EL SÍMBOLO DE LEGENDRE Y LA LEY DE RECIPROCIDAD CUADRÁTICA

Sea p un primo impar y $a \in \mathbb{Z}$. El Símbolo de Legendre $(\frac{a}{p})$ se define de la siguiente manera:

$$(\frac{a}{p}) := \begin{cases} 0, \text{ if } p \text{ divide a } a \\ 1, \text{ si existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv a \pmod{p} \text{ y } p \text{ no divide a } a \\ -1, \text{ en otro caso.} \end{cases}$$

Si $(\frac{a}{p}) = 1$ decimos que a es un residuo cuadrático módulo p.

Si $(\frac{a}{p}) = -1$ entonces a es un no residuo cuadrático mod p.

Proposiciones Previas. Dos hechos que se deben tener presentes:

(1) Como p es primo $\mathbb{Z}_p$ es un cuerpo, por lo que

$$\mathbb{Z}^* = \mathbb{Z}_p - \{0\}$$

es el grupo multiplicativo de los elementos invertibles mod p. Tiene orden $p-1$. En particular, todo entero a no divisible por p satisface $a^{p-1} \equiv 1 \pmod{p}$ (pequeño Teorema de Fermat).

(2) si $f(x) \in K[x]$ tiene grado n, donde K es un cuerpo, entonces $f(x)$ tiene a lo sumo n raíces.

0.1. **Propiedades del Símbolo de Legendre (PSL).**

$PLS1$ El símbolo está definido módulo p, es decir:
Si $a \equiv b \pmod{p}$, entonces $(\frac{a}{p}) = (\frac{b}{p})$.

Demostración:

Es una consecuencia inmediata de las propiedades básicas de la noción de congruencia. □

Se deduce de $PLS1$ que la función $(\frac{\cdot}{p})$ definida por

$(\frac{\cdot}{p})$: $\mathbb{Z} \longrightarrow \{0, \pm 1\}$
$a \longmapsto (\frac{a}{p})$

induce la función

$(\frac{\bar{\cdot}}{p})$: $\mathbb{Z}_p \longrightarrow \{0, \pm 1\}$
$a + p\mathbb{Z} \longmapsto (\frac{a}{p})$

La restricción de $(\frac{\bar{\cdot}}{p})$ al grupo multiplicativo $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ de unidades o elementos invertibles de $\mathbb{Z}_p$ es un homomorfismo del grupo multiplicativo $\mathbb{Z}_p^*$ en $\{\pm 1\}$, por tanto un caracter de $\mathbb{Z}_p^*$. Es el único caracter cuadrático (de orden 2) del grupo de caracteres de $\mathbb{Z}_p^*$.

Si $a \in Z_p^*$, es frecuente el abuso de notación siguiente: $(\frac{a}{p})$ en lugar de $(\frac{\bar{a}}{p})$. Observe también que a es un cuadrado en Z_p^* si, y sólo si, cualquier entero representante de a en Z_p es un residuo cuadrático módulo p.

PSL2 (*La propiedad de Euler del Símbolo de Legendre*).

$\forall a \in \mathbb{Z}$, $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demostración:

(1) (Gauss) Sea p primo impar. Sea $C = \{1, \cdots, \frac{p-1}{2}\}$.
Si a y $b \in C$; $a \neq b$, entonces $a^2 \not\equiv b^2 \pmod{p}$ (verifíquelo).
Sigue que existen al menos $\frac{p-1}{2}$ cuadrados en $\mathbb{Z}_p^*$.

(2) Suponga que $(\frac{a}{p}) = 1$. Sea $x \in \mathbb{Z}$ t. q. $x^2 \equiv a \pmod{p}$.

Entonces $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ donde la última congruencia se cumple por el pequeño teorema de Fermat pues p no divide a a (i.e. la propiedad de Euler se cumple para residuos cuadráticos módulo p).

de la igualdad siguiente, que se cumple en $\mathbb{Z}_p[x]$

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} + 1)(x^{\frac{p-1}{2}} - 1),$$

y de la Proposición previa, se deduce que ambos polinomios del lado derecho tienen exactamente $\frac{p-1}{2}$ raíces en $\mathbb{Z}_p^*$. Como hay al menos $\frac{p-1}{2}$ cuadrados en $\mathbb{Z}_p^*$ y todos son raíces del polinomio

$(x^{\frac{p-1}{2}} - 1)$, se concluye que los no cuadrados de son exactamente las raíces del polinomio $(x^{\frac{p-1}{2}} + 1)$, lo que concluye la demostración de la propiedad de Euler $\square$

