo si

$$b \equiv a^{2j} \,(mod\, p)$$

para algún $j = 1, 2, \cdots, (p-1)/2$. Por lo tanto existen exactamente $(p-1)/2$ residuos cuadráticos, dejando $(p-1)/2$ no residuos cuadráticos en S.

Símbolo de Legendre

Sean $c \in \mathbb{Z}$ y $p > 2$ un número primo, entonces:

$$\left(\frac{c}{p}\right) = \begin{cases} 0 & si \quad p \mid c \\ 1 & si \quad c \text{ es un residuo cuadrático módulo } p \\ -1 & si \quad \text{cumple otros casos} \end{cases}$$

y $\left(\frac{c}{p}\right)$ es llamado el **símbolo de Legendre** de c con respecto a p.

Ejemplo:

Del ejemplo anterior se tiene que:

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1 \text{ y}$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Teorema (Criterio de Euler para residuos cuadráticos)

Si $p > 2$ es un número primo, entonces

$$\left(\frac{c}{p}\right) \equiv c^{(p-1)/2} \,(mod\ p).$$

Teorema

Sea p un número primo impar, definamos $s_1 = 4$ y recursivamente para $i \geq 2$, $s_i = s_{i-1}^2 - 2$. Entonces $M_p = 2^p - 1$ es un número primo si y sólo si

$$s_{p-1} \equiv 0 \,(mod\ M_p).$$

Teorema

Si $p > 2$ es un número primo y $b, c \in \mathbb{Z}$, entonces:

1) *Si $b \equiv c \,(mod\, p)$ entonces $\left(\frac{b}{p}\right) = \left(\frac{c}{p}\right)$.*
2) $\left(\frac{b}{p}\right)\left(\frac{c}{p}\right) = \left(\frac{bc}{p}\right)$.
3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Prueba:

2) Usando el Criterio de Euler para residuos cuadráticos se tiene:

$$\begin{aligned}\left(\frac{b}{p}\right)\left(\frac{c}{p}\right) &\equiv b^{(p-1)/2}c^{(p-1)/2} \,(mod\, p)\\ &\equiv (bc)^{(p-1)/2} \,(mod\, p)\\ &\equiv \left(\frac{bc}{p}\right) \,(mod\, p)\end{aligned}$$

Ejemplo: Como $-3 \equiv 11 \,(mod\, 7)$ se tiene que:

$$\left(\frac{-3}{7}\right) = \left(\frac{11}{7}\right) = 1.$$

Lema (Lema de Gauss para residuos cuadráticos)

Sea $p > 2$ un número primo y $c \in \mathbb{Z}$ con $MCD(c, p) = 1$. Sea el conjunto R conformado por los residuos positivos r_i tal que $r_i \equiv ic \,(mod\, p)$ con $i = 1, 2, \cdots, (p-1)/2$ y $S = \{r_i \in R : r_i > p/2\}$, con $\mid S \mid = s$ se tiene que:

$$\left(\frac{c}{p}\right) = (-1)^s.$$

Ejemplo:

Para $c = 3$ y $p = 11$, se debe hallar los residuos $r_i \equiv 3i \,(mod\, 11)$ con $i = 1, 2, 3, 4, 5$. Al resolver se tiene que:

$$r_1 = 3, r_2 = 6, r_3 = 9, r_4 = 1 \text{ y } r_5 = 4.$$

Luego $S = \{6, 9\}$, por ello $s = \mid S \mid = 2$, por lo tanto

$$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

Teorema

Para todo número primo $p > 2$ se cumple:

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8} (mod\ p).$$

Corolario

Si p es un número primo impar, entonces

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

Prueba:

Si $p \equiv \pm 1\,(mod\,8)$ entonces $p^2 \equiv 1\,(mod\,16)$ entonces $p^2 - 1 = 16k$ para algún $k \in \mathbb{N}$, luego por el teorema anterior se tiene que:

$$\left(\frac{2}{p}\right) \equiv (-1)^{2k}\,(mod\,p) \longrightarrow \left(\frac{2}{p}\right) = 1.$$

Ejemplo:

Usando el teorema anterior se puede concluir que:

$$\left(\frac{2}{11}\right) \equiv (-1)^{(11^2-1)/8} \equiv -1\,(mod\,11)$$

$$\left(\frac{2}{7}\right) \equiv (-1)^{(7^2-1)/8} \equiv 1\,(mod\,7)$$

$$\left(\frac{2}{13}\right) \equiv (-1)^{(13^2-1)/8} \equiv -1\,(mod\,13)$$

$$\left(\frac{2}{17}\right) \equiv (-1)^{(17^2-1)/8} \equiv -1\,(mod\,17)$$

Ley de Reciprocidad cuadrática

Teorema (Ley de Reciprocidad cuadrática)

Si $p \neq q$ son primos impares entonces

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

Ejemplo:

Para $p = 7$ y $q = 101$ se tiene por reciprocidad cuadrática que:

$$\left(\frac{7}{101}\right)\left(\frac{101}{7}\right) = (-1)^{3\cdot 50} = 1.$$