

# PRIMERA DEMOSTRACIÓN DE LA LEY DE RECIPROCIDAD CUADRÁTICA REALIZADA POR CARL FRIEDERICH GAUSS

CAROLINA MARTÍNEZ CARO

UNIVERSIDAD NACIONAL DE COLOMBIA  
Facultad de Ciencias – Departamento de Matemáticas  
Bogotá. Colombia  
cmartinezca@unal.edu.co

## Resumen

La Ley de Reciprocidad Cuadrática tiene un papel muy importante en la Teoría de Números, ya que en base a esta, se han obtenido otros resultados interesantes en diversos campos de la matemática.

El objetivo de este trabajo es presentar y estudiar la primera demostración completa de esta ley, realizada por Carl Friederich Gauss en 1796, la cual descubrió independientemente, a pesar que esta ya había sido enunciada primero por Leonard Euler en su *Opuscula Analytica* y luego por Adrien Marie Legendre.

## Abstract

The Quadratic Reciprocity Law has a very important role in Number Theory, because some other interesting results in several topics of mathematics have been derived from this result.

The objective of this work is to present and study the first complete proof of this law done by Carl Friederich Gauss in 1796, which he discovered independently, although it has been already stated by Leonard Euler in his *Opuscula Analytica* and later by Adrien Marie Legendre.

## INTRODUCCIÓN HISTÓRICA

Haciendo un recorrido por la historia de la matemática y teniendo a la ley de reciprocidad cuadrática como eje central, el primero que ofrece de manera implícita una parte de la primera ley complementaria de la *L.R.C.* es Diofanto de Alejandría, en su obra *Arithmetica*. Luego, Fermat motivado por este libro encuentra parte esencial de la primera ley complementaria de la *L.R.C.* como lo expresa en una carta a su amigo Mersenne en 1640.

Fue Kronecker, quien en 1875 sugirió el hecho de que la *L.R.C.* había sido ya expuesta por Euler en 1783, quien se inició en el estudio de esta ley gracias al trabajo antes realizado por Fermat. Euler encuentra entre 1741 y 1742 la primera o forma implícita de la *L.R.C.* y posteriormente en 1772 consigue la segunda o forma explícita de la *L.R.C.*, publicada después de su muerte en *Opuscula Analítica* de 1783.

Cabe notar ahora que ninguno de estos matemáticos demostró la *L.R.C.* Tan solo posteriormente Legendre ofreció una prueba parcial de dicho teorema.

Fue en 1796 cuando Carl Friederich Gauss realizó la primera demostración completa de la *L.R.C.*, publicándola posteriormente en su magna obra *Disquisitiones Arithmeticae*. A lo largo de su vida Gauss realizó 8 demostraciones de esta ley que el denominó ***Theorema aureum***.

Es importante resaltar que las demostraciones de Gauss sirvieron de impulso para que otros grandes matemáticos se dieran a la tarea de desarrollar teorías tan importantes como la teoría algebraica de números y que otros encaminaran sus esfuerzos en trabajos paralelos a este.

## PRIMERA DEMOSTRACIÓN DE LA LEY DE RECIPROCIDAD CUADRÁTICA

Para empezar con el estudio de la primera demostración de la *L.R.C.* realizada por Gauss, se darán algunas definiciones, y algunos términos se traspondrán al lenguaje moderno para facilitar la lectura de este documento.

**Definición 1.** Sean  $a$  y  $b$  números enteros cualesquiera y  $n$  un entero positivo. Si  $n$  divide la diferencia entre los números  $a$  y  $b$ , se dice que  $a$  y  $b$  son congruentes módulo  $n$  y se nota  $a \equiv b \pmod{n}$ ; si no lo son, se dice que son incongruentes. Ambos números  $a$  y  $b$ , en el primer caso son llamados uno residuo del otro y, en el segundo caso, no residuos.