PSL3 (*El símbolo de Legendre es multiplicativo)*):

$\forall a, b \in \mathbb{Z}$, $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Demostración: Se deduce de la propiedad de Euler del Símbolo de Legendre pues la función

$$\begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z}_p \\ a \longmapsto a^{\frac{p-1}{2}} \pmod p \end{array}$$

satisface $(ab)^{\frac{p-1}{2}} \pmod p = a^{\frac{p-1}{2}} \pmod p b^{\frac{p-1}{2}} \pmod p$ $\square$

Ejercicio 1

(1) Haga la lista de todos los residuos cuadráticos módulo p para $p = 3, 5, 13$ and 19.

(2) Deduzca el valor de $(\frac{7}{19})$

(3) Use la propiedad de Euler del símbolo para calcular $(\frac{2}{31})$ and $(\frac{3}{31})$.

(4) Sea $RC =: \{a \in \mathbb{Z} \mid (\frac{a}{p}) = 1\}$; $\bar{RC} := \{a + p\mathbb{Z} \mid (\frac{a}{p}) = 1\}$. Demuestre que $\bar{RC}$ es un subgrupo de índice 2 en $\mathbb{Z}_p^*$.

(5) Complete los detalles de la demostración de la Propiedad de Euler del símbolo de Legendre.

(6) *Prueba "moderna" de PSL1,2 y 3*:

Verifique:

- $\forall m > 0 \in \mathbb{Z}$, la función $e(m) =$ "elevar a la m"

  $$\begin{array}{rl} e(m): & \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^* \\ & x \longmapsto x^m \end{array}$$

  es un endomorfismo de $\mathbb{Z}_p^*$.

- La imagen de $e(2) := e(2)(\mathbb{Z}_p^*)$ es el conjunto de cuadrados en $\mathbb{Z}_p^*$; el conjunto de residuos cuadráticos $\mod p$ es el conjunto de enteros representantes de los elementos de la imagen de $e(2)$).

- Como el kernel de $e(2) = \{\pm 1 \ + p\mathbb{Z}\}$, del primer Teorema de Isomorfismos de grupos se deduce que la "imagen de $e(2)$"$= e(2)(\mathbb{Z}_p^*)$ es un subgrupo de $\mathbb{Z}_p^*$ con $\frac{p-1}{2}$ elementos.
- La multiplicatividad del símbolo de Legendre(PSL3) se deduce (para enteros no divisibles por p) del hecho que el cociente $\frac{\mathbb{Z}_p^*}{e(2)(\mathbb{Z}_p^*)}$ es isomorfo al grupo $\{\pm 1\}$ (porque es un grupo de dos elementos).
- PSL2 es consecuencia de que la siguiente sucesión es exacta:

$$\mathbb{Z}_p^* \xrightarrow{e(2)} \mathbb{Z}_p^* \xrightarrow{e(\frac{p-1}{2})} 1$$

1. La Ley de Reciprocidad Cuadrática (LRC)

Teorema. *Sea p un primo impar. Entonces:*

(1) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ si } p \equiv 1 \pmod 4 \\ -1, \text{ si } p \equiv -1 \pmod 4 \end{cases}$

(2) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ si } p \equiv \pm 1 \pmod 8 \\ -1, \text{ si } p \equiv \pm 3 \pmod 8 \end{cases}$

(3) Sea $q \neq p$ otro primo impar. Entonces

$$(\frac{q}{p}) = (-1)^{(\frac{p-1}{2}\frac{q-1}{2})}(\frac{p}{q}) = \begin{cases} (\frac{p}{q}), \text{ si } p \text{ ó } q \equiv 1 \pmod 4 \\ -(\frac{p}{q}), \text{ si } p \text{ y } q \equiv -1 \pmod 4 \end{cases}$$

Ejercicio 2

(1) Demuestre el item (1) of LRC.

(2) verifique que el item (2) de LRC se cumple para todo primo impar $p \leq 17$.

(3) Use LRC y la propiedad multiplicativa del símbolo para obtener el valor de $(\frac{-2}{p})$.

(4) Dado que 3617 es primo, use la LRC para calcular $(\frac{a}{3617})$ para $a = 11, 25, 40$ y 41.

2. LRC para el símbolo de Jacobi (SJ)

(SJ)

Sea $a \in \mathbb{Z}$; $n > 1$ impar. Sea $n = p_1 \cdots p_k$ la factorización de n como producto de primos. El símbolo de Jacobi $(\frac{a}{n})$ se define como $(\frac{a}{n}) := \prod_{i=1}^{i=k} (\frac{a}{p_i})$.

