Facultad
de
Ciencias

La Ley de Reciprocidad Cuadrática: Algunas pruebas clásicas
(Quadratic Reciprocity Law: Some classical proofs)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Mar Lazcano Coca

Director: María Pilar Fernández-Ferreiros Erviti

Septiembre - 2017

Resumen:

El objetivo de este trabajo es estudiar seis demostraciones de la Ley de Reciprocidad Cuadrática, elegidas entre una larga lista. Para ello, presentaremos algunas definiciones y teoremas que nos serán muy útiles a la hora de estudiar las pruebas. Más tarde analizaremos cada una de las demostraciones, las cuales han sido seleccionadas, algunas por su carácter clásico, y otras, aunque quizá menos conocidas, por utilizar métodos muy distintos, lo que aporta una variedad e interés al trabajo.
Palabras clave: Ley de Reciprocidad Cuadrática

Abstract:

The purpose of this report is to study six different proofs of the Quadratic Reciprocity Law, choosen from a large list. In order to do this, we start giving some definitions and theorems which will be useful when studying the proofs. After that, we analyze each one of them. Some of them have been selected because they are the classic proofs, but we have chosen other because they use very different methods. Thus, we achive a more interesting and varied work.
Key words: Quadratic Reciprocity Law

Índice general

Capítulo 1

Introducción

La teoría de números es la rama de las matemáticas que estudia los números enteros y los problemas que derivan de su estudio. Otro término que se utilizaba mas antiguamente para referirse a ella es aritmética, o alta aritmética. Considerada fascinante para muchos matemáticos como Gauss, que será el matemático más mencionado en este trabajo, llamaba a ésta "la reina de las matemáticas". El tema que vamos a tratar en este trabajo es uno de los resultados importantes asociado a esta rama: la Ley de Reciprocidad Cuadrática que fue denominada por Gauss como el Teorema Áureo. El matemático alemán Erich Hecke afirmó al respecto: "La teoría de números moderna comenzó con el descubrimiento de la Ley de Reciprocidad Cuadrática".

Esta ley es uno de los resultados con más demostraciones distintas de la Historia de las Matemáticas, contando actualmente con mas de 200 demostraciones diferentes (véase Apéndice). El objetivo de este trabajo es ahondar en algunas de las pruebas de esta larga lista, entre ellas, algunas tan importantes y conocidas como la tercera de Gauss. Aparecerán otras demostraciones no tan conocidas, pero muy interesantes e ingeniosas, como la de Ygor Zolotarev, que usa permutaciones para obtener la Ley de Reciprocidad Cuadrática. En total daremos seis demostraciones distintas, además de un par de modificaciones a la tercera de Gauss. Hemos incluido demostraciones tan clásicas como la cuarta de Gauss, conocida por usar las sumas cuadráticas de Gauss, y otras menos conocidas y más recientes como la de G. Rousseau, de 1990, pero que es igual de interesante.

De esta manera, se revela el gran interés que tiene la Ley de Reciprocidad Cuadrática: a partir de puntos muy distintos, y de ramas muy distantes de

las matemáticas, llegamos un resultado común.

1.1. Historia

Podríamos decir que la primera cuestión relacionada con la reciprocidad cuadrática data del siglo II d.C. con el trabajo de Diofanto de Alejandría publicado en su obra Arithmetica, donde aparece de una manera implícita. En su estudio de las ecuaciones diofánticas, que son de la forma $x^n + y^n = a$, Diofanto resuelve un problema del libro 6 de su obra: *¿*$x^2 + y^2 = 15$ *tiene soluciones en los enteros?*
Utilizando la siguiente afirmación no demostrada "Si a es un entero de la forma $4n + 3$ entonces $x^2 + y^2 = a$ no tiene soluciones enteras", concluye que no tiene solución.
Fermat se interesó por la obra de Diofanto en el siglo XV, lo que supuso que el estudio de la teoría de números experimentara un desarrollo muy importante, y por ello algunos lo consideran el padre de la teoría de números moderna. Fue muy raro que Fermat se interesara por esta rama de las matemáticas en la Europa del siglo XVII, en la que el estudio de los números enteros se consideraba inútil ya que no tenía ninguna aplicación directa. Sólo un par de problemas clásicos atraían la atención de los matemáticos: el estudio de números perfectos, y la caracterización de las ternas pitagóricas. Este último es el que lleva a Fermat a interesarse por la descomposición de los primos de la forma $4n + 1$. El hecho de que en la época de Fermat no existieran diarios matemáticos unido a que Fermat se negaba a publicar sus resultados, nos lleva a que lo único de lo que tenemos constancia sobre su trabajo esté en cartas o en los márgenes de sus libros, como es el caso del famoso "último teorema de Fermat". En una carta a Mersenne, Fermat enuncia la primera ley complementaria de la L.R.C:

"Todo número primo, que supere por una unidad un múltiplo de 4, es una única vez la suma de cuadrados, y es una única vez la hipotenusa de un triángulo rectángulo". Con un lenguaje matemático más actual lo escribiríamos de la siguiente manera:

$$p = x^2 + y^2 \text{ con } x, y, \in \mathbb{Z} \Longleftrightarrow p \equiv 1 \text{ mód } 4$$

Fermat probó la implicación a la izquierda mediante el método del descenso infinito, pero no fue capaz de demostrar la afirmación hacia la derecha, que no la obtuvimos hasta que Euler la proporcionó. Este matemático es el

siguiente a mencionar en el lento desarrollo y descubrimiento de la L.R.C. Muchas de las ideas de Fermat no se exploraron hasta siglos después de su muerte y Euler fue uno de los interesados por su trabajo. Su interés por la teoría de números parece venir del intercambio de cartas sobre este tema con Goldbach. En una de estas cartas, Euler comienza enunciando el teorema citado anteriormente, de la siguiente manera:
Si x e y numeros enteros positivos primos entre sí, la fórmula $x^2 + y^2$ no tiene otros divisores primos que aquellos de la forma $4n + 1$, y estos mismos primos se pueden escribir todos de la forma $x^2 + y^2$.