**Definición 2.** Sea  $p$  un número primo impar, y  $a$  un entero tal que  $(a, p) = 1$ . Si la congruencia  $x^2 \equiv a \pmod{p}$  tiene solución, decimos que  $a$  es un residuo cuadrático módulo  $p$ .

Teniendo como base estas definiciones, se hará un seguimiento cuidadoso de la primera demostración de la *L.R.C.*. Lo que a continuación se estudiará será un criterio para determinar si dados  $a$  y  $p$  con  $(a, p) = 1$  y  $p$  primo impar,  $a$  es o no es un residuo cuadrático módulo  $p$ .

**Criterio de Euler.** Cualquier número  $a$  no divisible por un número primo de la forma  $2m + 1$  es un residuo o no residuo de este número primo según que:  $a^m \equiv +1 \pmod{2m + 1}$  o  $a^m \equiv -1 \pmod{2m + 1}$ .

Para Gauss este criterio valía la pena mencionarse pues era simple y gozaba de generalidad. Sin embargo lo consideraba un resultado inútil si los números que se tomaban eran muy grandes.

A continuación lo que hace Gauss es estudiar la situación en la cual, propuesto algún número, averiguar todos los números, de los cuales aquel será un residuo o no residuo, esto es: dado  $a$ , encontrar todo número primo  $p$  del cual  $a$  sea un residuo. Este problema lo aborda comenzando con los casos más sencillos, empezando de la siguiente manera:

*i)* En el artículo 108 de las *Disquisitiones Arithmeticae*, demuestra que  $-1$  es un residuo cuadrático de  $p$  primo si y solo si  $p$  es de la forma  $4n + 1$ , pero es un no residuo cuadrático de todos los números primos de la forma  $4n + 3$ .

Aquí se presenta un bosquejo de la demostración:

Sea  $p$  un número primo de la forma  $4n + 1$ , entonces  $-1$  es un residuo cuadrático módulo  $4n + 1$  si

$$(-1)^{\frac{(4n+1-1)}{2}} \equiv +1 \pmod{4n+1},$$

efectivamente,

$$(-1)^{\frac{4n}{2}} = (-1)^{2n} \equiv 1 \pmod{4n+1},$$

pero para un número primo de la forma  $4n + 3$  se tiene que

$$(-1)^{\frac{(4n+3-1)}{2}} \equiv -1 \pmod{4n+3},$$

esto es:

$$(-1)^{\frac{4n+2}{2}} = (-1)^{\frac{2(2n+1)}{2}} = (-1)^{2n+1} \equiv -1 \pmod{4n+3},$$

de donde se tiene el anterior teorema.

**ii)** En los artículos 112 - 114 de las *D.A.* estudia el problema cuando  $a = \pm 2$  para los primos

$$p \equiv 3 \pmod{8}$$

$$p \equiv 5 \pmod{8}$$

$$p \equiv 7 \pmod{8}$$

$$p \equiv 1 \pmod{8}$$

A continuación se especifican los casos, para luego hacer, a modo ilustrativo la demostración de dos de ellos:

- (1)  $+2$  es un no residuo de los primos de la forma  $8n + 3$ .
- (2)  $-2$  es un residuo de los primos de la forma  $8n + 3$ .
- (3)  $+2$  es un no residuo de los primos de la forma  $8n + 5$ .
- (4)  $-2$  es un no residuo de los primos de la forma  $8n + 5$ .
- (5)  $-2$  es un no residuo de los primos de la forma  $8n + 7$ .
- (6)  $+2$  es un residuo de los primos de la forma  $8n + 7$ .
- (7)  $+2$  es un residuo de los primos de la forma  $8n + 1$ .
- (8)  $-2$  es un residuo de los primos de la forma  $8n + 1$ .

*Demostración de los casos 1. y 3.*

Tomemos los primos menores que 100 de los cuales  $+2$  es un residuo: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Ninguno de éstos números es de la forma  $8n + 3$  ni  $8n + 5$ . Veamos si con esta pequeña inducción puede realizarse la demostración.

