Lecturas Matemáticas
Volumen **30** *(2009), páginas 17–27*
ISSN 0120–1980

La Gema de la Reina: Una breve revisión histórica de la ley de reciprocidad cuadrática

Edwin León Cardenal
Universidad Nacional de Colombia, Bogotá, Colombia

Abstract. Quadratic reciprocity law is one of the most useful and fruitful theorems in number theory. It was stated in 1754 by Euler and proven by the first time by Gauss in 1796. In this work we make a brief historical reconstruction of the steps behind the formulation and later proof of this remarkable result.

Key words and phrases. History of Mathematics, quadratic reciprocity law, Legendre symbol.

2000 AMS Mathematics Subject Classification. 01A55, 1103.

Resumen. La ley de reciprocidad cuadrática es uno de los resultados más útiles y prolíficos en teoría de números. Fue enunciada por Euler en 1754 y fue probada por primera vez por Gauss en 1796. En este trabajo hacemos una breve reconstrucción histórica de los pasos conducentes a la formulación y posterior demostración de este magnífico resultado.

1. Introducción

La ley de reciprocidad cuadrática es uno de los resultados más útiles y prolíficos de la teoría de números. Desde que fue enunciada (explícitamente) en 1772 por Euler ha sido materia de estudio de numerosos personajes. Se puede afirmar que la teoría de números moderna comenzó con el descubrimiento de la ley de reciprocidad cuadrática. En este documento ilustramos al lector sobre algunos de los pasajes más relevantes de esta interesante historia.

Empezaremos con algunas definiciones pertinentes tales como la de resto cuadrático y la del símbolo de Legendre. Luego recordaremos parte de los trabajos de Diofanto, Fermat, Euler, Legendre, Gauss y Eisenstein en torno a la ley de reciprocidad cuadrática. En la parte final de este trabajo

presentamos una de las pruebas de este resultado obtenida por EISENSTEIN en 1845.

Definición 1.1. Si existe un x tal que $x^2 \equiv a \pmod{q}$, se dice que a es un **residuo** o **resto cuadrático** de q (o módulo q). Si no existe tal x, se dice que a no es un resto cuadrático de q.

En 1798 LEGENDRE, propone el siguiente símbolo para describir esta relación. Sea $a \in \mathbb{Z}$ y p un número primo impar, entonces

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{si } a \text{ es resto cuadrático módulo } p\ ; \\ 0, & \text{si } p \mid a\ ; \\ -1, & \text{si } a \text{ no es resto cuadrático módulo } p\ . \end{cases}$$

Dados p y q dos primos impares distintos, la ley de reciprocidad cuadrática (LRC de aquí en adelante) afirma que:

> Si p o q son de la forma $4k+1$, entonces p es un resto cuadrático de q si y sólo si q es un resto cuadrático de p. Si ambos, p y q son de la forma $4k+3$, entonces p es un resto cuadrático de q si y sólo si q no es un resto cuadrático de p.

En términos del símbolo de Legendre esto se expresa así:

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

Existen además dos leyes complementarias:

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{1}{2}(q-1)} \quad \text{y} \quad \left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}(q^2-1)}.$$

2. Diofanto (¿250 a.c.?)

En el problema XIV del libro 6 de la *Arithmetica* de DIOFANTO se prueba que la ecuación $x^2 + y^2 = 15$ no tiene soluciones enteras. Este hecho, elemental al considerar las posibilidades para x y y, se puede obtener también como consecuencia del siguiente teorema:

> Si a es un entero de la forma $4n+3$, la ecuación $a = x^2 + y^2$ no tiene soluciones enteras.

En particular, *si p es un primo de la forma $4n+3$, la ecuación $p = x^2 + y^2$ no tiene soluciones enteras.* O, de manera equivalente,

Teorema 2.1. *Si $p \neq 2$ y la ecuación $p = x^2 + y^2$ tiene soluciones enteras, entonces $p = 4n+1$ para algún $n \in \mathbb{Z}$.*

Veremos más adelante que usando el hecho de que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo para p primo (EULER 1775), se puede escribir el teorema 2.1 en la siguiente forma equivalente

Teorema 2.2. *Si $p \neq 2$ es un número primo y la ecuación $p = x^2 + y^2$ tiene soluciones enteras, entonces* $\left(\frac{-1}{p}\right) = 1$.

