La ley de reciprocidad cuadrática. una breve revisión histórica

Edwin León Cardenal
Estudiante Universidad Nacional de Colombia
Bogotá D.C, Colombia
eleonc@unal.edu.co

Resumen

La Ley de Reciprocidad Cuadrática es uno de los resultados más útiles y prolíficos en Teoría de Números. Desde que fue enunciada por Euler en 1754, ha sido materia de interesantes desarrollos.
Este escrito pretende hacer una breve reconstrucción histórica de los pasos que condujeron a la formulación y posterior demostración de la Ley de Reciprocidad Cuadrática. Además de exponer una demostración, hacemos un recuento de algunos desarrollos posteriores y generalizaciones a que ha dado lugar este resultado.

1. Introducción

La Ley de Reciprocidad Cuadrática fue enunciada por primera vez por *Euler* en 1754-55, esencialmente en los siguientes términos:
"Si existe un x tal que $x^2 - p$ es divisible por q, entonces p se dice un residuo o resto cuadrático de q. Si no existe tal x , p se dice un no resto cuadrático de q".

La Ley de Reciprocidad Cuadrática tiene dos partes:

a) Si alguno de los dos, p o q, es de la forma $4k+1$, entonces p es un residuo cuadrátrico de q si y solo si q es un resto cuadrático de p.

b) Si ambos, p y q son de la forma $4k+3$, entonces p es un residuo cuadrático de q si y solo si q es un no resto cuadrático de p."

2. El trabajo de *Euler*

Inspirado en el trabajo de *Fermat* sobre los primos de la forma $p = x^2 + Ny^2$ con x,$y \in \mathbf{Z}$ para $N = 1, \pm 2, 3$, *Euler* trabajando en formas cuadráticas encuentra los dos problemas siguientes:

I) Dado $n \in \mathbb{Z}$, describa los primos $p \neq 2$ para los cuales $p = x^2 + Ny^2$ es soluble con x,$y \in \mathbb{Z}$.

El segundo de los problemas es una forma mas débil del primero

II) Dado $N \in \mathbb{Z}$,describa los primos $p \neq 2$ para los cuales $p \mid m$, donde m es un entero de la forma $m = x^2 + Ny^2$, con x,$y \in \mathbb{Z}$.

Usando el símbolo de *Legendre*, el problema II queda en estos términos:
Dado $N \in \mathbb{Z}$ y p un primo tal que $(N,p)=1$. ¿ Cuáles son los primos $p \neq 2$, para los que $\left(\frac{-N}{p}\right)=1$?

Definición 1. $P_N := \{primosp \neq 2 : \left(\frac{-N}{p}\right)=1\}$

En estos términos el problema II sería:

Dado $N \in \mathbb{Z}$ describa P_N

Las observaciones de *Euler* y $Fermat$, muestran que los primos $p \in P_N$ pueden ser descritos mediante condiciones de congruencia módulo $4|N|$. Los primeros descubrimientos fueron hechos por $Fermat$ para $N = 1, 2, 3$. Sin embargo,Fermat no dio ninguna prueba de estos hechos.
El caso $N = 1$ fue probado por *Euler* en 1758 junto con una prueba del recíproco. Para $N = 2$ y $N = 3$ *Euler* también dio pruebas satisfactorias y estableció que el recíproco también era cierto, pero estos hechos fueron ambos demostrados por *Lagrange* en 1775.
Entre 1741 y 1742 en *Theoremata circa divisores numerorum in hac porma* $pa^2 \pm qb^2$ *contentorum* , *Euler* establece la *Primera o Forma Implícita* de la Ley de Reciprocidad Cuadrática :

Teorema 1. *Dado $N \in \mathbb{Z}$ y p un primo con $(p, 2N) = 1$. Entonces se tienen las siguientes propiedades:*

1) $p \in P_N$ si y solo si $p \in 4|N|\mathbb{Z} + r =: C(r)$ para ciertos residuos $r \in \mathbb{N}$ módulo $4|N|$ con $0 < r < 4|N|$ y $(r, 4N) = 1$.

Mas precisamente, si:

$R_N := \{C(r) \cap P_N \neq \emptyset, 0 < r < 4|N|\}$ y $E_N := (\mathbb{Z}/4|N|\mathbb{Z})^\times$ es el grupo de unidades módulo $4|N|$.

Entonces:

2) R_N es un subgrupo de E_N de índice [$E_N : R_N$=2].