Notamos primero que todo número compuesto de la forma  $8n + 3$  u  $8n + 5$  necesariamente involucra un factor primo de una de las formas  $8n + 3$  u  $8n + 5$ . Por tanto si la inducción es cierta en general, no se presentará ningún número de la forma  $8n + 3$  u  $8n + 5$  cuyo residuo sea

+2. Lo que hemos visto es que no existe ningún número de esta forma menor que 100 del cual +2 es un residuo. Sin embargo supongamos que se encuentran tales números más allá de 100, entonces llamemos  $t$  al menor de ellos, de tal manera que  $t$  será de la forma  $8n + 3$  o de la forma  $8n + 5$ . Entonces +2 será un residuo de  $t$ , pero un no residuo de todos los números menores que  $t$ . Si se pone  $2 \equiv a^2 \pmod{t}$ , siempre  $a$  podrá tomarse como impar y a la vez  $a < t$ , puesto que atenderá al menos dos valores positivos menores que  $t$ , de los cuales uno es par y el otro impar (*Art. 104 - 105, D.A.*). Por la misma razón, sea  $a^2 = 2 + tu$ , es decir  $a^2 - 2 = tu$ , en donde  $a^2$  será de la forma  $8n + 1$ ,  $tu$  por lo tanto de la forma  $8n - 1$ , y así  $u$  será de la forma  $8n + 3$  u  $8n + 5$  según sea  $t$  de la segunda forma o de la primera forma. Pero de la ecuación  $a^2 = 2 + tu$  se sigue también que  $2 \equiv a^2 \pmod{u}$ , esto es 2 también será un residuo de  $u$ . De esto, se percibe que  $u < t$ , de donde  $t$  no es el número menor, lo cual contradice la hipótesis de inducción, de donde se tiene que +2 no es residuo de los primos de la forma  $8n + 3$  ni de los primos de la forma  $8n + 5$ .

*iii*) En los artículos 117 - 119 de las *D.A.* estudia el problema para  $a = \pm 3$  y para los primos

$$p \equiv 5 \pmod{12}$$

$$p \equiv 1 \pmod{12}$$

$$p \equiv 7 \pmod{12}$$

$$p \equiv 11 \pmod{12}$$

indicando en el artículo 120 de *D.A.* que Fermat conocía el resultado para  $a = \pm 3$  y reconociendo que Euler fue el primero en dar demostraciones de estos hechos. A continuación se especifican los casos, luego a manera de ejemplo se realiza la demostración de dos de ellos, pues los casos precedentes se prueban de manera análoga a los del numeral *ii*).

- (1) +3 es un no residuo de los primos de la forma  $12n + 5$ .
- (2) -3 es un no residuo de los primos de la forma  $12n + 5$ .
- (3) -3 es un no residuo de los primos de la forma  $12n + 11$ .
- (4) +3 es un residuo de los primos de la forma  $12n + 11$ .
- (5) +3 es un no residuo de los primos de la forma  $12n + 7$ .
- (6) -3 es un residuo de los primos de la forma  $12n + 7$ .
- (7) +3 es un residuo de los primos de la forma  $12n + 1$ .
- (8) -3 es un residuo de los primos de la forma  $12n + 1$ .

*Demostración de los casos 7. y 8.*

Por inducción se prueba fácilmente que  $+3$  y  $-3$  son residuos de todos los números de esta forma. Solo debe mostrarse que  $-3$  es un residuo de tales números, ya que necesariamente  $+3$  será un residuo, pues de manera general se tiene que si  $r$  es un residuo de algún número primo de la forma  $4n + 1$ , también  $-r$  será un residuo de este primo. Sin embargo se demostrará que  $-3$  es un residuo de cualquier número primo de la forma  $3n + 1$ .