La equivalencia entre las conclusiones de los teoremas 2.1 y 2.2 es precisamente la primera ley complementaria de la LRC. Pero sólo en 1638 el teorema 2.1 es establecido explícitamente por Fermat. La primera ley complementaria fue enunciada explícitamente por Fermat en 1640 y probada por Euler en 1750.

3. **Fermat (1601-1665)**

Como sabemos, la lectura de la obra de Diofanto [Arithmetica, traducción de Bachet] condujo a Fermat a establecer métodos, teoremas y problemas de gran impacto en el desarrollo del universo matemático. Uno de tales teoremas es la primera ley complementaria de la LRC. En una carta a Mersenne de 1640 [5], anota:

> *Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypotenuse d'un triangle rectangle.*

Más adelante completaría esta afirmación y enunciaría orgullosamente dos teoremas más en el mismo sentido. En un lenguaje más moderno [3], los resultados son:

Teorema 3.1. $p = x^2 + y^2,\ x, y \in \mathbb{Z}$ *si y sólo si* $p \equiv 1 \pmod 4$.

Teorema 3.2. $p = x^2 + 2y^2,\ x, y \in \mathbb{Z}$ *si y sólo si* $p \equiv 1 \pmod 8$ *o* $p \equiv 3 \pmod 8$.

Teorema 3.3. $p = x^2 + 3y^2,\ x, y \in \mathbb{Z}$ *si y sólo si* $p \equiv 1 \pmod{12}$ *o* $p \equiv 7 \pmod{12}$.

Fermat probó la afirmación recíproca del teorema 3.1 mediante el método del descenso infinito. Una discusión bastante interesante sobre este método y sobre el testamento matemático de Fermat se puede encontrar en [1] y en [2]. La implicación del teorema 3.1 fue probada en 1750 por Euler, en 1774 el mismo Euler probó la implicación del teorema 3.2 y un recíproco parcial para $p = 8n + 1$, el recíproco para $8n + 3$ fue probado por Legendre en 1775. Euler también probó la implicación del teorema 3.3 en 1758 y estableció el recíproco en 1759 pero este sólo sería probado hasta 1775 por Legendre.

En terminología actual, una condición necesaria para que un número primo p se pueda representar como $p = x^2 + Ny^2$, con $N \in \mathbb{Z}$ y $x, y \in \mathbb{N}$ es que $\left(\frac{-N}{p}\right) = 1$ [6]. Así que el teorema 3.1 corresponde a la primera ley complementaria de la LRC, mientras que los teoremas 3.2 y 3.3 son casos particulares del teorema general.

4. **Euler (1707-1783)**

Muchas de las investigaciones aritméticas de FERMAT permanecen inexploradas luego de su muerte en 1665. En particular, las ideas sobre los primos de la forma $p = x^2 + Ny^2$, con $x, y \in \mathbb{Z}$ ($N = 1, 2, 3$), aguardan hasta 1741 por la intervención de EULER, quien inspirado por el trabajo de FERMAT plantea el siguiente problema:

> Dado $N \in \mathbb{Z}$, describir los primos $p \neq 2$ para los cuales $p = x^2 + Ny^2$ es soluble con $x, y \in \mathbb{Z}$.

Definición 4.1. $p \mid x^2 + Ny^2$ si existen $a, b \in \mathbb{Z}$ con $(a, b) = 1$ tales que $p \mid a^2 + Nb^2$.

Mediante esta definición EULER debilita el problema anterior y se propone resolver el siguiente problema:

> Dado $N \in \mathbb{Z}$, describir 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 $x, y \in \mathbb{Z}$.

La solución a este último problema es precisamente la ley de reciprocidad cuadrática, pues $p \mid Q(x, y) = x^2 + Ny^2 \Leftrightarrow$ existen $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ y $p = a^2 + Nb^2 \equiv 0 \pmod{p} \Leftrightarrow ab^{-1}$ es solución de $x^2 \equiv -N \pmod{p} \Leftrightarrow \left(\frac{-N}{p}\right) = 1$.

