Capítulo

4

Reciprocidad Cuadrática

En este capítulo estudiamos una serie de resultados dirigidos a demostrar la Ley de Reprocidad Cuadrática, la cual fue probada por Gauss en su libro *Disquisitiones Arithmeticae* en 1801. Gauss dio tres pruebas diferentes de este teorema, y desde entonces han aparecido más de 150 demostraciones distintas.

Por intermedio de esta ley, se pueden determinar si existen soluciones o no, de una ecuación cuadrática del tipo:

$$x^2 \equiv a \ mod \ p, \quad (*)$$

donde p es primo y $(a, p) = 1$.

4.1 Símbolo de Legendre

De ahora en adelante, supondremos que p es primo.

Definición 4.1.1 *Diremos que un entero a es un* **resto cuadrático módulo** *p si la ecuación $(*)$ es soluble.*

Con la finalidad de simplificar las demostraciones introducimos el siguiente símbolo.

Definición 4.1.2 *Sea p primo, y sea a entero, con $(a, p) = 1$. Entonces $\left(\frac{a}{p}\right)$, llamado símbolo de Legendre de a sobre p, se define por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } a \text{ es un entero cuadrático mod } p \\ -1, & \text{si } a \text{ no es un resto cuadrático mod } p \end{cases}$$

Ejemplo 1: $\left(\frac{2}{7}\right) = 1$, porque $2 \equiv 3^2 \ mod \ 7$.

Ejemplo 2: $\left(\frac{5}{7}\right) = -1$, porque no existe x tal que $5 \equiv x^2 \ mod\ 7$.

Algunas propiedades elementales del símbolo de Legendre, vienen dadas en el siguiente:

Teorema 4.1.1 *Sea p primo y a, b enteros, primos relativos con p. Luego*

i) $\left(\frac{1}{p}\right) = 1$.

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

iii) Si $a \equiv b \ mod\ p$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Demostración:

Ciertamente *i)* y *ii)* son triviales.
Para probar *iii)* consideremos dos casos:

Caso I: Si $\left(\frac{a}{p}\right) = 1$, entonces existe un x tal que $a \equiv x^2 \ mod\ p$. Por lo tanto

$$b \equiv a \equiv x^2 \ mod\ p,$$

lo que implica

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

Caso II: Sea $\left(\frac{a}{p}\right) = -1$, y supongamos que $\left(\frac{b}{p}\right) = 1$, entonces repitiendo el mismo argumento del caso anterior se concluía $\left(\frac{a}{p}\right) = 1$, lo cual contradice la hipótesis. Por lo tanto se debe tener $\left(\frac{b}{p}\right) = -1$. ♠

Teorema 4.1.2 *(Criterio de Euler) Sean p primo y a un entero, con $(a,p)=1$. Entonces*

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

Demostración 1:

Sea b uno cualquiera de entre los números $1, 2, \cdots, p-1$ y consideremos la congruencia

$$bx \equiv a \ mod\ p. \tag{4.1}$$

la cual tiene solución, pues $(b,p)=1$.

Si b' es solución de (4.1), diremos que b y b' son asociados.

Si $\left(\frac{a}{p}\right)=1$, entonces existe un b_1 con $1 \leq b_1 \leq p-1$, y tal que

$$b_1^2 \equiv a \ mod\ p.$$

Además

$$(p-b_1)^2 = p^2 - 2pb_1 + b_1^2 \equiv a \ mod\ p.$$

Luego b_1 y $p-b_1$ son dos soluciones de la ecuación

$$x^2 \equiv a \ mod\ p, \tag{4.2}$$

y por el Teorema de Lagrange, sabemos que éstas son las únicas soluciones.

Podemos concluir, entonces que en el conjunto

$$\{1, 2, \cdots, p-1\} - \{b_1, p-b_1\},$$

cada elemento es diferente de su asociado.

Luego se tienen $(p-3)/3$ pares (b, b'), de elementos asociados distintos, tales que $bb' \equiv a \ mod \ p$, junto con los elementos b_1 y $p - b_1$. Estos son todos los elementos de $\{1, 2, \cdots, p-1\}$.