Propiedades de SJ:

El símbolo de Jacobi comparte las propiedades (1) y (3) del Símbolo de Legendre, pero no la propiedad de Euler de SL (por qué?). De modo que:

(1) Si $a \equiv b \pmod{n}$, entonces $(\frac{a}{n}) = (\frac{b}{n})$.

(2) $\forall a, b \in \mathbb{Z}$, $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.

LRC para SJ

Teorema. Sea $n > 1$ impar. Entonces:

(1) $(\frac{-1}{n}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{si} n \equiv 1 \pmod{4} \\ -1, \text{si } n \equiv -1 \pmod{4} \end{cases}$

(2) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1, \text{si } n \equiv \pm 1 \pmod{8} \\ -1, \text{si } n \equiv \pm 3 \pmod{8} \end{cases}$

(3) Sea $m \neq n$ impar. Entonces

$$(\frac{m}{n}) = (-1)^{(\frac{n-1}{2}\frac{m-1}{2})}(\frac{n}{m}) = \begin{cases} (\frac{n}{m}), \text{si } n \text{ ó } m \equiv 1 \pmod{4} \\ -(\frac{n}{m}), \text{si } n \text{ y } m \equiv -1 \pmod{4} \end{cases}$$

Ejercicio 3

(1) Demuestre las dos *propiedades de SJ* enunciadas arriba.

(2) El siguiente ejercicio es sobre como se deriva LRC para SJ a partir de LRC.

(a) Sea $k > 1$. Defina f como la funciíon

$$\begin{array}{c} f : 1 + k\mathbb{Z} \longrightarrow \mathbb{Z} \\ 1 + xk \longmapsto x \end{array} .$$

En otras palabras

$$\begin{array}{c} f : 1 + k\mathbb{Z} \longrightarrow \mathbb{Z} \\ a \longmapsto \frac{a-1}{k} \end{array} .$$

Sea π la proyección canónica $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_k$. Sea $h = \pi \circ f$. Demuestre que $h(ab) = h(a) + h(b)$, $\forall a, b \in 1 + k\mathbb{Z}$.

(b) Use la parte (a) y LRC de "Gauss" para demostrar *LRC* de "Jacobi".

3. El lema de Gauss en la demostración de LQR

Lema de Gauss: *Sea p un primo impar y a un entero no divisible por p. Considere los enteros $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ y sus menores residuos positivos módulo p. (Estos residuos son todos diferentes, por lo que hay $(p-1)/2$ de ellos.)*

Sea m el número de estos residuos que son mayores que $p/2$. Entonces

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

El Lema de Gauss es usado en varias de las pruebas LRC. La más común y simple aplicación es la demostración del item (2) de LCR, como mostramos a continuación.

Sea $C = \{1, 2, \cdots, \frac{p-1}{2}\}$. Según el lema de Gauss $\left(\frac{2}{p}\right) = (-1)^m$, donde

$$m = |\{i \in S \mid 2i \mod p \notin S\}| = |\{i \in [\frac{p-1}{2}] \mid \frac{p-1}{2} < 2i \leq p-1\}|$$
$$= [\frac{p-1}{2}] - [\frac{p-1}{4}]$$

donde $[x]$ denota la *parte entera de* x, esto es, El mayor entero que es menor o igual que x. La demostración concluye verificando que $[\frac{p-1}{2}] - [\frac{p-1}{4}]$ es par si $p \equiv \pm 1 \pmod 8$ e impar si $p \equiv \pm 3 \pmod 8$. □

Ejercicio 4

(1) Use LRC para mostrar que:

$$(\tfrac{3}{p}) = \begin{cases} 1, \text{ si } p \equiv \pm 1 \pmod{12} \\ -1, \text{ si } p \equiv \pm 5 \pmod{12} \end{cases}$$

y que

$$(\tfrac{5}{p}) = \begin{cases} 1, \text{ si } p \equiv \pm 1 \pmod{5} \\ -1, \text{ si } p \equiv \pm 3 \pmod{5} \end{cases}$$

(2) Use el Lema de Gauss para obtener el mismo resultado en cada caso.

4. Aplicación de LRC a primalidad

PM3: Si q es un divisor de $2^k - 1$, donde $k \geq 3$ es impar, entonces $q \equiv \pm 1 \pmod 8$.