Sea  $p$  uno de tales primos y  $a$  un número que, para el módulo  $p$ , pertenece al exponente 3, ya que 3 es divisor de  $p - 1$ . Por eso será  $a^3 \equiv 1 \pmod{p}$ , es decir,  $a^3 - 1 \equiv 0 \pmod{p}$ , o sea  $(a^2 + a + 1)(a - 1)$  será divisible por  $p$ . Pero es claro que  $a$  no puede ser congruente con  $1 \pmod{p}$  ya que 1 pertenece al exponente 1, por lo que  $a - 1$  no será divisible por  $p$ , pero  $a^2 + a + 1$  lo será, y de allí también  $4a^2 + 4a + 4 = (2a + 1)^2 + 3$ , por lo que  $(2a + 1)^2 \equiv -3 \pmod{p}$ , o sea  $-3$  es residuo de  $p$ .

*iv)* En los artículos 121–123 de las *D.A.* estudia el problema cuando:

- a)  $a = \pm 5$  y  $p \equiv 2 \pmod{5}$  o  $p \equiv 3 \pmod{5}$
- b)  $a = \pm 5$  y  $p \not\equiv 2 \pmod{5}$  ni  $p \not\equiv 3 \pmod{5}$ .

*Demostración del caso a).*

Por inducción se tiene que  $+5$  no es un residuo de ningún número impar de la forma  $5n + 2$  o  $5n + 3$ , es decir, de ningún número impar que sea no residuo de 5. Se demuestra que esta regla no tiene excepción.

Sea  $t$  el número menor que constituya una excepción de esta regla, este por lo tanto es un no residuo del número 5, pero 5 es un no residuo de  $t$ . Sea  $a^2 = 5 + tu$  tal que  $a$  sea par y menor que  $t$ . Entonces  $u$  será impar y menor que  $t$ , pero  $+5$  será un residuo de  $u$ . Ahora si  $a$  no es divisible por 5, tampoco lo será  $u$ . Pero es claro que  $tu$  es un residuo de 5 (*Art. 98 D.A.*), por lo que, puesto que  $t$  es un no residuo de 5, tampoco lo será  $u$ , es decir, existe un no residuo impar del número 5 cuyo residuo es  $+5$ , pero menor que  $t$ , lo cual contradice la hipótesis.

Si por otro lado  $a$  es divisible por 5, se toma  $a = 5b$  y  $u = 5v$  de donde  $tv \equiv -1 \equiv 4 \pmod{5}$ , es decir  $tv$  será un residuo del número 5. De aquí en adelante la demostración es análoga al caso anterior.

*v)* En el artículo 123 de las *D.A.* demuestra la Ley de Reciprocidad Cuadrática para  $a = \pm 5$ . Aquí un bosquejo de cómo se llega a esta hecho:

Por inducción se descubre que  $+5$  y  $-5$  son residuos de todos los números primos de la forma  $20n + 1$  o  $20n + 9$ . Ahora bien, si esto es cierto en general, se tendrá la siguiente ley:  *$+5$  es un residuo de todos los números primos que sean residuos de 5, pero es un no residuo de todos los números impares que son no residuos de 5.* Este teorema es suficiente para juzgar si  $+5$  (y también  $-5$  si se considera como producto de  $+5$  y  $-1$ ) es un residuo o un no residuo de cualquier número dado.

*vi)* En el artículo 124 de *D.A.* se estudia el caso para  $a = \pm 7$ , esto es, se demuestra que  *$-7$  es un no residuo de cualquier número que sea no residuo de 7* y por inducción se concluye que:  *$-7$  es un residuo de cualquier número primo que sea residuo de 7.*

La demostración es sencilla para los residuos de 7 cuya forma sea  $4n - 1$ , pues puede mostrarse que  $+7$  siempre es un no residuo de tales números primos y así  $-7$  es un residuo.