Multiplicando todos estos $p-1$ elementos se tendrá

$$(p-1)! = 1 \cdot 2 \cdots (p-1) \equiv \ a^{(p-3)/2} b_1 (p - b_1) \ mod \ p$$

o sea

$$(p-1)! \equiv -a^{(p-1)/2} \ mod \ p \tag{4.3}$$

Por otro lado, si $\left(\frac{a}{q}\right) = -1$, los elementos $1, 2, \cdots, p-1$ se pueden agrupar en $(p-1)/2$ pares de asociados distintos. Por lo tanto

$$(p-1)! \equiv a^{(p-1)/2} \ mod \ p \tag{4.4}$$

Usando el teorema de Wilson, tenemos

$$-1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \ mod \ p$$

o sea

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

♠

Demostración 2:

Caso I) Si $\left(\frac{a}{p}\right) = 1$, entonces existe x tal que

$$a \equiv x^2 \ mod \ p$$

luego

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv x^{2\frac{(p-1)}{2}} \ mod\ p \\ &\equiv x^{p-1} \ mod\ p \\ &\equiv 1 \ mod\ p \end{aligned}$$

Por lo tanto

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

Caso II) Si $\left(\frac{a}{p}\right) = -1$, entonces a no es cuadrado módulo p. Sean $x_1, \cdots x_s$ los cuadrados en $\mathbb{Z}_p$, donde $s = (p-1)/2$, entonces los elementos no nulos de $\mathbb{Z}_p$ son precisamente

$$x_1, \cdots, x_s, ax_1, \cdots, ax_s$$

por lo tanto

$$x_1 \cdots x_s a x_1 \cdots a x_s \equiv -1 \, mod\, p$$

por el teorema de Wilson.

Pero si x_i es cuadrado, su inverso x_i^{-1} es también cuadrado.

luego

$$\prod_{i=1}^{s} x_i \equiv 1 \, mod\, p$$

Entonces tendremos

$$\begin{aligned} x_1 \cdot x_s a x_1 \cdots a x_s &= a^s (x_1 \cdots x_s)^2 \\ &\equiv a^s \ mod\ p. \end{aligned}$$

Comparando ambos resultados se tiene

$$a^{\frac{p-1}{2}} \equiv -1 \, mod \, p \qquad \spadesuit$$

Veamos a continuación algunas aplicaciones del teorema 4.1.2

Ejemplo 3:

Probar que 5 es un resto cuadrático módulo 13.

Solución:

Usando (4.1.2) con $a = 5$ y $t = 3$ tenemos

$$\begin{aligned} \left(\frac{5}{13}\right) &\equiv 5^{(13-1)/2} \, mod \, 13 \\ &\equiv 5^6 \, mod \, 13 \\ &\equiv 15625 \, mod \, 13 \\ &\equiv 12 \, mod \, 13 \\ &\equiv -1 \, mod \, 13 \end{aligned}$$

Luego

$$\left(\frac{5}{13}\right) = -1$$

Teorema 4.1.3 *Sea p un número primo y a y b dos enteros primos relativos con* $(a, p) = 1$ *y (b,p)=1. Entonces*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Demostración:

Por intermedio del teorema 4.1.2 se obtiene

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

Nótese que los posibles valores de los términos en la congruencia

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) mod\, p$$

son todos ± 1, luego la congruencia anterior se convierte en igualdad con lo cual se obtiene el resultado.

♠

Teorema 4.1.4 *Si* $(a, b) = 1$ *y* $(c, p) = 1$ *se tiene*

$$\left(\frac{c^2 a}{p}\right) = \left(\frac{a}{p}\right)$$

Demostración:

Usando el teorema 4.1.3 , se obtiene

$$\left(\frac{c^2 a}{p}\right) = \left(\frac{c^2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$$

Ejemplo 6:

Calcular $\left(\frac{70}{11}\right)$.

Solución:

Aplicando las propiedades vistas en los ejemplos anteriores se tiene

$$\left(\frac{70}{11}\right) = \left(\frac{7}{11}\right)\left(\frac{5}{1}\right)\left(\frac{2}{11}\right)$$

Para calcular estos tres valores del lado derecho de la igualdad, construimos una tabla de cuadrados módulo 11:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	10

Usando los valores de la tabla, calculamos los símbolos de Legendre por inspección directa.

$$\left(\frac{7}{11}\right) = -1 \ , \ \left(\frac{5}{11}\right) = 1 \ , \ \left(\frac{2}{11}\right) = -1$$

luego

$$\left(\frac{70}{11}\right) = 1.$$

En la próxima sección, veremos un método más eficiente para calcular símbolos de Legendre sin necesidad de usar tablas.