Este teorema, a pesar de haberlo enunciado, no lo consiguió probar hasta 1758. Generalizando la expresión anterior a las de la forma $x^2 + ny^2$, Euler consiguió dar pruebas, tanto para $n = 2$ como para $n = 3$, y estableció los recíprocos, que fueron demostrados por Lagrange años más tarde. En la década de 1770, Euler consige dar por primera vez un enunciado de la Ley de Reciprocidad Cuadrática de forma implícita, también llamada Primera Forma y ahora conocida como "Criterio de Euler", y más tarde la forma explícita, aunque no conocimos este resultado hasta su publicación en 1783, posterior a su muerte en su obra *Opúscula Analítica*.

Teorema 1.1 *Sean p y q dos primos impares y distintos. Entonces $p \mid x^2 - q \iff p$ es de la forma $4p + b$ para algún entero impar b.*

A pesar de ser Euler el autor de este hallazgo, nunca supo dar más que pruebas empíricas de este resultado. A pesar de ello, el esfuerzo de comprobarlo estimuló mucho el trabajo que realizó posteriormente, y también el de otros grandes teóricos de números del siglo XVIII, Lagrange y Legendre. Éste último fue otro de los pioneros en el estudio de la L.R.C. y fue el primero en creer haber dado una demostración para ella. Además, una notación que usaremos muchísimo durante todo el trabajo se la debemos precisamente a él, llamado el símbolo de Legendre, $\left(\frac{p}{q}\right)$, que definiremos en el capítulo 2.
Teniendo como base el trabajo de Euler, Legendre distingue 8 casos que dependen de la congruencia $p, q \equiv \pm 1$ mód 4 y de $\left(\frac{p}{q}\right) = \pm 1$, y dado $\left(\frac{p}{q}\right)$ él deduce el signo de $\left(\frac{q}{p}\right)$, sin embargo la prueba que da solo es cierta para el caso $q = 4m + 3$. Para el resto de casos, Legendre acaba asumiendo un hecho no probado en la época: existe al menos un primo en una cierta clase de congruencia modulo $4pq$. Cosa que no fue probada hasta 1837 por Dirichlet.

Pero por fin llegamos al matemático verdaderamente brillante que dio el paso definitivo: Karl Friedrich Gauss. Mientras que la pregunta que se hacía Euler era si, dado un un $r \in \mathbb{Z}$ y un primo p, p divide un número de la forma $x^2 + r$, Gauss aproximó el tema desde un punto de vista diferente, aplicando su método de inversión: es relativamente simple calcular todos los residuos cuadráticos de un módulo dado pero, ¿encontrar todos los módulos para los cuáles un número dado es un residuo cuadrático? Entonces, ¿cuál es la norma que determina la distribución de los residuos cuadráticos entre los módulos? La Ley de Reciprocidad Cuadrática toma este nombre justamente por esta propiedad recíproca. Gauss estaba fascinado por la Ley de Reciprocidad Cuadrática, la cual descubrió a los 19 años, dio la primera demostración del teorema en el año 1801, recogida, junto con otra más, en su gran obra *Disquisitiones Arithmeticae*. Gauss volvió a este resultado durante toda su vida dando en total ocho demostraciones distintas. Gauss estaba particularmente satisfecho por este resultado, al que denominó "Theorema Aureum", por la simplicidad de su enunciado y por su gran complicación a la hora de demostrarlo. La versión de Gauss de este teorema es la siguiente:

Teorema 1.2 *Sean p y q primos impares. Entonces*

1. *Si p es de la forma* $4n + 1$ *entonces q es un residuo cuadrático módulo p* $\iff$ *p es un residuo cuadrático módulo q.*

2. *Si p es de la forma* $4n + 3$ *entonces q es un residuo cuadrático módulo p* $\iff$ *-p es un residuo cuadrático módulo q.*

Detrás de esta Ley de Reciprocidad Cuadrática, y tomándola como base, han aparecido las denominadas Leyes de Reciprocidad Superiores, entre las que están la Ley de Reciprocidad Cúbica y la ley de Reciprocidad Bicuadrática o Cuártica (ver [9] y [11]).

Capítulo 2

Resultados Básicos

En este capítulo incluiremos algunas definiciones y teoremas básicos a los que recurriremos durante todo el trabajo.

Definición 2.1 (Residuo cuadrático) *Llamaremos residuo cuadrático módulo p a cualquier entero n coprimo con p para el que tenga solución la siguiente congruencia:*

$$x^2 \equiv n \text{ mód } p$$

Proposición 2.1 *Si p es un primo impar, exactamente la mitad de los enteros a, con* $1 \leq a \leq p-1$*, son residuos cuadráticos módulo p.*

Demostración Definamos el conjunto $S = \{1^2, 2^2, ..., (\frac{p-1}{2})^2\}$, en el que no hay ningún par de números congruentes módulo p, lo que nos indica que al menos tenemos $\frac{p-1}{2}$ residuos cuadráticos.
Por otro lado supongamos que a es un residuo cuadrático. Entonces existe z tal que $z^2 \equiv a$ mód p. Pero como también $(p-z)^2 \equiv (-z)^2 \equiv a$ mód p, y alguno del par $z, -z$ es menor o igual que $\frac{p-1}{2}$, entonces necesariamente $a \in S$, y todo residuo cuadrático tiene que pertenecer a S. Por tanto, hay exactamente $\frac{p-1}{2}$ residuos cuadráticos.

Definición 2.2 (Símbolo de Legendre) *Para cada número primo impar p y cada entero n primo con p, definimos el símbolo de Legendre de n respecto de p como*

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \textit{si } n \textit{ es residuo cuadrático módulo } p \\ -1 & \textit{si } n \textit{ no es residuo cuadrático módulo } p \end{cases}$$

Para completar esta definición, en el caso en el que n sea múltiplo de p, se adopta el convenio $\left(\frac{n}{p}\right) \equiv \left(\frac{0}{p}\right) = 0$.
El teorema que daremos a continuación es un resultado que fue atribuido a John Wilson, que lo dejó anotado en un cuaderno pero sin la demostración correspondiente, y fue Lagrange en 1771 quien dio la primera prueba.

Teorema 2.1 (Teorema de Wilson) *Sea p un entero mayor que 1. Entonces p es primo si y sólo si*

$$(p-1)! \equiv -1 \text{ mód } p$$

Demostración

Observamos primero que los casos $p = 2$ y $p = 3$ son triviales, por lo que supondremos que $p > 3$.