Definición 4.2. $P_N := \{\text{primos } p \neq 2 \ ; \ p \mid x^2 + Ny^2\} = \{\text{primos } p \neq 2 \ ; \ \left(\frac{-N}{p}\right) = 1\}$.

Usando esta definición el problema anterior consiste en describir P_N, dado $N \in \mathbb{Z}$.

Las observaciones de FERMAT y EULER, muestran que los primos en P_N pueden ser descritos mediante condiciones de congruencia módulo $4|N|$. Experimentalmente EULER observó que los divisores primos de la forma cuadrática $x^2 + Ny^2$ son precisamente aquellos que pertenecen a cierto número de progresiones aritméticas

$$C(r) = \{r, 4|N| + r, 8|N| + r, 12|N| + r, \ldots\},$$

donde r es primo con $4|N|$ y $0 < r < 4|N|$.

El conjunto de clases de congruencia módulo $4|N|$ determinado por los enteros r para los cuales $C(r)$ tiene la propiedad de que $-N$ es un resto cuadrático se denomina R_N. Más precisamente, en 1741 EULER establece el siguiente teorema (Primera Forma o Forma Implícita de la LRC):

Teorema 4.1. *Dado $N \in \mathbb{Z}$ y p un primo con $(p, 2N) = 1$. Se tiene que $p \in P_N$ si y sólo si $p \in C(r) := 4|N|\mathbb{Z} + r$ para ciertos residuos r módulo $4|N|$ con $0 < r < 4|N|$ y $(r, 4N) = 1$.*

De hecho, si $R_N := \{\bar{p}; p \in P_N\} = \{C(r) \cap P_N \neq \emptyset; 0 < r < 4|N|\}$ y $E_N := (\mathbb{Z}/4|N|\mathbb{Z})^\times$ es el grupo de unidades módulo $4|N|$. Entonces [Véase [6], página 72.]:

Teorema 4.2. *R_N está caracterizado por las siguientes propiedades:*

1. *R_N es un subgrupo de E_N de índice $[E_N : R_N = 2]$.*
2. *Si $\bar{p} = \bar{r}^2$ para algún $\bar{r} \in E_N$, entonces $\bar{p} \in R_N$.*
3. *$\overline{-1} \in R_N$ si y sólo si $N < 0$.*

Además se tiene que 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 $|N|$. Por lo que se concluye que $4|N|$ y $|N|$ son los únicos módulos que caracterizan a P_N.

Aunque esta *Primera Forma* brinda una buena descripción de la estructura de R_N, no ofrece una descripción explícita, ni de R_N ni de P_N. Por ejemplo, para $N = 2$, $E_N = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Como $\bar{1}^2 = \bar{1}$ entonces $\bar{1} \in R_N$, luego se tienen tres posibilidades para R_N. $R_N = \{\bar{1}, \bar{3}\}$ ó $\{\bar{1}, \bar{5}\}$ ó $\{\bar{1}, \bar{7}\}$. Ahora, ya que $7 \equiv -1$ (mód 8) se puede excluir $\{\bar{1}, \bar{7}\}$, pero no es posible decidir entre $\{\bar{1}, \bar{3}\}$ y $\{\bar{1}, \bar{5}\}$.

Experimentalmente, Euler y Fermat determinaron que $R_2 = \{\bar{1}, \bar{3}\}$ y $R_{-2} = \{\bar{1}, \bar{7}\}$. En los casos $N = 1, 2, -2$, Euler brindó descripciones completas de R_N con sus correspondientes pruebas. Los casos $N = 1$ y $N = -2$ son respectivamente la primera y la segunda leyes complementarias de la LRC.

Más tarde, en 1772, Euler enuncia la *Segunda Forma* o Forma Explícita de la LRC, publicada póstumamente en *Opuscula Analytica* (1783). Aquí reproducimos estos enunciados.