3) Si $\bar{p} = \bar{r}^2$ para algún $\bar{r} \in E_N$, entonces $\bar{p} \in R_N$

4) $\overline{-1} \in R_N$ si y solo si $N < 0$

5) Si $N = 4n - 1$, entonces P_N está caracterizado por las condiciones de congruencia módulo $|N|$. Si $N \neq 4n - 1$, entonces P_N está caracterizado por las condiciones de congruencia módulo $4|N|$, pero no $|N|$

6) Excepto para $4|N|$ y $|N|$ (si $N = 4n - 1$) no existe otro módulo $m \in \mathbb{N}$ que caracterize a P_N.

Aunque esta *Primera Forma* brinda una completa descripción de la estructura de R_N, no ofrece una descripción explicita, ni de R_N ni de P_N. Por ejemplo, para $N = 2$:
$E_N = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$
y para R_N, tenemos tres posibilidades :
$R_N = \{\bar{1}, \bar{3}\}$ ó $\{\bar{1}, \bar{5}\}$ ó $\{\bar{1}, \bar{7}\}$,
por 4) podemos excluir $\{\bar{1}, \bar{7}\}$, pero no es posible decidir entre $R_N = \{\bar{1}, \bar{3}\}$ y $R_N = \{\bar{1}, \bar{5}\}$.

Experimentalmente, Euler y Fermat determinaron que $R_2 = \{\bar{1}, \bar{3}\}$ y $R_{-2} = \{\bar{1}, \bar{7}\}$.
Los casos $N = 1$ y $N = -2$, que fueron probados por *Euler*, son respectivamente la primera y la segunda ley complementarias de la Ley de Reciprocidad Cuadrática, veamos:

Teorema 2. *(1)* $R_1 = \{\bar{1}\}$, *es decir* $p \mid x^2 + y^2 \Leftrightarrow p = 4n + 1$

(2) $R_{-2} = \{\bar{1}, \bar{7}\}$, *es decir* $p \mid x^2 - 2y^2 \Leftrightarrow p = 8n + 1$ *o* $p = 8n - 1$

Más tarde, en 1772, *Euler* enuncia la *Segunda o Forma explícita* de la Ley de Reciprocidad Cuadrática, publicada en *Opuscula Analytica (1783)*

Teorema 3. *Sean p y q dos primos impares y distintos:*

(1) Si $p = 4n + 1$ *entonces* $p \mid x^2 - qy^2 \Leftrightarrow q \mid x^2 - py^2$

(2) Si $p = 4n + 3$ *entonces* $p \mid x^2 - qy^2 \Leftrightarrow q \mid x^2 + py^2$

En términos del símbolo de *Legendre* :

(1*) Si $p = 4n + 1$ entonces $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

(2*) Si $p = 4n + 3$ entonces $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$

3. Un intento fallido

Adrien Marie Legendre (1752-1833) fue otro de los pioneros en el estudio de la Ley de Reciprocidad Cuadrática, de hecho fue el primero en dar una demostración (parcial). Basado en el trabajo de *Euler* y usando el siguiente lema, *Legendre* distingue 8 casos que dependen de la congruencia $p, q \equiv \pm 1 \pmod 4$ y de $\left(\frac{p}{q}\right) = \pm 1$.

Lema 1. *Sean a,b,c* $\in \mathbb{Z}$ *no todos del mismo signo y tales que abc es un cuadrado libre. Entonces* $ax^2 + by^2 + cz^2 = 0$ *tiene una solución entera no trivial* $x,y,z \in \mathbb{Z}$ *si y solo si las siguientes tres condiciones se satisfacen simultáneamente:*

a) $-bc$ *es un residuo cuadrático módulo* $|a|$,

b) $-ca$ *es un residuo cuadrático módulo* $|b|$,

c) $-ab$ *es un residuo cuadrático módulo* $|c|$.

La prueba de *Legendre*, publicada en *Essai sur la Théorie des Nombres (1798)*, hace uso de ecuaciones como $x^2 + py^2 - qz^2 = 0$ (una para cada caso). A continuación considera las soluciones enteras módulo 4 y así dos de las tres condiciones establecidas en el lema anterior se satisfacen, mientras que la tercera no, lo que dá lugar a la Ley de Reciprocidad.

En términos del símbolo de *Legendre*, introducido por el mismo en 1798, tenemos:

Teorema 4. *Sean* p *y* q *primos impares distintos y* $q = 4m + 3$

1) Si $p = 4n + 1$ *y* $\left(\frac{p}{q}\right) = -1$ *entonces* $\left(\frac{q}{p}\right) = -1$

2) Si $p = 4n + 3$ *y* $\left(\frac{p}{q}\right) = 1$ *entonces* $\left(\frac{q}{p}\right) = -1$

Se dice que está demostración es parcial pues en ella se hace uso de un teorema que fué probado hasta 1837 por *Dirichlet*, que afirma que dada una progresión aritmética de módulo m y razón fija r, siempre es posible encontrar un número primo en ella. Al parecer este hecho fue tomado por *Legendre* como un axioma.