Probaremos primero que "Si p no es primo, $(p-1)! \not\equiv -1$ mód p". Si p tiene algún factor propio d, será $1 < d \leq p-1$ y entonces d divide a $(p-1)!$. Si fuese $(p-1)! \equiv -1$ mód p, resulta que p divide a $(p-1)!+1$ y entonces d divide también a $(p-1)!+1$. Por tanto d tiene que dividir a 1, lo que nos lleva a una contradicción con la hipótesis $d > 1$.

Supongamos ahora que p es primo. Entonces, todos los enteros $1, 2, ..., p-1$ son primos con p. Por otra parte sabemos que estos son los elementos del cuerpo $\mathbb{Z}_p$ de los enteros módulo p. Por ser $\mathbb{Z}_p^*$ grupo, tenemos que $\forall a \in \mathbb{Z}_p$, existe un $b \in \mathbb{Z}_p$, tal que $ab \equiv 1$ mód p, el inverso. Además, los únicos elementos de esta lista que coinciden con su inverso, es decir $a = b$, son aquellos tales que $a^2 \equiv 1$ mód p, que son 1 y $p-1$. Esto es porque si $a^2 \equiv 1$ mód p, que es lo mismo que decir que $a^2 - 1 = (a-1)(a+1) \equiv 0$ mód p, p divide a $(a+1)$ o a $(a-1)$, por lo que $a \equiv \pm 1$ mód p. Con esto llegamos a la conclusión de que el resto de elementos, $2, 3, ..., p-2$, no coinciden con su inverso y lo tienen en ese mismo conjunto. Es decir, este conjunto está formado por pares de inversos distintos entre sí. Por lo que si hacemos el producto de todos ellos obtenemos que

$$2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 \text{ mód } p$$

y como sabemos que $p - 1 \equiv -1$ mód p, añadiéndolo a este producto se obtiene:

$$2 \cdot 3 \cdot ... \cdot (p-2)(p-1) \equiv 1(-1) \text{ mód } p$$

$$(p-1)! \equiv -1 \text{ mód } p$$

El siguiente resultado fue conjeturado por Lambert en 1769 y probado por Euler en 1772.

Teorema 2.2 (Criterio de Euler) *Sea p un primo impar y a un entero primo con p. Entonces*

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \textit{si } a \textit{ es residuo cuadrático módulo } p \\ -1 & \textit{si } a \textit{ no es residuo cuadrático módulo } p \end{cases}$$

Utilizando la notación del símbolo de Legendre, quedaría en la forma

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

Demostración

Para probar este teorema vamos a utilizar el anteriormente demostrado Teorema de Wilson.

Consideramos las parejas de elementos (x, y) tal que $x \leq y \leq p-1$ y $x \cdot y \equiv a$ mód p. Observamos que, para cada $x \in \{1, \ldots, p-1\}$, existe sólo un y tal que $xy = a$. Esto es debido a que si existiese otro y' que lo cumpliese, tendría que ser congruente con y módulo p, y el único entero menor que $p-1$ que lo cumple es él mismo.

Distinguimos las dos posibilidades para a.
Si a no es un residuo cuadrático, los elementos que forman cada uno de los pares posibles tienen que ser necesariamente distintos entre sí. Como hay $p-1$ términos, y por lo tanto $\frac{p-1}{2}$ parejas, si los multiplicamos todos ellos, y utilizamos el teorema de Wilson, obtenemos que

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

Si a es un residuo cuadrático, existirán los pares $(\sqrt{a}, \sqrt{a})$, $(\sqrt{-a}, \sqrt{-a})$ y en el resto de pares estarán los $p-3$ elementos que quedan, siendo todos ellos distintos. Tendremos $\frac{p-3}{2} + 2$ pares, es decir, $\frac{p+1}{2}$. El producto de todos estos pares es $a^{\frac{p+1}{2}}$, y por otra parte, es el producto de los $p-3$ elementos pertenecientes a las parejas de elementos distintos multiplicado dos veces por $\sqrt{a}$ y otras dos por $\sqrt{-a}$ que recordamos que representan a dos enteros menores que $p-1$, es decir, $(p-1)!\sqrt{a}\sqrt{-a}$.

Resulta que

$$a^{\frac{p+1}{2}} \equiv (p-1)!(\sqrt{a})(\sqrt{-a}) = -a(p-1)! \text{ mód } p$$

y entonces

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

Lema 2.1 (Lema de Gauss) *Sean p un número primo impar, n un entero positivo primo con p y*

$$S := n, 2n, ..., \frac{p-1}{2}n$$

Se representa por S' el conjunto formado por todos los restos positivos obtenidos al hacer la división entera por p de los elementos de S y por k el número de elementos de S' que son mayores que $\frac{p}{2}$. Entonces

$$\left(\frac{n}{p}\right) = (-1)^k$$

.

Demostración

En primer lugar observamos que S no contiene ningún elemento múltiplo de p y que tampoco contiene dos elementos distintos que sean congruentes módulo p ya que si $na \equiv nb$ mód p, por ser n primo con p, se cumple que $a \equiv b$ mód p y esto es imposible si $a \neq b$ y $1 \leq a, b \leq \frac{p-1}{2}$. Por tanto, S' contiene $\frac{p-1}{2}$ elementos.

Si llamamos ahora $r_1, ..., r_l$ a los elementos de S' menores que $\frac{p}{2}$ y $s_1, ..., s_k$ a los mayores que $\frac{p}{2}$, demostraremos que

$$\{r_1, ..., r_l, p-s_1, ..., p-s_k\} = \{1, 2, \ldots, \frac{p-1}{2}\} \tag{2.1}$$

Por la definición de los elementos r_i y s_j con $i \in \{1, ..., l\}, j \in \{1, ..., k\}$, sabemos que $1 \leq r_i < \frac{p}{2}$ y que $\frac{p}{2} < s_j < p$. Entonces es evidente que

$$1 \leq r_1, ..., r_l, p-s_1, .., p-s_k < \frac{p}{2}$$

Lo único que necesitamos probar para demostrar la igualdad es que estos elementos son distintos dos a dos.