Demostración: Supongamos que q divide a $2^k - 1$. Entonces

$$2^k \equiv 1 \pmod q \Longrightarrow (\frac{2^k}{q}) = (\frac{1}{q}) = 1 \Longrightarrow (\frac{2}{q}) = (\frac{2}{q})^k = 1 \ \square$$

El teorema de Proth:

Sean A y t enteros positivos, $A < 2^t$ impar. Sea $n = 1 + A2^t$ y $a \in \mathbb{Z}$ tal que $(\frac{a}{n}) = -1$, donde $(\frac{\cdot}{n})$ denota el símbolo de Jacobi. Las siguientes afirmaciones son equivalentes:

(1) *n es primo*

(2) $(a^{\frac{n-1}{2}}) \equiv -1 \pmod n$

Demostración: $(a) \Rightarrow (b)$ es consecuencia de la propiedad de Euler del símbolo de Legendre (PSL2).

$(b) \Rightarrow (a)$: Sea p un divisor de n. La hipótesis implica que

$$(a^{\frac{n-1}{2}}) \equiv -1 \pmod p$$

,

de donde $(a^A)^{2^{t-1}} \equiv -1 \pmod p$. Se deduce que el orden de a^A módulo p es 2^t (por qué?);

sigue que 2^t divide a $p - 1 = |\mathbb{Z}_p^*|$, es decir que

$$p \equiv 1 \pmod{2^t} \Rightarrow p > 2^t > \sqrt{n},$$

donde la última desigualdad se deduce de $A < 2^t$ y $n = 1 + A2^t$.

Pero $p > \sqrt{n}$ $\forall$ divisor primo p de $n \Rightarrow n$ es compuesto $\ \square$

Ejercicio 5

(1) Demuestre que la conclusión del Teorema de Proth se cumple bajo la hipótesis $A \leq 3 + 2^{t+1}$.

(2) Sea $A \in \mathbb{N}$, A impar y $A \not\equiv 0 \pmod 3$. Sea $n_t = A \cdot 2^t + 1$. Use el Teorema de Proth para verificar que para todo $t > 1$ tal que $3 + 2^{t+1} > A$, tenemos las siguientes posibilidades:
   (a) $(A, t) = (1 \pmod 3, 1 \pmod 2)$ ó $(A, t) = (-1 \pmod 3, 0 \pmod 2)$, en cuyo caso $n_t \equiv 0 \pmod 3$ y n_t no es primo.
   (b) $(A, t) = (1 \pmod 3, 1 \pmod 2)$ ó $(A, t) = (1 \pmod 3, 1 \pmod 2)$, en cuyo caso $n_t \equiv -1 \pmod 3$.
   En este caso demuestre que

$$n_t \text{ es primo } \iff 3^{\frac{n_t-1}{2}} = -1 \pmod{n_t}$$

   .

(3) Diseñe e implemente un programa que encuentre todos los primos $n_t = A \cdot 2^t + 1$, con $1 < t < 2000$, para $A = 1, 5, 7, 11$ ó 13.

(4) Pruebe que si $A = 3$ entonces, para cualquier conjunto finito de enteros $\{a_1, \cdots, a_k\}$, existen infinitos $t's$ tales que $(\frac{a_i}{n_t}) = 1$ for all $i = 1, 2, \cdots, k$.

(5) Tome esto en cuenta para encontrar los primos de la familia de los n_t, con $A = 3$ y $A = 9$, $1 < t < 2000$.

(6) Primos de Sophie Germain. Un primo p es de Sophie Germain si $q = 2p+1$ también es primo. Sea p un primo impar. Demuestre que p es un primo de Sophie Germain si, y sólo si, $p \not\equiv 1 \pmod 3$ y $2^q \equiv 2 \pmod q$

   (Sugerencia: Para todo divisor primo Q de q considere los posibles valores de $ord_Q(2)$. Concluya que $Q \leq \sqrt{q}$.)

Teorema (El Test de Lucas-Lehmer).

Sea p un primo impar. Sea $M_p = 2^p - 1$ un número de Mersenne. Sea A el anillo $\mathbb{Z}_{M_p}[\sqrt{3}]$. Sea β la imagen de $-2 + \sqrt{3}$ en A.

Las siguientes afirmaciones son equivalentes:

(1) M_p es primo.
(2) $\beta^{2^{p-1}} = -1$
(3) La sucesión S_k definida por:

$S_0 = 4$;
$S_{k+1} = S_k^2 - 2$ si $k \geq 0$, satisface
$S_{p-2} \equiv 0 \pmod{M_p}$.