Ejercicios

1) Sea p un número primo.

a) Probar que en $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, la mitad de los elementos son cuadrados y la otra mitad son no cuadrados.

b) Si a es no cuadrado y $x_1, \cdots, x_s$ son los cuadrados de $\mathbb{Z}_p^*$ entonces $ax_1, \cdots, ax_s$, son todos los no cuadrados de $\mathbb{Z}_p^*$.

2) Demostrar

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$$

3) Calcular

a) $\left(\frac{10}{3}\right)$ b) $\left(\frac{100}{5}\right)$ c) $\left(\frac{200}{3}\right)$

d) $\left(\frac{34}{7}\right)$ e) $\left(\frac{-10}{7}\right)$ f) $\left(\frac{80}{13}\right)$

4) Decidir cuáles de las siguientes ecuaciones posee solución

a) $x^2 \equiv 5 \ mod\ 13$

b) $x^2 \equiv -3 \ mod\ 7$

c) $x^2 \equiv -4 \ mod\ 19$

d) $x^2 \equiv 2 \ mod\ 7$

4.2 Ley de Reciprocidad Cuadrática

Comenzaremos por estudiar algunos resultados preliminares, que necesitamos para demostrar la Ley de Reciprocidad cuadrática.

Definición 4.2.1 *Sea x un número real cualquiera. La parte entera de x que se denota por $[x]$, se define como aquel entero n, tal que*

$$n \leq x < n+1$$

Ejemplos

$$[3,5]=3 \ ; \ [12]=12 \ ; \ [-3,1]=-4$$

Ejercicio:

Para todo real x se cumple.

$$x=[x]+\alpha \quad \text{con} \quad 0 \leq \alpha < 1.$$

Teorema 4.2.1 *Si m es un entero y x es real, se tiene*

$$[x+m] = [x] + [m]$$

Demostración:

De acuerdo al ejercicio anterior se debe cumplir

$$x = [x] + \alpha \quad , \quad 0 \leq \alpha < 1$$

luego

$$x + m = [x] + m + \alpha = t + \alpha,$$

donde $t = [x] + m$

Nótese que t es un entero y además satisface

$$t \leq x + m < t + 1$$

por lo tanto se debe tener

$$[x+m] = t = [x] + m$$

♠

Teorema 4.2.2 *Sean a y b enteros positivos. Entonces existe r tal que*

$$a = b\left[\frac{a}{b}\right] + r \quad , \quad 0 \leq r < b$$

Demostración:

De acuerdo al algoritmo de división, existen r y q tales que

$$a = bq + r \quad , \quad 0 \leq r < b \qquad (*)$$

Luego $a/b = q + (r/b)$. Nótese que q es un entero y además $0 \leq (r/b) < 1$.

Luego debemos tener

$$\left[\frac{a}{b}\right] = q$$

y al sustituir la útima relación en $(*)$ se obtiene el resultado.

♠

En lo sucesivo p y q serán dos números primos distintos. También pondremos

$$s = (p-1)/2 \quad \text{y} \quad t = (q-1)/2$$

Teorema 4.2.3 *(Lema de Gauss) Sea a entero positivo y p un número primo tal que $(a,p) = 1$ y sea K el número de residuos módulo p, mayores que $p/2$ en el conjunto $\{a, 2a, \cdots, sa\}$. Entonces*

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

Demostración:

El conjunto $\mathcal{A} = \{a, 2a, \cdots, sa\}$ se divide en dos partes

$$\mathcal{A}_r = \{x \in \mathcal{A} \mid x \equiv r_i \, mod \, p \quad , \quad 0 < r_i < p/2\}$$

y

$$\mathcal{A}_s = \{x \in \mathcal{A} \mid s_i \equiv r_j \, mod \, p \quad , \quad s_i > p/2\}$$

Sea $H = s - K$. Afirmamos que

$$r_1, r_2, \cdots, r_H, p - s_1, p - s_2, \cdots, p - s_K \qquad (*)$$

son todos elementos del conjunto $\{1, 2, 3, \cdots, s\}$

En primer lugar, notemos que los elementos en $(*)$ son todos mayores que cero y menores que $p/2$. Además, hay s de ellos. Luego si

podemos demostrar que esos s elementos son todos distintos, la afirmación quedará probada. Tenemos tres casos a considerar:

Caso I) Si $r_i = r_j$, para algunos i, j, entonces, existen $1 \leq R_i, R_j \leq s$, tales que

$$aR_i \equiv aR_j \ mod \ p.$$

Luego p divide a $a(R_i - R_j)$, lo cual implica que p divide a $R_i - R_j$, pues $(a, b) = 1$. Notemos ahora que

$$-p < R_i - R_j < p \quad y \quad R_i \equiv R_j \ mod \ p.$$

Estas dos condiciones se sastifacen, si y sólo si $R_i = R_j$, de donde se obtiene $i = j$.