Puesto que S no contiene dos elementos distintos que sean congruentes módulo p, es claro que los elementos $r_1, \ldots, r_l$ de S' son todos distintos;

lo mismo ocurre para los elementos $s_1, \ldots, s_k$ y también entonces para los elementos $p - s_1, \ldots, p - s_k$

Si $r_i = p - s_j$, para algún par i, j, existe un par de elementos $nx, ny \in S$ con $x \neq y$ y $1 \leq x < y \leq \frac{p-1}{2}$ tales que $nx \equiv -ny$ mód p. Pero entonces es $nx + ny \equiv 0$ mód p y $x \equiv -y$ mód p, lo cual es imposible.

De esta forma queda demostrado que

$$\{r_1, ..., r_l, p - s_1, ..., p - s_k\} = \{1 \leq j \leq \frac{p-1}{2}, j \in \mathbb{Z}\}$$

con lo cual el producto de los elementos del conjunto S' es $(\frac{p-1}{2})!$. Entonces

$$(\frac{p-1}{2})! = \prod_{i=1}^{l} r_i \prod_{j=1}^{k} (p - s_j) \equiv (-1)^k \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \text{ mód } p$$

Teniendo ahora en cuenta que los restos de la división por p de los elementos de S son congruentes módulo p con los elementos de S' se puede escribir

$$(\frac{p-1}{2})! \equiv (-1)^k \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \equiv (-1)^k n^{\frac{p-1}{2}} (\frac{p-1}{2})! \text{ mód } p$$

Como $(\frac{p-1}{2})!$ no es múltiplo de p, simplificamos la congruencia anterior a

$$(-1)^k n^{\frac{p-1}{2}} \equiv 1 \text{ mód } p$$

que equivale a

$$n^{\frac{p-1}{2}} \equiv (-1)^k \text{ mód } p$$

y, aplicando el Criterio de Euler (Teorema 2.2), concluimos que

$$\left(\frac{n}{p}\right) \equiv (-1)^k \text{ mód } p$$

Probaremos ahora algunas propiedades del símbolo de Legendre que nos serán útiles en la realización de las demostraciones del Caítulo 3.

Proposición 2.2 *Sean p un primo impar y n, m dos enteros primos con p. Se cumple que:*

1. $\left(\frac{n^2}{p}\right) = 1$, *en particular* $\left(\frac{1}{p}\right) = 1$.
2. *Si* $n \equiv m$ mód p, *entonces* $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$
3. $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2}$ mód p.
4. $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right)$
5. *Si* k *es un entero no negativo,* $\left(\frac{n^k}{p}\right) = \left(\frac{n}{p}\right)^k$

Demostración

1. Esta propiedad es trivial por la definición de residuo cuadrático.
2. Para probarlo, vamos a considerar 2 casos:
   - Si $\left(\frac{n}{p}\right) = 1$, entonces existe un x tal que $n \equiv x^2$ mód p.
     Como $m \equiv n \equiv x^2$ mód p, entonces $\left(\frac{m}{p}\right) = 1$.
   - Si $\left(\frac{n}{p}\right) = -1$, vamos a demostrarlo por reducción al absurdo. Supongamos que $\left(\frac{m}{p}\right) = 1$, pero entonces, razonando como en el caso anterior, tendremos que $\left(\frac{n}{p}\right) = 1$, lo que contradice nuestra hipótesis.
3. Esta propiedad es la ya probada en el Criterio de Euler (Teorema 2.2).
4. Aplicando de nuevo el criterio de Euler

$$\left(\frac{nm}{p}\right) \equiv (nm)^{(p-1)/2} \text{ mód } p \equiv n^{(p-1)/2} m^{(p-1)/2} \equiv \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right) \text{ mód } p$$

5. Esta propiedad se deduce directamente de la anterior:

$$\left(\frac{n^k}{p}\right) = \left(\frac{n}{p}\right) \overset{k)}{\cdots} \left(\frac{n}{p}\right) = \left(\frac{n}{p}\right)^k$$

.

La Ley de Reciprocidad Cuadrática sólo se aplica a los casos en los que p y q son primos impares, por lo que, para poder calcular el valor de cualquier símbolo de Legendre $\left(\frac{n}{p}\right)$, necesitaremos saber respecto de qué primos p son 2 y -1 restos cuadráticos.

Lema 2.2 *Si p es un primo impar:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & si\ p \equiv 1 \text{ mód } 4 \\ -1 & si\ p \equiv 3 \text{ mód } 4 \end{cases}$$

Demostración Usando el Criterio de Euler, sabemos que

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

Por lo tanto lo único que hay que analizar es la paridad de $\frac{p-1}{2}$, es decir, el valor de p módulo 4. Si $p \equiv 1$ mód 4, la fracción anterior es un número par, luego $\left(\frac{-1}{p}\right) = 1$.
En otro caso, por ser p impar, será $p \equiv 3$ mód 4. Entonces $\frac{p-1}{2}$ será un número impar y $\left(\frac{-1}{p}\right) = -1$ si $p \equiv 3$ mód 4.

Lema 2.3 *Si p es un primo impar:*

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

Demostración

Llamemos $s = \frac{p}{2}$ para simplificar la notación. Se sabe por el Lema de Gauss (Lema 2.1) que si k es el número de residuos módulo p de los elementos de $S = \{2, 4, 6, ..., p-1\}$ que son mayores que s, se cumple que $(-1)^k = \left(\frac{2}{p}\right)$.

Por otro lado, teniendo en cuenta que cada elemento de S coincide con su resto al dividirlo por p, puede considerarse k como el número de enteros de la forma $2x$ tales que $s = \frac{p}{2} < 2x < p$. Estas desigualdades equivalen, por ser p impar, a $\frac{p}{4} < x \leq \frac{p-1}{2}$, por lo que

$$k = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$$

siendo $\lfloor \frac{p}{4} \rfloor$ la parte entera de la fracción $\frac{p}{4}$.

Ahora, considerando las únicas 4 posibilidades de un p primo impar en módulo 8, ya que lo que nos interesa es la paridad de k, obtenemos lo siguiente:

- $p = 8n+1$: En este caso $k = 4n - \lfloor 2n + \frac{1}{4} \rfloor = 4n - 2n = 2n$. Por lo que k va a ser par y obtenemos que si $p \equiv 1$ mód 8, entonces $\left(\frac{2}{p}\right) = 1$.

