2.1 Símbolo de Legendre y sus propiedades.

Sea p un primo impar. Diremos que un número natural a primo con p es un *resto cuadrático* módulo p si $x^2 \equiv a(mód.p)$, para cierto entero x. En caso contrario, siempre suponiendo que p es primo, diremos que a es un *resto no cuadrático*. Se conoce como *símbolo de Legendre* a la expresión

$$\left(\frac{a}{p}\right)=(a/p)=\begin{cases} 1 \text{ si } a \text{ es resto cuadratico } módulo\ p \\ -1 \text{ si } a \text{ es resto no cuadrático } módulo\ p \\ 0 \text{ si } p \mid a \end{cases}$$

Si a es un resto cuadrático respecto al módulo p, se tiene $a^{\frac{p-1}{2}} \equiv 1(mód.p)$. Si a es un no cuadrático respecto al módulo p, se tiene $a^{\frac{p-1}{2}} \equiv -1(mód.p)$. En efecto, según el teorema de Fermat, $a^{p-1} \equiv 1(mód.p)$ donde $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0(mód.p)$. De aquí podemos deducir que $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)(mód.p)$ que nos permite la solución a la ecuación $x^2 \equiv a(mód.p)$ aplicando propiedades del símbolo de Legendre.
El símbolo de Legendre satisface algunas propiedades interesantes como:

i. Si $a \equiv b(mód.p)$, entonces $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$. Esta propiedad se debe a que los números de una misma clase son simultáneamente restos o no restos cuadráticos.

ii. Si $a \equiv 1(mód.p)$, tenemos $\left(\frac{1}{p}\right)=1$. En efecto, $1=1^2$ y, por tanto, 1 es un resto cuadrático.

iii. Si $a \equiv -1(mód.p)$, entonces $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. Esta propiedad se deduce de la anterior para $a=-1$ y denota un resto no cuadrático.

iv. Si $a \equiv 2(mód.p)$, entonces $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

v. Si $a \equiv -3(mód.p)$, entonces $\left(\frac{-3}{p}\right)=\begin{cases} 1 \text{ si } p \equiv 1(mód.6) \\ -1 \text{ si } p \equiv 5(mód.6) \end{cases}$.

vi. Si $a \equiv 5(mód.p)$, entonces $\left(\frac{5}{p}\right)=\begin{cases} 1 \text{ si } p \equiv 1,9(mód.10) \\ -1 \text{ si } p \equiv 3,7(mód.10) \end{cases}$.

vii. Sea $\left(\frac{abb}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right)$. Se deduce, en particular, que $\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{a}{p}\right)$, ya que $\left(\frac{b}{p}\right)^2=1$. Esto significa que en el numerador del *símbolo de Legendre* se puede eliminar cualquier factor cuadrático.

viii. Si p y q son números primos impares, $\left(\frac{q}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{p}{q}\right)$. Esta propiedad es conocida como *Ley de Reciprocidad Cuadrática*.

Nota: La *Ley de Reciprocidad Cuadrática* tiene un papel muy importante en la teoría de los números, ya que en base a ésta, se han obtenido otros resultados interesantes en diversos campos de las matemáticas. Descubierta por $Euler$ ($1707-1783$) en 1742, gracias a los trabajos realizados por $Fermat$ ($1601-1665$, revisada en 1772, fue publicada en su *Opuscula Analitica* de 1873, después de su muerte. $Legendre$ ($1752-1833$) fue otro de los pioneros en el estudio de esta ley, de hecho fue el primero en dar una demostración. Basándose en los trabajos de Euler, en 1798 publica en su obra *Essai sur la Théorie des Nombres* un lema que hoy se conoce como *símbolo de Legendre*. El primero que ofrece una demostración completa de la *Ley de Reciprocidad Cuadrátic*a fue $Gauss$ ($1777-1855$), a la que llama *Theorema Aureum* (Teorema áureo), recogida en su obra Disquisitiones Arithmeticae y publicada en 1796.