Teorema 4.3. *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 $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$.*

5. Legendre (1752-1833)

Legendre fue otro de los pioneros en el estudio de la LRC, de hecho fue el primero en dar una demostración, aunque incompleta, de este resultado. 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 5.1. *Sean a,b,c* $\in \mathbb{Z}$ *no todos del mismo signo y tales que abc es libre de cuadrados. 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 resto cuadrático módulo* $|a|$,
b) $-ca$ *es un resto cuadrático módulo* $|b|$,
c) $-ab$ *es un resto cuadrático módulo* $|c|$.

Así que dado $\left(\frac{p}{q}\right)$, él deduce el signo de $\left(\frac{q}{p}\right)$ con ayuda del lema 5.1. Sin embargo, su prueba, publicada en *Essai sur la Théorie des Nombres (1798)*, es completa sólo en los siguientes casos:

Teorema 5.2. *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* $\left(\frac{q}{p}\right) = -1$.

Demostración. Considérese la ecuación $x^2+py^2-qz^2 = 0$. Como $x^2+py^2-qz^2 \equiv x^2 + y^2 + z^2 \equiv 0 \pmod 4$ que no tiene soluciones enteras con $(x, y, z) = 1$, se tiene que $x^2 + py^2 - qz^2 = 0$ no tiene soluciones no triviales en $\mathbb{Z}$. Por el lema 5.1 no todas las condiciones se satisfacen simultáneamente. La primera y la tercera se satisfacen, luego la segunda condición no se debe cumplir, es decir $\left(\frac{q}{p}\right) = -1$.

Para la segunda parte del teorema se puede considerar la ecuación $x^2-py^2-qz^2 = 0$ y se deduce similarmente que $\left(\frac{q}{p}\right) = -1$. ☑

En los casos restantes LEGENDRE usa el hecho de que existe al menos un primo en una cierta clase de congruencia módulo $4pq$. Según GAUSS esto es equivalente a encontrar un número primo en una determinada progresión aritmética, hecho que solo fue probado en 1837 por DIRICHLET.

6. Gauss (1777-1855)

El primero en ofrecer una demostración completa de la LRC fue GAUSS en 1796. GAUSS estaba fascinado con este resultado y lo consideraba una de las joyas de la teoría de números, lo llamaba el *Theorema Aureum*.

Durante su vida publicó seis demostraciones y dos más fueron halladas en sus documentos después de su muerte.

Aquí presentamos una tabla que menciona los métodos usados en las pruebas de GAUSS [6, 8].

No.	Fecha (m/a)	Método
1	4/1796	Inducción, 8 casos
2	6/1796	Género de las formas cuadráticas
3	3/1807(?)	Lema de Gauss
4	5/1801	Sumas de Gauss
5	8/1808	Lema de Gauss
6	5/1808(?)	Ciclotomía en $\mathbb{Q}[x]/(1+x+\cdots+x^{p-1})$
7	9/1796	Ciclotomía y restos superiores (≥ 3)
8	9/1796	Ciclotomía y restos superiores

Esta tabla refleja el intenso trabajo de Gauss alrededor del tema. Cabe resaltar que las ideas esgrimidas en estas pruebas representaron avances considerables en la teoría de números de la época (aún en la teoría de números moderna). Temas como la teoría de formas cuadráticas, la teoría de cuerpos ciclotómicos y la teoría algebraica de números vieron la luz gracias a los trabajos de este gran matemático.

Al realizar sus estudios sobre formas cuadráticas y la LRC, Gauss visualiza la extensión de estos resultados. En particular, da las pautas para probar las leyes de reciprocidad cúbica y bicuadrática o cuártica, que consisten esencialmente en hallar los divisores primos de las formas $x^3 - N$ y $x^4 - N$, respectivamente.

7. Eisenstein (1823-1852)

Eisenstein fue uno de los discípulos más brillantes de Gauss y según Weil [9] fue uno de los matemáticos más grandes de la historia.

Eisenstein realizó cinco pruebas de la LRC y sigue las pautas de Gauss para probar las leyes de reciprocidad cúbica y bicuadrática, véase la última sección. Hemos escogido su prueba de 1845 para este trabajo, tal vez una de las pruebas más hermosas de este resultado. La prueba que presentamos se puede hallar en [7].