Caso II) Si $p - s_i = p - s_j$, se obtiene $s_i = s_j$, y usando el mismo argumento del caso I, se deduce $i = j$.

Caso III) Si $r_i = p - s_j$ se sigue entonces

$$r_i \equiv -s_j \ mod \ p,$$

o sea,

$$aR_i \equiv -aS_j \ mod \ p,$$

con $1 \leq R_i, \ S_j \leq s$

Cancelando a en la última ecuación produce:

$$R_i + S_j \equiv 0 \ mod \ p$$

lo cual es imposible, pues R_i y S_j son dos elementos distintos del conjunto $\{1, 2, \cdots, s\}$ con $s = (p-1)/2$.

Por útimo concluimos $r_i \neq p - s_j$.

Con esto queda probada la afirmación.

Seguidamente, consideremos el producto de todos los elementos en $(*)$. Dicho producto resulta ser igual a el producto $1 \cdot 2 \cdots s = s!$, por la afirmación anterior. Se tiene entonces

$$\begin{aligned} s! &= (r_1 \cdots r_H)(p - s_1) \cdots (p - s_K) \\ &\equiv (-1)^K r_1 \cdots r_H s_1 \cdots s_K \, mod \, p. \end{aligned}$$

De donde

$$(-1)^K s! \equiv r_1 \cdots r_H s_1 \cdots s_K \ mod \ p \tag{4.5}$$

Por otro lado

$$\begin{aligned} s! a^s &\equiv (aR_1) \cdots (aR_H)(aS_1) \cdots (aS_K) \, mod \, p \\ s! a^s &\equiv r_1 \cdots r_H s_1 \cdots s_K \, mod \, p \end{aligned} \tag{4.6}$$

Igualando las ecuaciones (4.5) y (4.6) tenemos

$$s! a^s \equiv (-1)^K \ mod \ p$$

Como $1, 2, \cdots, s$ son primos relativos con p, tenemos $(s!, p) = 1$ y por lo tanto podemos cancelar $s!$ en la ecuación anterior, luego

$$a^s \equiv (-1)^K \ mod \ p.$$

Por lo tanto

$$\left(\frac{a}{p}\right) \equiv (-1)^K \ mod \ p$$

♠

Ejemplo:

Usar el lema de Gauss para calcular $\left(\frac{5}{31}\right)$.

Tenemos que $s = \frac{31 - 1}{2} = 15$ y $\frac{p}{2} = 15.5$.

Sea $L = \{5, 2 \cdot 5, 3 \cdot 5, \ldots, 15 \cdot 5\}$, los residuos módulo 31 de los elementos de L son

$$\overline{L} = \{5, 10, 15, 20, 25, 30, 4, 9, 14, 19, 24, 29, 3, 8, 13\}.$$

Luego el conjunto de los elementos de $\overline{L}$ mayores que 15.5 viene dado por

$$A = \{19, 20, 24, 25, 29, 30\}$$

Tenemos entonces, que el número de elementos de A es igual a 6 y por lo tanto $K = 6$.Luego

$$\left(\frac{5}{31}\right) = (-1)^6 = 1$$

A fin de simplificar las demostraciones introduciremos las siguientes notaciones

$$A = r_1 + r_2 + \cdots r_H \tag{4.7}$$

$$B = s_1 + s_2 + \cdots s_K,$$

con $H + K = s$ y $s = \dfrac{(p-1)}{2}$

$$M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{sa}{p}\right] \tag{4.8}$$

Lema 4.2.1 *Con las notaciones anteriores se tiene*

$$\frac{(a-1)(p^2-1)}{8} = (M - K)p + 2B.$$

Demostración:

Usando las mismas notaciones del teorema 4.2.3 tenemos:

$$R_i a = p\left[\frac{R_i a}{p}\right] + r_i$$

$$S_j a = p\left[\frac{S_j a}{p}\right] + s_j.$$

Luego

$$\begin{aligned}\sum_{i=1}^{s} ia &= \sum_{i=1}^{H} R_i a + \sum_{j=1}^{K} S_j a \\ &= p\sum_{i=1}^{H}\left[\frac{R_i a}{p}\right] + \sum_{i=1}^{H} r_i + p\sum_{j=1}^{K}\left[\frac{S_j a}{p}\right] + \sum_{j=1}^{K} sj\end{aligned}$$