2.2 Símbolo de Jacobi y sus propiedades.

Consideremos el símbolo $\left(\frac{n}{m}\right)$ ó (n/m) para números impares m con $m>1,$ no necesariamente primos, donde $m=p_1\cdot p_2\cdot\ldots\cdot p_n,$ con $mcd(n,m)\neq 1.$
El *Símbolo de Jacobi* se define como

$$\left(\frac{n}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_2}\right)\ldots\left(\frac{l}{p_n}\right)$$

Sus propiedades son similares a las propiedades al S*ímbolo de Legendre*.
El uso del S*ímbolo de Jacobi* proporciona la generalización del S*ímbolo de Legendre* y la del teorema de los recíprocos cuadráticos $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{(m-1)(n-1)/4}$, para m,n relativamente primos enteros, con $n\geq 3.$ Esta igual es equivalente a

$$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

que también podemos escribir como:

$$\left(\frac{n}{m}\right)=\begin{cases}+\left(\frac{m}{n}\right)\ \text{para}\ m\ \acute{o}\ n\equiv 1(mód.4)\\ -\left(\frac{m}{n}\right)\ \text{para}\quad m,n\equiv 3(mód.4)\end{cases}.$$

Estos es lo que hemos definido anteriormente como *Ley de Reciprocidad Cuadrática*.

2.3 Demostrar que si p es primo y a y b son dos enteros con $a\equiv b(mód.p),$ entonces $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$

El valor de $\left(\frac{a}{p}\right)$ depende sólo de si a es restos cuadrático, esto es, si $x^2\equiv a(mód.p)$ tiene solución. Como esto sólo depende de la clase de equivalencia de a respecto a $p,$ se verifica que $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ si, y sólo si $a\equiv b(mód.p).$

Si p es primo y $mcd(a,p)=1,$ obtenemos $\left(\frac{a}{p}\right)\equiv a^{(p-1)/2}(mód.p),$ que es el *criterio de Euler*.

Por el *pequeño teorema de Fermat* sabemos que $a^{p-1}\equiv 1(mód.p),$ esto nos permite deducir que $\left(a^{p-1}\right)^2\equiv a^{p-1}\equiv \pm 1(mód.p),$ y para que $a^{p-1}\equiv 1(mód.p)$ será necesario que $\left(\frac{a}{p}\right)=1.$

Por ejemplo, si $a=7$ y p es de la forma $p\equiv 1(mód.4),$ tenemos

$$\left(\frac{7}{p}\right)=\left(\frac{p}{7}\right)=\begin{cases} 1\ si\ p\equiv 1,2,4(mód.7) \\ -1\ si\ p\equiv 3,5,6(mód.7)\end{cases}$$

Si p es de la forma $p\equiv 3(mód.4),$ tenemos

$$\left(\frac{7}{p}\right)=-\left(\frac{p}{7}\right)=\begin{cases} 1\ si\ p\equiv 3,5,6(mód.7) \\ -1\ si\ p\equiv 1,2,4(mód.7)\end{cases}$$

o, también

$$\left(\frac{7}{p}\right)=\begin{cases} 1\ si\ p\equiv 1,3,9,19,25,27(mód.28) \\ -1\ si\ p\equiv 5,11,13,15,17,23(mód.28)\end{cases}$$

2.4 Demostrar que si p es primo y a y b son dos enteros no divisibles con $q,$ entonces $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$

Sabemos que $a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)(mód.p),$ entonces $(ab)^{(p-1)/2}\equiv\left(\frac{ab}{p}\right)(mód.p)$ donde $mcd(ab,p)=1,$

como $a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)(mód.p)$ y $b^{(p-1)/2}\equiv\left(\frac{b}{p}\right)(mód.p),$ se cumple que $\left(\frac{ab}{p}\right)\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mód.p),$ y

como p no es par, $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$ luego $\left(\frac{ab}{p}\right)=a^{(p-1)/2}b^{(p-1)/2}=(ab)^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(mód.p).$