Demostración. Partimos de una afirmación clásica, conocida como el lema de Gauss.

Lema 7.1. [Lema de Gauss] *Sean $a \in \mathbb{Z}$ y p un primo impar con $p \nmid a$. Si*

$$S = \{1 \cdot a, 2 \cdot a, \ldots, \frac{(p-1)}{2} \cdot a\}$$

y μ denota el número de elementos de S cuyos restos mínimos módulo p son negativos. Entonces

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

Ahora usaremos una afirmación sobre las raíces de la unidad.

Afirmación 7.1. Si $n > 0$ es impar, se tiene que

$$x^n - y^n = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y), \text{ donde } \zeta = e^{2\pi i/n}.$$

Demostración. Notemos que $z^n - 1 = \prod_{k=0}^{n-1}(z - \zeta^k)$. Si hacemos $z = x/y$ tendremos $\frac{x^n}{y^n} - 1 = \prod_{k=0}^{n-1}(x/y - \zeta^k)$, multiplicando por y^n obtenemos $x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^k y)$. Ahora, al variar k sobre un sistema completo de residuos módulo n, $-2k$ también lo hace. Por consiguiente

$$\begin{aligned} x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^k y) = \prod_{k=0}^{n-1}(x - \zeta^{-2k} y) = \prod_{k=0}^{n-1} \zeta^{-k}(\zeta^k x - \zeta^{-k} y) \\ = \zeta^{-\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y) = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y). \quad \boxtimes \end{aligned}$$

Proposición 7.2. *Si n es un entero positivo impar y $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, entonces*

$$\frac{f(nz)}{f(z)} = \prod_{k=0}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Demostración. En la afirmación anterior sean $x = e^{2\pi iz}$ y $y = e^{-2\pi iz}$, entonces

$$\begin{aligned} f(nz) = e^{2\pi izn} - e^{-2\pi izn} = \prod_{k=0}^{n-1}(\zeta^k e^{2\pi iz} - \zeta^{-k} e^{-2\pi iz}) \\ = \prod_{k=0}^{n-1}(e^{2\pi i(\frac{z+k}{n})} - e^{-2\pi i(\frac{z+k}{n})}) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right). \end{aligned}$$

Además $f\left(z + \frac{k}{n}\right) = f\left(z + \frac{k}{n} - 1\right) = f\left(z - \frac{(n-k)}{n}\right)$, pues las funciones involucradas tienen período 1. Cuando k varía desde $\frac{n+1}{2}$ hasta $n-1$, $n-k$ varía desde $\frac{n-1}{2}$ hasta 1, por tanto

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Proposición 7.3. *Si a es un entero no divisible por p, un primo impar. Entonces*

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Demostración. Sea m_l el resto mínimo de la en el conjunto descrito en el lema de Gauss. Entonces $la \equiv \pm m_l \pmod{p}$, donde $1 \leq m_l \leq (p-1)/2$. Así que $\frac{la}{p}$ y $\frac{\pm m_l}{p}$ difieren por un entero, por tanto

$$f\left(\frac{la}{p}\right) = f\left(\frac{\pm m_l}{p}\right) = \pm f\left(\frac{m_l}{p}\right).$$

Al tomar producto entre 1 y $(p-1)/2$ a ambos lados y aplicar el lema de Gauss obtenemos lo requerido.

7.1. La Prueba. Finalmente se puede probar ahora la LRC. Sean p y q dos primos impares. Por la proposición anterior

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Y de la proposición 7.2 se tendrá

$$\frac{f(ql/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Al unir estas ecuaciones se obtiene

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Al intercambiar los papeles de p y q y repetir el proceso, se obtendrá

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right).$$

Y como $f\left(\frac{m}{q} - \frac{l}{p}\right) = -f\left(\frac{l}{p} - \frac{m}{q}\right)$, se tiene que

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

8. Comentarios Finales

Como mencionamos antes, la prueba de la LRC que hemos reproducido aquí es una versión de la prueba original de Eisenstein [4]. En la prueba original Eisenstein usa la función seno, en vez de la función $f(z)$ que hemos usado aquí, pero las ideas son esencialmente las mismas. Recuérdese de la teoría de variable compleja que

$$\operatorname{sen} z = \frac{e^{iz} - e^{-iz}}{2i} = \frac{1}{2}\left[e^{i(z-\pi/2)} - e^{-i(z+\pi/2)}\right].$$

La escogencia de la función $f(z)$ elimina la aparición de una inoportuna constante en la prueba original de Eisenstein.