- $p = 8n+3$: En este caso $k = 4n+1-\lfloor 2n + \frac{3}{4} \rfloor = 4n+1-2n = 2n+1$. Por lo que k va a ser impar y obtenemos que si $p \equiv 3$ mód 8, entonces $\left(\frac{2}{p}\right) = -1$.

- $p = 8n+5$: En este caso $k = 4n+2-\lfloor 2n + \frac{5}{4} \rfloor = 4n+2-2n-1 = 2n+1$. Por lo que k va a ser impar y obtenemos que si $p \equiv 5$ mód 8, entonces $\left(\frac{2}{p}\right) = -1$.

- $p = 8n+7$: En este caso $k = 4n+3-\lfloor 2n + \frac{7}{4} \rfloor = 4n+3-2n-1 = 2n+2$. Por lo que k va a ser par y obtenemos que si $p \equiv 7$ mód 8, o entonces $\left(\frac{2}{p}\right) = 1$.

En resumen, hemos obtenido que

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & si\ p \equiv \pm 1 \text{ mód } 8 \\ -1 & si\ p \equiv \pm 3 \text{ mód } 8 \end{cases}$$

Ahora comparamos lo obtenido con la expresión dada en el enunciado.

Si $p \equiv \pm 1$ mód 8, $p = 8n \pm 1$. Entonces $p^2 - 1 = (p+1)(p-1) = 64n^2 \pm 16n$ y $\frac{p^2-1}{8} = 8n \pm 2n$ es par.

Por otra parte, si $p \equiv \pm 3$ mód 8, $p = 8n \pm 3$. Entonces $p^2 - 1 = 64n^2 \pm 48n + 8$ y $\frac{p^2-1}{8} = 8n \pm 6n + 1$ es impar.

Antes de terminar con este capítulo vamos a ver un ejemplo de cómo se utiliza la Ley de Reciprocidad Cuadrática para calcular un símbolo de Legendre, en el que utilizaremos además algunas de las propiedades que ya hemos visto de dicho símbolo.

Calculamos $\left(\frac{11}{61}\right)$. Lo primero apliquemos la LRC:

$$\left(\frac{11}{61}\right) = (-1)^{\frac{10}{2}\frac{60}{2}} \left(\frac{61}{11}\right) = \left(\frac{61}{11}\right) = \left(\frac{-5}{11}\right)$$

Apliquemos la propiedad 4 de la Proposición 2.2, y la LRC otra vez:

$$\left(\frac{-5}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{5}{11}\right) = \left(\frac{-1}{11}\right)(-1)^{\frac{4}{2}\frac{10}{2}} \left(\frac{11}{5}\right) = \left(\frac{-1}{11}\right)\left(\frac{1}{5}\right)$$

Utilizando por último el Lema 2.2.

$$\left(\frac{-1}{11}\right)\left(\frac{1}{5}\right) = \left(\frac{-1}{11}\right) = (-1)^{10/2} = -1$$

Capítulo 3

Demostraciones

3.1. Tercera demostración de Gauss

Teorema 3.1 *Si p y q son números primos distintos se tiene*

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

Demostración:
La demostración se basa en el Lema de Gauss, ya demostrado anteriormente (Lema 2.1) y se divide en dos partes. Sea $\lfloor n/p \rfloor$ la representación de la parte entera de la fracción $\frac{n}{p}$, es decir, el cociente de la división entera de n entre p.

Por una parte vamos a demostrar que, si n es un entero impar, p un primo tal que $mcd(n,p) = 1$ y $\rho = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jn}{p} \rfloor$, entonces

$$\left(\frac{n}{p}\right) = (-1)^{\rho} \tag{3.1}$$

Sea S' como en el Lema 2.1, $r_1, \ldots, r_l$ los elementos de S' menores que $\frac{p}{2}$ y $s_1, \ldots, s_k$ los elementos de S' mayores que $\frac{p}{2}$.

Para cada $j \in \{1, \ldots, \frac{p-1}{2}\}$, es $jn = \lfloor \frac{jn}{p} \rfloor p + t$ con $t \in S'$ y es evidente la siguiente igualdad

$$\sum_{j=1}^{\frac{p-1}{2}} jn = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jn}{p} \rfloor p + \sum_{i=1}^{l} r_i + \sum_{i=1}^{k} s_i \tag{3.2}$$

Por otra parte, teniendo en cuenta que $\{r_1, \ldots, r_l, p - s_1, \ldots, p - s_k\} = \{1, 2 \ldots, \frac{p-1}{2}\}$, resulta

$$\sum_{1}^{\frac{p-1}{2}} j = \sum_{i=1}^{l} r_i + \sum_{j=1}^{k} (p - s_j) = \sum_{i=1}^{l} r_i + kp - \sum_{j=1}^{k} s_j \tag{3.3}$$

y restando la ecuación (3.3) de la ecuación (3.2):

$$(n-1) \sum_{1}^{\frac{p-1}{2}} j = p(\sum_{j=1}^{\frac{p-1}{2}} \lfloor jn/p \rfloor - k) + 2 \sum_{j=1}^{k} s_j$$

Analizamos ahora la paridad de cada uno de los miembros de esta ecuación.

Como n es impar, la parte izquierda de la ecuación es par, al igual que $2 \sum_{j=1}^{k} s_j$. Entonces, por ser p impar, $\sum_{j=1}^{\frac{p-1}{2}} \lfloor jn/p \rfloor - k$ tiene que ser par y, por lo tanto tanto, $\sum_{j=1}^{\frac{p-1}{2}} \lfloor jn/p \rfloor$ y k deben tener la misma paridad. Esto nos lleva a que

$$(-1)^{\rho} = (-1)^k$$

y aplicando el Lema de Gauss se cumple que

$$(-1)^k = \left(\frac{n}{p}\right)$$

La segunda parte de la demostración va a consistir en demostrar que si p y q son dos primos impares distintos, entonces

$$\frac{(p-1)(q-1)}{4} = \sum_{j=1}^{(p-1)/2} \lfloor jq/p \rfloor + \sum_{k=1}^{\frac{q-1}{2}} \lfloor kp/q \rfloor \tag{3.4}$$

Para ello vamos a calcular la suma

$$\rho = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$$

Vamos a suponer $q < p$. Con esta suposición, vamos a analizar los valores que toman cada uno de los sumandos:

- El primer sumando, que corresponde a $j = 1$, tiene valor 0.
- El último sumando ($j = \frac{p-1}{2}$) se puede escribir de la siguiente manera :

$$\left\lfloor \frac{\frac{p-1}{2}q}{p} \right\rfloor = \left\lfloor \frac{p\frac{q-1}{2} + \frac{p-q}{2}}{p} \right\rfloor$$

en la que podemos ver fácilmente que el valor de este término es de $\frac{q-1}{2}$.