Se resolverá un caso en particular a saber: si  $p$  es un número primo de la forma  $7n + 1$ , y  $a$  pertenece al exponente 7 para el módulo  $p$ , se observa que:

$$\frac{4(a^7 - 1)}{a - 1} = (2a^3 + a^2 - a - 2)^2 + 7(a^2 + a)^2$$

es divisible por  $p$ , de donde  $-7(a^2 + 2)^2$  será un residuo de  $p$ . Pero  $(a^2 + 2)^2$ , como cuadrado, es un residuo de  $p$  y no divisible por  $p$ . Puesto que se supone que  $a$  pertenece al exponente 7, no puede ser ni congruente con cero, ni congruente con  $-1 \pmod{p}$ , es decir, ni  $a$  ni  $a+1$  serán divisibles por  $p$ , ni tampoco lo será el cuadrado  $(a + 1)^2 a^2$ . De donde también resulta que  $-7$  será un residuo de  $p$ .

Esta demostración la encontró también Lagrange.

Después de haber estudiado todos estos casos, Gauss generalizará lo anterior por el método de inducción, por lo que a continuación puede enunciar la **ley de reciprocidad cuadrática** así: (*Art. 131 D.A.*)

*Si  $p$  es un número primo de la forma  $4n + 1$ ,  $+p$  será un residuo o no residuo de cualquier número primo que, tomado positivamente, es un residuo o no residuo del mismo  $p$ . Si  $p$  es un número primo de la forma  $4n + 3$ ,  $-p$  tendrá la misma propiedad.*

Se introduce la siguiente notación:

La letra  $R$  puesta entre dos cantidades indicará que la primera es un *residuo* de la siguiente, mientras que la letra  $N$  tendrá el significado

contrario. Entonces con esta notación la *L.R.C.* queda:

$$pRq \Leftrightarrow qRp \text{ si } p \text{ o } q \equiv 1(\text{mod}4).$$

$$pRq \Leftrightarrow qNp \text{ si } p \text{ y } q \equiv -1(\text{mod}4).$$

*vii)* Después de realizado el estudio particular de estos casos, en los artículos siguientes (*Art. 136 - 144 de D.A.*) Gauss hace la demostración rigurosa de la *L.R.C.*, sirviéndose de 8 casos generales, que a continuación describiremos.

***Demostración de la Ley de Reciprocidad Cuadrática:***

Por inducción se puede comprobar que la *L.R.C.* es válida para números pequeños, de tal manera se determina un límite hasta el cual sea válida.

Ahora, si la *L.R.C.* no es verdadera en general, existirá algún límite  $J$  hasta el cual será válida, de manera que ya no lo sea más para el próximo número mayor que  $J + 1$ .

Esto es lo mismo que suponer que existen dos números primos, de los cuales el mayor es  $J + 1$  y que comparados entre sí contradicen la *L.R.C.*, y además que otros pares cualesquiera de números primos, siendo ambos menores que  $J + 1$ , cumplen esta ley. Se mostrará que esta suposición es contradictoria, con lo cual se demuestra la Ley de Reciprocidad Cuadrática.

A continuación se presentan los 8 casos en un orden estricto, ya que algunos de ellos son dependientes de otros.

***Primer caso.*** Cuando  $J + 1$  es de la forma  $4n + 1$  (llamemos a uno de estos números  $a$ ), y  $p$  es de la misma forma, si  $\pm pRa$ , entonces no puede ser que  $\pm aNp$ .

***Segundo caso.*** Cuando  $J + 1$  es de la forma  $4n + 1$  (llamemos a uno de estos números  $a$ ),  $p$  de la forma  $4n + 3$ , y  $\pm pR(J + 1)$ , no puede ser ni  $+(J + 1)Np$  ni  $-(J + 1)Rp$ .

***Tercer Caso.*** Cuando  $J + 1$  es de la forma  $4n + 1$  (llamemos a uno de estos números  $a$ ),  $p$  de la misma forma y  $\pm pNa$ , entonces no puede ser que  $\pm aRp$ .