Después de agrupar los términos en p, y utilizar las fórmulas en (4.1), nos queda

$$\sum_{i=1}^{s} ia = pM + A + B.$$

Por otro lado

$$\sum_{i=1}^{s} i = \frac{s(s+1)}{2} = \frac{p^2-1}{8}, \tag{4.9}$$

luego se tendrá

$$\frac{a(p^2-1)}{8} = pM + A + B. \tag{4.10}$$

De acuerdo a la demostración del teorema 4.2.3, se deduce

$$\begin{aligned}\sum_{i=1}^{s} i &= \sum_{i=1}^{H} r_i + \sum_{j=1}^{K} p - s_j \\ &= A + Kp - B.\end{aligned}$$

Luego, podemos usar la ecuación anterior y (4.2), para obtener

$$\frac{p^2-1}{8} = A + Kp - B. \tag{4.11}$$

Restando (4.4) de (4.3) queda

$$\frac{(a-1)(p^2-1)}{8} = (M-K)p + 2B,$$

con lo cual terminamos la demostración ♠

En el desarrollo de la prueba del lema anterior se obtuvo el siguiente resultado (ver ecuación 4.11).

Lema 4.2.2 *Si $p \neq 2$ es primo, entonces*

$$\frac{p^2-1}{8}$$

es un entero.

El siguiente lema permite calcular el símbolo de Legendre $\left(\frac{a}{p}\right)$, para el caso especial $a = 2$.

Lema 4.2.3

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

Demostración:

Haciendo $a = 2$ en (4.9), se tiene

$$\frac{p^2-1}{8} = (M-K)p + 2B.$$

Podemos calcular el valor de M, directamente de la definición

$$M = \left[\frac{2}{p}\right] + \left[\frac{4}{p}\right] + \cdots + \left[\frac{s2}{p}\right].$$

Obsérvese ahora, que cada uno de los términos que aparece dentro de los corchetes son mayores de cero y menores que uno, luego podemos concluir: $M = 0$.

Por lo tanto

$$\begin{aligned} \frac{p^2-1}{8} &= -Kp + 2B \\ &\equiv -Kp \, mod \, 2 \\ &\equiv K \, mod \, 2. \end{aligned}$$

Finalmente, usando el lema de Gauss se obtiene

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

Con esto terminamos la demostración. ♠

Ejemplo:

Calcular $\left(\frac{2}{13}\right)$.

Solución:

$$\left(\frac{2}{13}\right) = (-1)^{169-1)/2} = (-1)^2 1 = -1.$$

Seguidamente, damos una fórmula para obtener el símbolo de Legendre $\left(\frac{q}{p}\right)$, donde q es primo ($q \neq p \quad , \quad q \neq 2$).

Teorema 4.2.4 *Sean p y q dos números primos diferentes. Entonces*

$$\left(\frac{q}{p}\right) = (-1)^M,$$

donde

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots \left[\frac{sq}{p}\right].$$

Demostración:

Tomando $a = q$ en el lema (4.2.3), se tiene

$$\frac{(q-1)(p^2-1)}{8} = (M-K)p + 2B.$$

Por ser q impar y $(p^2-1)/8$ entero, se deduce de lo anterior

$$(M-K)p \equiv 0 \ mod\ 2.$$

Usando el hecho $(p, 2) = 1$, obtenemos

$$M \equiv k \ mod\ 2.$$

Combinando esta útima ecuación con el lema de Gauss se deduce el resultado

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

♠

Observación: Si en la ecuación anterior, se intercambian p y q obtenemos

$$\left(\frac{p}{q}\right) = (-1)^N,$$

donde

$$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{tp}{q}\right]$$

$t = (q-1)/2$.

El resultado siguiente es clave para la demostración de la Ley de Reciprocidad Cuadrática.

Lema 4.2.4 *Con las notaciones anteriores se tiene*

$$M + N = s.t.$$

Demostración:

La idea de la demostración es de tipo geométrico, y se debe a Einsenstein, un discípulo de Gauss.

Consideramos un sistema de coordenadas cartesianas en el plano, y sean los puntos $O = (0, 0)$, $A = (p/2, 0)$, $B = (0, q/2)$ y $C = (p/2, q/2)$.

Sea L el conjunto de puntos de coordenadas enteras, dentro del rectángulo $\square OACB$ (ver el diagrama).