El número de sumandos que tenemos es $\frac{p-1}{2}$, y los valores de los dos que acabamos de calcular nos indican que el valor de cada uno de los sumandos estará comprendido entre 0 y $\frac{q-1}{2}$, por lo que es evidente que vamos a tener sumandos que tengan el mismo valor; como además los elementos $\frac{jq}{p}$ están igualmente espaciados, para cada n tal que $0 \leq n \leq \frac{q-1}{2}$ habrá algún sumando que tome ese valor.
Por lo tanto nuestra forma de calcular ρ va a ser agrupando los sumandos según el valor que toman y contando cuántos hay para cada uno de los valores posibles.
Para ello vamos a considerar dos sumandos consecutivos que cumplan lo siguiente

$$\left\lfloor \frac{jq}{p} \right\rfloor = n - 1 \qquad \left\lfloor \frac{(j+1)q}{p} \right\rfloor = n$$

Entonces

$$\frac{jq}{p} < n < \frac{(j+1)q}{p} \Rightarrow j < \frac{np}{q} < j + 1 \Rightarrow \left\lfloor \frac{np}{q} \right\rfloor = j$$

Esto quiere decir que, fijado n, todos los sumandos hasta el valor $j = \left\lfloor \frac{np}{q} \right\rfloor$, tienen valor menor que n, y el siguiente ya toma el valor n. Se deduce ahora que el número de términos de la suma que toman el valor exacto n será

$$\left\lfloor \frac{(n+1)p}{q} \right\rfloor - \left\lfloor \frac{np}{q} \right\rfloor$$

.

Teniendo esto en cuenta, se escribe la suma con sus sumandos agrupados según el valor que toman y se evalúa cada grupo multiplicando el valor que

toman sus sumandos por el número de estos. Tendremos

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor &= 1\left(\left\lfloor\frac{2p}{q}\right\rfloor-\left\lfloor\frac{p}{q}\right\rfloor\right)+2\left(\lfloor\frac{3p}{q}\rfloor-\lfloor\frac{2p}{q}\rfloor\right)+\\ &\quad+\cdots+\frac{q-1}{2}\left(\frac{p-1}{2}-\left\lfloor\frac{\frac{q-1}{2}p}{q}\right\rfloor\right)\\ &= -\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{kp}{q}\right\rfloor+\frac{q-1}{2}\frac{p-1}{2}\end{aligned}$$

Por lo que la ecuación (3.4) queda demostrada.

Para finalizar la demostración, si utilizamos la notación siguiente para simplificar

$$\rho_1 := \sum_{j=1}^{\frac{p-1}{2}}\lfloor jq/p\rfloor \qquad \rho_2 := \sum_{k=1}^{\frac{q-1}{2}}\lfloor kp/q\rfloor$$

y tenemos en cuenta (3.4) y (3.1), resulta que

$$(-1)^{(p-1)(q-1)/4} = (-1)^{\rho_1+\rho_2} = (-1)^{\rho_1}(-1)^{\rho_2} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

3.1.1. Aportación de Eisenstein

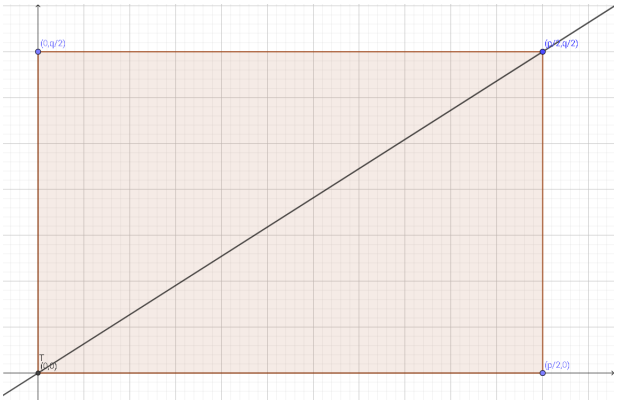
Esta prueba fue publicada en 1844 ([6]) y simplifica la tercera prueba de Gauss proporcionando además una original forma de demostrar la ecuación (3.4).

Dados dos primos impares distintos p, q, se considera, en el plano ordinario, el rectángulo R con vértices $(0,0)$, $(0,\frac{q}{2})$, $(\frac{p}{2},0)$, $(\frac{p}{2},\frac{q}{2})$ y se cuentan de dos formas distintas el número de puntos de coordenadas enteras que hay en el interior de R.

Es claro que los puntos (x,y) del interior de R con $x,y\in\mathbb{Z}$ son aquellos tales $0<x\leq\frac{p-1}{2}$ y $0<y\leq\frac{q-1}{2}$. Por tanto, el número total de puntos con coordenadas enteras en el interior de R es $\frac{p-1}{2}\frac{q-1}{2}$, valor que coincide con el primer miembro de la ecuación (3.4).

Para ver la igualdad con el otro miembro de (3.4), contaremos esos mismos puntos de una manera diferente. Para ello, trazamos la diagonal T que pasa por los vértices $(0,0)$ y $(\frac{p}{2},\frac{q}{2})$.

$$T := \{(x,y) \in \mathbb{R}^2 : qx = py\}$$



La recta T no contiene ningún punto de coordenadas enteras del interior de R ya que, como q y p son dos números primos distintos, los puntos de coordenadas enteras que están en T son todos de la forma (pu, qu) con $u \in \mathbb{Z}$. Determinaremos ahora cuántos puntos hay en el interior de R contando los que hay por encima y por debajo de la recta T.

Contamos primero los que están por debajo de T.

Puesto que $T = \{(x,y)$, con $y = \frac{q}{p}x, 0 \leq x \leq \frac{p}{2}, 0 \leq y \leq \frac{q}{2}\}$, los puntos del rectángulo con coordenadas enteras que están bajo T son aquellos (j,l) tales que $1 \leq l \leq qj/p$ y, evidentemente, el cardinal de este conjunto es $\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor$.