***Cuarto caso.*** Cuando  $J + 1$  es de la forma  $4n + 1$  (llamemos a uno de estos números  $a$ ),  $p$  de la forma  $4n + 3$ , y  $\pm pNa$ , no podrán ser ni  $+aRp$  ni  $-aNp$ .

**Quinto caso.** Cuando  $J + 1$  es de la forma  $4n + 3$  (llamemos a uno de estos números  $b$ ),  $p$  de la misma forma, y  $+pRb$  o  $-pNb$ , no será ni  $+bRp$  ni  $-bNp$ .

**Sexto caso.** Cuando  $J + 1$  es de la forma  $4n + 3$  (llamemos a uno de estos números  $b$ ),  $p$  de la forma  $4n + 1$ , y  $pRb$ , no puede ser  $\pm bNp$ .

**Séptimo caso.** Cuando  $J + 1$  es de la forma  $4n + 3$  (llamemos a uno de estos números  $b$ ),  $p$  de la misma forma, y  $+pNb$  o  $-pRb$ , no pueden ser  $+bNp$ , ni  $-bRp$ .

**Octavo caso.** Cuando  $J + 1$  es de la forma  $4n + 3$  (llamemos a uno de estos números  $b$ ),  $p$  de la forma  $4n + 1$ , y  $+pNb$  o  $-pRb$ , no puede ser  $\pm bRp$ .

Demostrados estos casos se da por terminada la prueba de la *Ley de Reciprocidad Cuadrática*.

En los artículos siguientes Gauss soluciona problemas con la colaboración de la recién demostrada ley, y hace alusión en el artículo 151 de las *D.A.*, a los trabajos que otros matemáticos realizaron sobre este tema, resaltando los de Euler consignados algunos de ellos en una memoria titulada *Novae demonstrationes circa divisores numerorum formae  $xx+nyy$* , y otros en *Opuscula Analytica*, y los de Lagrange contenidos en el notable tratado *Recherches d'analyse indéterminée*.

**BIBLIOGRAFÍA**

- [1] ALBIS, Víctor. *El Señor Fermat y sus problemas, III*. Boletín de Matemáticas **10** 1976.
- [2] BUHLER W. K. *Gauss a Biographical Study*. New York-Heidelberg: Springer-Verlag, 1981
- [3] CARLITZ L. *A note on Gauss' first proof of the quadratic reciprocity theorem*. Proc. Amer. Math. Soc. **11** (1960), 563–565.
- [4] EDWARDS, Harold M. *Euler and Quadratic Reciprocity*, Mathematics Magazine **56** (5) (1983), 285–291.
- [5] FREI, Günter. *The Reciprocity Law from Euler to Eisenstein*, en *The Intersection of History and Mathematics*. Birkhäuser: Boston, 1994, 67–90.
- [6] GAUSS, Carl Friederich. *Disquisitiones Arithmeticae*. Academia Colombiana de Ciencias Exactas, Físicas y Naturales: Bogotá, 1995.
- [7] GAUSS, Carl Friederich. *Werke*. Multivolume Work, Digital Collections: Mathematica. Dietrich. 1863. Disponible en <http://gdz.sub.uni-goettingen.de/en/>
- [8] IRELAND, Kenneth. Rosen, Michael. *A Classical Introduction to Modern Number Theory*. Springer-Verlag: New York-Heidelberg, 1982.
- [9] JIMÉNEZ, Rafael, GORDILLO, Enrique & RUBIANO, Gustavo. *Teoría de Números para Principiantes*. Universidad Nacional de Colombia: Bogotá, 1999.
- [10] LEÓN CARDENAL, Edwin. *La Ley de Reciprocidad Cuadrática, una breve revisión histórica*. Manuscrito inédito.
- [11] <http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html/>