Afirmamos que no hay puntos de L sobre la diagonal. La ecuación de la misma esta dada por:

$$py = qx$$

Si (x_1, y_1) es un punto L sobre la diagonal, se cumple $py_1 = qx_1$, lo cual implica que p divide a x_1. Esto es una contradicción pues $1 \leq x_1 < p/2$. Por lo tanto la afirmación es válida.

A continuación contaremos el número de puntos de L, el cual será denotado por ℓ, de dos formas distintas:

Forma I): Sea ℓ = puntos dentro del triángulo $\triangle OAC$+ puntos localizados dentro del triángulo $\triangle OBC$.

Sea λ_r, $1 \leq r \leq s$, el número de puntos de L dentro del triángulo $\triangle OAC$ y sobre la línea $x = r$, luego es fácil ver que

$$\lambda_r = \left[\frac{rq}{p}\right] \quad , \quad 1 \leq r \leq s.$$

Si sumamos sobre r obtenemos:

$$\text{puntos dentro del triángulo } \triangle OAC = \sum_{r=1}^{s} \lambda_r = M.$$

De la misma forma se demuestra:

$$\text{puntos dentro del triángulo } \triangle OBC = N.$$

Luego

$$\ell = M + N.$$

Forma II): Por otro lado, viendo a L como un rectángulo se tiene:

$$\ell = \text{puntos en la base} \times \text{puntos en la altura} = s \cdot t.$$

Comparando ambos resultados, se deduce

$$M + N = s \cdot t.$$

♠

Teorema 4.2.5 *(Ley de Reciprocidad Cuadrática) Sean p y q dos primos impares distintos, entonces*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}} \tag{4.12}$$

Demostración:

En el teorema 4.2.5 hemos probado

$$\left(\frac{q}{p}\right) = (-1)^M \quad \text{y} \quad \left(\frac{p}{q}\right) = (-1)^N.$$

De esto se sigue

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{st} \quad 4.11,$$

lo cual nos conduce al resultado deseado, al hacer la sustitución

$$s = \frac{p-1}{2} \quad \text{y} \quad t = \frac{q-1}{2}$$

♠

Observación : La Ley de Reciprocidad Cuadrática puede ser escrita de otra manera. Podemos multiplicar la ecuación (4.12) por $\left(\frac{q}{p}\right)$ para obtener

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

Ejemplo:

Calcular $\left(\frac{13}{37}\right)$, usando la Ley de Reciprocidad Cuadrática.

Solución:

Denotemos por LRC="Ley de Reciprocidad Cuadrática".

$$\begin{aligned}\left(\frac{13}{37}\right) &= (-1)^{\frac{13-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{13}\right) \quad \text{(por LRC)} \\ &= \left(\frac{37}{13}\right) \\ &= \left(\frac{11}{13}\right),\end{aligned}$$

pero

$$\begin{aligned}\left(\frac{11}{13}\right) &= (-1)^{\frac{11-1}{2}\cdot\frac{13-1}{2}}\left(\frac{13}{11}\right) \quad \text{(por LRC)}\\ &= \left(\frac{13}{11}\right)\\ &= \left(\frac{2}{11}\right)\\ &= (-1)^{(11^2-1)/8} \quad \text{por} \quad (4.11)\\ &= (-1)^{15}\\ &= -1.\end{aligned}$$

Ejemplo:

Decidir si la congruencia

$$x^2 \equiv 5 \; mod \; 227,$$

es soluble.

Solución:

La congruencia será soluble si y sólo si 5 es un resto cuadrático módulo 227; si sólo si

$$\left(\frac{5}{227}\right) = 1.$$

Evaluando este símbolo, tenemos

$$\begin{aligned}\left(\frac{5}{227}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{227-1}{2}}\left(\frac{227}{5}\right)\\ &= \left(\frac{227}{5}\right)\\ &= \left(\frac{2}{5}\right)\\ &= (-1)^{(5^2-1)/8}\\ &= -1.\end{aligned}$$

Concluimos entonces que la ecuación no es soluble.

4.3 Símbolo de Jacobi

El símbolo de Legendre $\left(\frac{a}{p}\right)$, se define únicamente para p, un número primo. En esta sección, daremos una generalización de este símbolo, en donde el "denominador" p, puede ser un número compuesto.