De la misma forma, obtenemos que el número de puntos por encima de la diagonal es de $\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor$. Sumando las dos cantidades obtenemos el segundo miembro de (3.4), por lo que queda demostrada la igualdad.

3.1.2. Aportación de Kronecker

Kronecker también publicó una demostración de la ley de reciprocidad cuadrática a partir de la tercera demostración de Gauss ([10]).

Como hemos hecho hasta ahora, supondremos que p y q son primos impares, y sea $j \in \mathbb{Z}$ tal que $1 \leq j \leq \frac{p-1}{2}$. Primero vamos a demostrar que, utilizando la notación que hemos venido usando hasta ahora,

$$(-1)^{\lfloor \frac{jq}{p} \rfloor} = sign \prod_{k=1}^{\frac{q-1}{2}} \left(\frac{k}{q} - \frac{j}{p} \right)$$

Para estudiar esta igualdad, lo que debemos mirar es cuándo $\frac{j}{p} > \frac{k}{q}$. Observamos que $\frac{k}{q} - \frac{j}{p} = 0$ cuando $k = \frac{jq}{p}$. Por lo tanto, los factores negativos son los correspondientes a los k tales que $k < \frac{jq}{p}$, que es lo mismo que decir que habrá $\left\lfloor \frac{jq}{p} \right\rfloor$ resultados negativos, por lo que se cumple la igualdad.

Utilizando la igualdad demostrada anteriormente para cada $j \in \{1, \ldots, \frac{p-1}{2}\}$ y multiplicando todas estas igualdades, resulta

$$sign \left(\prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} \left(\frac{k}{q} - \frac{j}{p} \right) \right) = sign \left(\prod_{j=1}^{\frac{p-1}{2}} (-1)^{\lfloor \frac{jq}{p} \rfloor} \right) = (-1)^{\lfloor \frac{p}{q} \rfloor + \lfloor \frac{2p}{q} \rfloor + \ldots + \lfloor \frac{\frac{q-1}{2}p}{q} \rfloor}$$

Ahora, la igualdad (3.1) demostrada antes en Teorema 3.1, afirma que

$$(-1)^{\lfloor \frac{p}{q} \rfloor + \lfloor \frac{2p}{q} \rfloor + \ldots + \lfloor \frac{\frac{q-1}{2}p}{q} \rfloor} = \left(\frac{p}{q} \right)$$

y entonces,

$$sign \left(\prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} \left(\frac{k}{q} - \frac{j}{p} \right) \right) = \left(\frac{p}{q} \right)$$

Por simetría, obtenemos que

$$sign \left(\prod_{k=1}^{\frac{q-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} \left(\frac{j}{p} - \frac{k}{q} \right) \right) = \left(\frac{q}{p} \right)$$

Realizamos el producto de estas dos igualdades y, puesto que

$$sign \left(\prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} \left(\frac{k}{q} - \frac{j}{p} \right) \right) sign \left(\prod_{k=1}^{\frac{q-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} \left(\frac{j}{p} - \frac{k}{q} \right) \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

obtenemos la ley de reciprocidad cuadrática.

3.2. Cuarta demostración de Gauss

Esta demostración es una de las más conocidas. En ella se utilizan las sumas cuadráticas de Gauss.

Antes de empezar la demostración definiremos lo que es una raíz primitiva de la unidad.

Definición 3.1 *Un número complejo ζ es una raíz n-ésima de la unidad si cumple que $\zeta^n = 1$ para algún $n > 0$. Si además ese n es el menor entero positivo que cumple esta propiedad, se dice que ζ es una raíz n-ésima primitiva de la unidad.*

Damos ahora una pequeña lista de propiedades:

- Para cada entero positivo $n > 1$, las raíces n-ésimas de la unidad en $\mathbb{C}$ son 1, $e^{2\pi i/n}$, $e^{2(2\pi i/n)}$,..., $e^{(n-1)(2\pi i/n)}$. De la lista anterior, son raíces primitivas n-simas las de la forma $e^{k(2\pi i/n)}$, con k y n coprimos.

- Si ζ es una n-ésima raiz de la unidad y $m \equiv l$ mód n, entonces se cumple que $\zeta^m = \zeta^l$. Si añadimos la condición de que ζ sea raíz primitiva, se cumple que
$$\zeta^m = \zeta^l \Leftrightarrow m \equiv l \text{ mód } n$$

En lo que sigue, será $\zeta = e^{2\pi i/p}$ con p primo impar.

Lema 3.1 $\sum_{t=0}^{p-1} \zeta^{at} = p$ *si* $a \equiv 0$ mód p. *Si* $a \not\equiv 0$ mód p, *es* $\sum_{t=0}^{p-1} \zeta^{at} = 0$.

Demostración

Si $a \equiv 0$ mód p, entonces $\zeta^a = 1$ y $\sum_{t=0}^{p-1} \zeta^{at} = p$.

Si $a \not\equiv 0$ mód p, entonces $\zeta^a \neq 1$ y

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0$$

.

Se deduce de este resultado que, si se define $\delta(x, y) = p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)}$, se cumple que $\delta(x, y) = 1$ si $x \equiv y$ mód p y $\delta(x, y) = 0$ si $x \not\equiv y$ mód p.

Lema 3.2 $\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$.

Demostración Por la definición de símbolo de Legendre, $\left(\frac{0}{p}\right) = 0$. Además sabemos por la Proposición 2.1 que el resto de los $p-1$ términos $\left(\frac{t}{p}\right)$ de la suma valen la mitad +1 y la otra mitad -1.

Definamos ahora las sumas de Gauss

Definición 3.2 *Para cada entero a, se define la suma cuadrática de Gauss* $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$.

Proposición 3.1 $g_a = \left(\frac{a}{p}\right) g_1$

Demostración Si $a \equiv 0$ mód p, entonces $\zeta^{at} = 1\ \forall t$, y $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$ por el Lema 3.2. Supongamos ahora que $a \not\equiv 0$ mód p. Entonces

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g_1$$

Para la última igualdad lo único que hemos utilizado es que, cuando t varía entre 0 y $p-1$, at recorre todos los restos módulo p y que $\left(\frac{x}{p}\right)$ y ζ^x dependen solo del valor de x módulo p.
Como se cumple siempre que $\left(\frac{a}{p}\right) = \pm 1$, multiplicando la ecuación $\left(\frac{a}{p}\right) g_a = g_1$ a ambos lados por $\left(\frac{a}{p}\right)$, resulta que

$$g_a = \left(\frac{a}{p}\right) g_1$$

Desde ahora denotaremos g_1 como g. De la Proposición 3.1 obtenemos que $g_a^2 = g^2$ si $a \not\equiv 0$ mód p. Ahora veamos cuánto vale g^2.