4. La primera prueba

El primero en ofrecer una demostración completa de la Ley de Reciprocidad Cuadrática fue *Gauss* en 1796, prueba que aparece publicada en *Disquisitiones Aritmeticae (1881)*, esta primera prueba consideraba también 8 casos y usaba inducción.

Gauss realizó 7 pruebas más, dos de ellas publicadas póstumamente. Es notable la admiración que desperto en *Gauss* este resultado, pues llegó a denominarlo el *Theorema Aureum* (Teorema áureo).

Las pruebas de *Gauss*, usan desde inducción hasta el *genus* de las formas cuadráticas y sumas de Gauss, así como las extensiones ciclotómicas.

5. Nuestraprueba

Uno de los alumnos de *Gauss*, *Gotthold Eisenstein*, aporto cinco demostraciones más. Con el propósito de exponer una de estas pruebas enunciaremos dos proposiciones (sin demostración), una de ellas es el lema de *Gauss*, que fue publicado en 1801, la otra proposición fue enunciada por *Eisenstein* y es el punto clave de la prueba que de el exhibiremos.

Proposición 1. ***(Lema de Gauss)***
Sea p *un primo impar y* D *un entero no divisible por* p. *Si* μ *denota el número de enteros en la secuencia*

$$1 \cdot D, 2 \cdot D, \ldots, \tfrac{1}{2}(p-1) \cdot D, \tag{1}$$

cuyos residuos principales módulo p *son mayores que* $\frac{1}{2}p$, *entonces*

$$\left(\frac{D}{p}\right) = (-1)^{\mu} \tag{2}$$

Proposición 2. *Sean a y b dos enteros impares mayores que 3. Si $(a,b)=1$, tenemos:*

$$\sum_{u=1}^{\frac{1}{2}(a-1)} \left[\tfrac{bu}{a}\right] + \sum_{v=1}^{\frac{1}{2}(b-1)} \left[\tfrac{av}{b}\right] = \tfrac{1}{2}(a-1)\tfrac{1}{2}(b-1). \tag{3}$$

Teorema 5. ***(Ley de Reciprocidad Cuadrática)***
Si p y q son dos primos impares distintos, tenemos:

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

Demostración. Por el *Lema de Gauss* tenemos $\left(\frac{q}{p}\right) = (-1)^M$, donde

$M \equiv \mu \pmod 2$ y $M = \sum_{u=1}^{\frac{1}{2}(p-1)} \left[\frac{qu}{p}\right]$. Intercambiando los papeles de p y de q, tendremos $\left(\frac{p}{q}\right) = (-1)^N$ donde $N = \sum_{v=1}^{\frac{1}{2}(q-1)} \left[\frac{pv}{q}\right]$.
Por tanto $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N}$. Usando la proposición 2 concluimos:
$M+N = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$. Con lo cual concluimos el resultado. □

6. Algunas generalizaciones

Finalmente cabe anotar que muchos otros grandes matemáticos han contribuido con sus propias pruebas a la larga historia de este resultado. Entre ellos *Cauchy, Jacobi, Dirichlet, y Lebesgue*. Actualmente existen más de 150 pruebas.

La Ley de Reciprocidad Cuadrática ha sido el fundamento para las denominadas *Leyes de Reciprocidad Superiores*, que comprenden entre otras, la Ley de Reciprocidad Cúbica y la Ley de Reciprocidad Bicuadrática o Cuártica. Estas leyes también ocuparon el tiempo de grandes como *Euler, Gauss,Jacobi* , y de nuevo, *Eisenstein*, entre otros.
A manera de ejemplo enunciaremos la Ley de Reciprocidad Cúbica.

Teorema 6. *Sean π_1 y π_2 primarios, es decir primos en $\mathbb{Z}(-1+\sqrt{-3}/2)$ que son congruentes con 2 módulo 3. Si $N\pi_1$,$N\pi_2 \neq 3$ y $N\pi_1 \neq N\pi_2$, entonces*

$$\chi_{\pi_1}(pi_2) = \chi_{\pi_2}(pi_1). \tag{5}$$

donde $\chi(\pi)$ denota el caracter cúbico de π.

Como es posible notar, este enunciado ha requerido de herramientas más elaboradas, las otras generalizaciones de la Ley de Reciprocidad Cuadrártica requieren igualmente un andamiaje cada vez mas sofisticado. Por ello nos limitaremos a nombrarlas. Algunas de ellas son : la ley de reciprocidad bicuadrática (cuártica), la ley de reciprocidad racional, propuesta por *Eisenstein* en 1850, y la generalización a extensiones abelianas finitas, debida a *Artin*.