Definición 4.3.1 *Sean a y b dos enteros primos relativos, y además b tiene descomposición como producto de primos $b = p_1 \cdot p_2 \cdots p_n$, donde los p_i no son necesariamente distintos. Entonces el* **símbolo de Jacobi** $\left(\frac{a}{b}\right)$, *se define por*

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n} \left(\frac{a}{p_i}\right),$$

donde $\left(\frac{a}{p_i}\right)$ es el símbolo de Legendre.

Ejemplo:

$$\left(\frac{7}{15}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right)$$

Observación: Si p es un número primo, entonces el símbolo de Jacobi y el símbolo de Legendre, cuando p va en la parte inferior, son indistinguibles.

Observación: Si b es compuesto, entonces la notación $\left(\frac{a}{b}\right) = 1$, no implica necesariamente que a sea un resto cuadrático módulo b.

Por ejemplo $\left(\frac{5}{9}\right) = 1$, pero no existe x tal que $x^2 \equiv 5 \ mod\ 9$.

El símbolo de Jacobi goza de muchas propiedades similares a las del símbolo de Legendre.

Teorema 4.3.1 *Sean a, b, c y d enteros tales que $(a, c) = 1$. Entonces*

1) $\left(\frac{a}{b}\right)\left(\frac{a}{d}\right) = \left(\frac{a}{bd}\right)$

2) $\left(\frac{a}{b}\right)\left(\frac{c}{b}\right)=\left(\frac{ac}{b}\right)$

3) $\left(\frac{a^2}{b}\right)=1$

4) $\left(\frac{a}{b^2}\right)=1$

5) $\left(\frac{ac^2}{b}\right)=\left(\frac{a}{b}\right)$

Demostración:

Ejercicio.

♠

Teorema 4.3.2 *Si b es impar positivo, se cumple:*

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

Demostración:

En efecto, sea $b = p_1 \cdot p_2 \cdots p_n$. Usando la definición del símbolo de Jacobi se tiene

$$\begin{aligned}\left(\frac{2}{b}\right) &= \prod_{i=1}^{n}\left(\frac{2}{p_i}\right)\\ &= \prod_{i=1}^{n}(-1)^{(p_i^2-1)/8}\\ &= (-1)^{\alpha},\end{aligned}$$

donde $\alpha = \sum_{i=1}^{n}(p_i^2-1)/8$.

Para nuestros propósitos, será suficiente conocer el valor de α módulo 2. Observar que si p_1 y p_2 son primos, entonces

$$\begin{aligned}\frac{p_1^2p_2^2-1}{8}-\left[\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}\right] &= \frac{(p_1^2-1)(p_2^2-1)}{8}\\ &\equiv 0\, mod\, 2.\end{aligned}$$

Luego

$$\frac{p_1^2p_2^2-1}{8}\equiv\left(\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}\right)\, mod\, 2.$$

Aplicando esta última identidad a los restantes primos p_i, nos da

$$\frac{\prod_{i=1}^n p_i^2-1}{8}\equiv\sum_{i=1}^n\frac{(p_i^2-1)}{8}\equiv\ mod\ 2.$$

Por lo tanto concluimos

$$\alpha\equiv\ \frac{\prod_{i=1}^n p_i^2-1}{8}\ mod\ 2,$$

esto es

$$\alpha\equiv\ \frac{b^2-1}{8}\ mod\ 2,$$

de donde se obtiene

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

♠

Seguidamente, pasamos a ver la Ley de Reciprocidad Cuadrática, para el símbolo de Jacobi.

Teorema 4.3.3 *Si a y b son enteros positivos impares primos entre sí, se tiene*

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

Demostración:

Supongamos que $a = p_1 \cdot p_2 \cdot p_n$, y $b = q_1 \cdot q_2 \cdots q_m$, entonces

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{m}\left(\frac{a}{q_i}\right)\prod_{j=1}^{n}\left(\frac{b}{p_j}\right) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}(-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} \\ &= (-1)^{\beta},\end{aligned}$$

donde

$$\begin{aligned}\beta &= \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{p_j-1}{2}\cdot\frac{q_i-1}{2} \\ &= \left[\sum_{j=1}^{n}\frac{p_j-1}{2}\right]\left[\sum_{i=1}^{m}\frac{q_i-1}{2}\right]\end{aligned}$$