EISENSTEIN también prueba las leyes de reciprocidad cúbica y bicuadrática. Para ello usa ciertas funciones elípticas de propiedades análogas a la función $f(z)$. Mayor información se puede encontrar en [6].

El estudio de las leyes de reciprocidad fue uno de los temas centrales de la teoría de números del siglo XIX, y exigió los mejores esfuerzos de grandes personajes como CAUCHY, JACOBI, DIRICHLET, KUMMER, EISENSTEIN, KRONECKER, DEDEKIND y HILBERT, entre muchos otros. Durante el siglo XX la LRC también fue tema de intensa investigación y prueba de ello es el gran número de pruebas que se han realizado [8].

La LRC se puede formular sobre otros conjuntos, tales como el anillo de los enteros gaussianos, el anillo de polinomios sobre un cuerpo finito y cuerpos de números algebraicos, por ejemplo. En la misma dirección de la LRC se encuentran la ley de reciprocidad racional (EISENSTEIN 1850), la ley de reciprocidad en campos ciclotómicos (TAKAGI 1922) y uno de los teoremas cumbres de la teoría de números contemporánea, la ley de reciprocidad de ARTIN en extensiones abelianas (ARTIN 1927).

Agradecimientos. El autor quiere agradecer al profesor VÍCTOR SAMUEL ALBIS G. por proponer el tema del presente artículo y por promover vivamente su publicación. Este trabajo es fruto de la tesis de pregrado en matemáticas realizada por el autor y dirigida por el profesor ALBIS.

Referencias

[1] ALBIS, VÍCTOR S. *El testamento matemático de Pierre de Fermat.* XVI Coloquio Distrital de Matemáticas y Estadística. Universidad Distrital Francisco José de Caldas, 1999.

[2] ALBIS, VÍCTOR S. *Clásicos de la matemática: La carta de Fermat a Carcavi. Agosto de 1659.* Lecturas Matemáticas. **20** (1999), 137–152.

[3] COX, DAVID A. *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* New York. Jhon Wiley & Sons, Inc. 1989.

[4] EISENSTEIN, GOTTHOLD. *Application de l'algèbre à l'arithmétique transcendante.* J. Reine Angew. Math. **29** (1845), 177-184; Math. Werke **I**, 291-298.

[5] FERMAT, PIERRE DE. *Carta a Mersenne*, 25.12.1640, Oeuvres, vols. **I** y **II**, 219-225. Publicados por Paul Tannery & Charles Henry, Gauthiers-Villars. 1891-1912.

[6] FREI, GÜNTER. *The Reciprocity Law from Euler to Eisenstein.* En *The intersection of history and mathematics.* Boston. Birkhauser. 1994, 67-90.

[7] IRELAND, KENNETH & ROSEN, MICHAEL. *A classical introduction to modern number theory.* New York. Springer-Verlag. 1990. Segunda edición.

[8] LEMMERMEYER, FRANZ. *Proofs of the Quadratic Reciprocity Law.* En `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

[9] WEIL, ANDRÉ. *Review of "Mathematische Werke, by Gotthold Eisenstein".* En *André Weil, Oeuvres scientifiques, Collected papers.* Vol. **III**. New York. Springer-Verlag. 1979. 398-403.

(Recibido en septiembre de 2006. Aceptado para publicación en mayo de 2009)

Edwin León Cardenal
Departamento de Matemáticas
Universidad Nacional de Colombia
Bogotá, Colombia, Av. Carrera 30 No. 45–03
e-mail: eleonc@unal.edu.co