2.5 Demostrar que si p es impar, entonces $\left(\frac{2}{p}\right)=(-1)(p^2-1)/2.$

Sea $\left(\frac{a}{p}\right)=(-1)^k$ donde k es el número de restos que son mayores que $p/2,$ como $(-1)^8\equiv k(mód.2),$ entonces

$$\left(\frac{2}{p}\right)=(-1)^k=(-1)^{(p^2-1)/8}$$

El profesor Vinogradov llega a esta conclusión utilizando el S*ímbolo de Jacobi*. Este matemático dice que si *P* es impar mayor que la unidad, esto es, $m = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ que es la descomposición factorial de P, y si el $mcd(a,P)=1$, entonces el Símbolo de Jacobi $\left(\frac{a}{m}\right)$ se define por la igualdad:

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)=\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

A partir de lo expuestos podemos obtener otras igualdades como

$$\left(\frac{a}{p}\right)=\left(\frac{ab^2}{p}\right),\ \left(\frac{1}{p}\right)=1 \text{ ó } \left(\frac{1}{p}\right)=(-1)^{(p-1)/2}\left(\frac{1}{p}\right)=(-1)^{(p-1)/2}$$

y también

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)$$

que nos lleva a que

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}},$$

de la que nos permite deducir dos propiedades muy importantes del *Símbolo de Legendre*. La primera es que para $a=1$:

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

la segunda es que si *p* es de la forma $p=8m+s,$ donde *s* es uno de los números *1, 3, 5, 7*, y además

$$\left(\frac{p^2-1}{8}\right)=8m^2+2ms+\frac{s^2-1}{8}$$

entonces este número será par si $s=1$ ó $s=7,$ e impar si $s=3$ ó $s=5.$ Por tanto, el número *2* será resto cuadrático respecto al módulo *p* si *p* es de la forma $p=8m+1$ ó $p=8m+7$ y será no resto cuadrático respecto al módulo *p* si *p* es de la forma $p=8m+3$ ó $p=8m+5.$

2.6 Demostrar que si P y Q son números impares positivos, primos entre sí, entonces $\left(\frac{Q}{P}\right)=(-1)^{(P-1)(Q-1)/4}\left(\frac{P}{Q}\right)$.

Como $\left(\frac{P-1}{2}\right)\cdot\left(\frac{Q-1}{2}\right)$ es impar solamente cuando ambos números, P y Q, son de la forma $4m+3$, y es par si al menos uno de estos números es de la forma $4m+1$, la propiedad señalada se puede formular así:

Si ambos números, P y Q, son de la forma $4m+3$, entonces $\left(\frac{Q}{P}\right)=-\left(\frac{P}{Q}\right)$.

Si al menos uno de los números, P y Q, es de la forma $4m+1$, entonces $\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)$.

Supongamos que $Q=q_1\cdot q_2\cdot\ldots\cdot q_n$ es la descomposición de Q en factores primos, se tiene

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\cdot\left(\frac{Q}{p_2}\right)\cdot\ldots\cdot\left(\frac{Q}{p_n}\right)=\prod_{\alpha=1}^{s}\cdot\prod_{\beta=1}^{t}\left(\frac{Q_\beta}{P_\alpha}\right)$$

y como

$$\prod_{\alpha=1}^{s}\cdot\prod_{\beta=1}^{t}\left(\frac{Q_\beta}{P_\alpha}\right)=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}\right)}\prod_{\alpha=1}^{s}\cdot\prod_{\beta=1}^{t}\left(\frac{P_\alpha}{Q_\beta}\right)$$

resulta:

$$\left(\frac{Q}{P}\right)=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}\right)}\frac{P}{Q}.$$

Si ahora hacemos que

$$\frac{P-1}{2}=\sum_{\alpha=1}^{r}\frac{P_\alpha-1}{2}+2N \quad \text{y} \quad \frac{Q-1}{2}=\sum_{\beta=1}^{s}\frac{Q_\beta-1}{2}+2N_1,$$

entonces:

$$\left(\frac{Q}{P}\right)=(-1)^{(P-1)(Q-1)/4}\left(\frac{P}{Q}\right).$$