Interesa entonces calcular el valor de β módulo 2, para lo cual

$$\frac{p_1p_2-1}{2} - \left\{\left[\frac{p_1-1}{2}\right] + \left[\frac{p_2-1}{2}\right]\right\} = \frac{(p_1-1)(p_2-1)}{2} \equiv 0\, mod\, 2,$$

luego

$$\frac{p_1p_2-1}{2} \equiv \frac{(p_1-1)}{2} + \frac{(p_2-1)}{2}\ mod\ 2.$$

Haciendo uso de esta última congruencia, tantas veces como se requiera, produce

$$\frac{p_1p_2\cdots p_n-1}{2} \equiv \sum_{i=1}^{n}\frac{p_i-1}{2}\ mod\ 2.$$

o sea

$$\frac{a-1}{2} \equiv \sum_{i=1}^{n}\frac{(p_i-1)}{2}\ mod\ 2.$$

De igual forma, se obtiene un resultado análogo para b.

$$\frac{b-1}{2} \equiv \sum_{i=1}^{n} \frac{(q_j-1)}{2} \ mod\ 2.$$

Por lo tanto

$$\beta \equiv \frac{(a-1)}{2} \cdot \frac{(b-1)}{2} \ mod\ 2,$$

y con esto finaliza la demostración. ♠

Ejercicios

1) Calcular

$$i)\left(\frac{5}{37}\right) \quad ii)\left(\frac{2}{37}\right) \quad iii)\left(\frac{10}{37}\right) \quad iv)\left(\frac{100}{101}\right) \quad v)\left(\frac{50}{13}\right)$$

2) Determinar cuáles de las siguientes congruencias tienen solución:

i) $x^2 \equiv -2 \ mod\ 59$

ii) $x^2 \equiv 2 \ mod\ 59$

iii) $x^2 \equiv -2 \ mod\ 41$

iv) $x^2 \equiv 2 \ mod\ 37$

v) $x^2 \equiv 2 \ mod\ 101$

3) Demostrar que para todo primo p se tiene:

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0.$$

4) Demuestre que si las ecuaciones $x^2 \equiv a \ mod\ p$ y $x^2 \equiv b \ mod\ p$ no son solubles, entonces $x^2 \equiv ab \ mod\ p$ es soluble.

5) Probar que $x^2 \equiv 2 \ mod\ p$ es soluble ($p \neq 2$), si y sólo si $p \equiv 1 \text{ ó } 7 \ mod\ 8$.

6) Si p es primo, $p \neq 2$. Probar $p^4 - 1 \equiv 0 \ mod\ 16$.

7) Sea $\mathcal{A}$ = conjunto de restos cuadráticos $mod\, p$ y $\mathcal{B}$ = al conjunto de restos no cuadráticos $mod\, p$. Probar:

i) aa' está en $\mathcal{A}$, para todo a y a' en $\mathcal{A}$.

ii) bb' está en $\mathcal{A}$, para todo b y b' en $\mathcal{B}$.

iii) ab está en $\mathcal{B}$, para todo a en $\mathcal{A}$ y b en $\mathcal{B}$.

8) Usando el problema anterior, demostrar $\|\mathcal{A}\| = \|\mathcal{B}\| = (p-1)/2$.

9) Probar

$$\prod_{i=1}^{p-1}\left(\frac{i}{p}\right) = \begin{cases} -1, & \text{si } p \equiv 1 \ mod\ 4, \\ 1, & \text{si } p \equiv 3 \ mod\ 4. \end{cases}$$

10) Usando la Ley de Reciprocidad Cuadrática, decidir cuáles de las siguientes ecuaciones tienen solución:

i)$x^2 \equiv 15 \ mod\ 103$

ii)$x^2 \equiv 20 \ mod\ 167$

iii)$x^2 \equiv -6 \ mod\ 157$

iv)$x^2 \equiv 8 \ mod\ 479$.

11) Probar que si $p \equiv 1 \ mod\ 4$, entonces

$$x^2 \equiv p \ mod\ q \text{ es soluble si y sólo si } x^2 \equiv q \ mod\ p \text{ lo es}$$

12) Usando el ejercicio 11) demuéstrese que si $p \equiv 1 \ mod\ 10$, entonces

$$\left(\frac{10}{p}\right) = 1.$$

13) Probar el recíproco del teorema de Wilson:
"Si $(p-1)! \equiv -1 \ mod\ p$, entonces p es primo".

14) Demuéstrese el teorema 4.3.1

15) Para cuáles primos p la congruencia:

$$x^2 \equiv -1 \ mod\ p$$

es soluble.

16) Mostrar que si p y q son dos primos diferentes de dos, entonces

$$\frac{(p^2-1)(q^2-1)}{8} \ \equiv \ 0 \ mod\ 2.$$