Proposición 3.2 $g^2 = (-1)^{(p-1)/2} p$.

Demostración Vamos a calcular el valor del sumatorio $\sum_{a=1}^{p-1} g_a g_{-a}$ de dos formas distintas. Si $a \not\equiv 0$ mód p, entonces $g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2$ y resulta que

$$\sum_{a=1}^{p-1} g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1) g^2$$

Por otra parte, utilizamos la definición 3.2, para cada a tenemos

$$g_a g_{-a} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}$$

Sumando las ecuaciones anteriores que corresponden a los valores de a desde 1 hasta $p-1$ y utilizando el Lema 3.1

$$\sum_{a=1}^{p-1} g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \delta(x,y)p = (p-1)p$$

Viendo estos dos resultados juntos obtenemos que $\left(\frac{-1}{p}\right)(p-1)g^2 = (p-1)p$. Entonces,

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

Sea ahora $p^* = (-1)^{\frac{p-1}{2}} p$ y q otro primo impar. Entonces,

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \text{ mód } q$$

y $g^q \equiv \left(\frac{p^*}{q}\right) g$ mód q. Por otro lado,

$$g^q \equiv \left(\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t\right)^q \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)^q \zeta^{qt} = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{qt} = g_q \text{ mód } q$$

Ya sabemos que $g^q \equiv g_q = \left(\frac{q}{p}\right) g$ mód q y entonces $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g$ mód q Multiplicamos los dos miembros de esta ecuación por g, y utilizando el resultado $g^2 = p^*$,resulta $\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^*$ mód q. Por tanto,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

Deshaciendo la notación de p^*, tenemos finalmente, que

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

3.3. Quinta demostración de Gauss

Teorema 3.2 *Sean p y q primos impares distintos. Sea n el número de restos positivos mayores que $\frac{q}{2}$ que obtenemos al dividir el conjunto $N = \{p, 2p, \ldots, \frac{q-1}{2}p\}$ entre q y sea m el número de restos positivos mayores que $\frac{p}{2}$ que obtenemos de dividor el conjunto $M = \{q, 2q, \ldots, \frac{p-1}{2}q\}$ entre p. Entonces o n, m y $\frac{(p-1)(q-1)}{4}$ son todos pares, o dos son impares y uno par. Que es lo mismo que decir que*

$$(-1)^m(-1)^n(-1)^{\frac{(p-1)(q-1)}{4}} = 1$$

Demostracion

Para esta demostración hemos de dar mucha notación y además definir muchos elementos:

- Se define $r = \frac{p-1}{2}\frac{q-1}{2}$.
- Denotamos como $\bar{y}_k$ al menor resto no negativo de la división de y entre k.
- Para un conjunto cualquiera S, $|S|$ indicará su cardinal.
- Definimos los conjuntos

$$r_p = \{1, \ldots, \frac{p-1}{2}\} \qquad R_p = \{\frac{p+1}{2}, \ldots, p-1\}$$

$$r_q = \{1, \ldots, \frac{q-1}{2}\} \qquad R_q = \{\frac{q+1}{2}, \ldots, q-1\}$$

Por cómo hemos definido n y m, tenemos claramente que

$$|\{x \in r_q : \overline{px}_q \in R_q\}| = n$$

$$|\{x \in r_p : \overline{qx}_p \in R_p\}| = m$$

- Y definimos estos dos conjuntos disjuntos

$$t = \{1, 2, \ldots, \frac{pq-1}{2}\} \qquad T = \{\frac{pq+1}{2}, \ldots, pq-1\}$$

cuya unión es $\mathcal{U} = \{1, 2, ..., pq-1\}$.

- Por último vamos a dividir t y T en 8 subconjuntos distintos:

$$\begin{aligned} t_1 &= \{y \in t : \bar{y}_p \in r_p,\ \bar{y}_q \in r_q\} \\ t_2 &= \{y \in t : \bar{y}_p \in r_p,\ \bar{y}_q \in R_q\} \\ t_3 &= \{y \in t : \bar{y}_p \in R_p,\ \bar{y}_q \in r_q\} \\ t_4 &= \{y \in t : \bar{y}_p \in R_p,\ \bar{y}_q \in R_q\} \\ t_5 &= \{y \in t : y \equiv 0 \text{ mód } p,\ \bar{y}_q \in r_q\} \\ t_6 &= \{y \in t : y \equiv 0 \text{ mód } p,\ \bar{y}_q \in R_q\} \\ t_7 &= \{y \in t : \bar{y}_p \in r_p,\ y \equiv 0 \text{ mód } q\} \\ t_8 &= \{y \in t : \bar{y}_p \in R_p,\ y \equiv 0 \text{ mód } q\} \end{aligned}$$

  Esta misma subdivisión es la que hacemos en T representando por T_i el subconjunto análogo a t_i para cada $i = 1, 2, \ldots, 8$.

Ahora vamos a dar una lista de propiedades relativas a los cardinales de estos subconjuntos:

a) Por una parte, notemos que

$$|t_6| = |\{y = px \in N,\ \bar{y}_q \geq \frac{q+1}{2}\}| = n$$

$$|t_8| = |\{y = qx \in M,\ \bar{y}_p \geq \frac{p+1}{2}\}| = m$$

b) $|t_i| + |T_i| = r$ para cada $i = 1, \ldots 4$.

Calculamos el cardinal del conjunto

$$t_1 \cup T_1 = \{y \in \mathcal{U} : \bar{y}_p \in r_p,\ \bar{y}_q \in r_q\}$$

que está formado por todos los $y \in \mathcal{U}$ tal que

$$y \equiv \tau_1 \text{ mód } q$$

$$y \equiv \tau_2 \text{ mód } p$$

con $0 < \tau_1 \leq \frac{q-1}{2}$ y $0 < \tau_2 \leq \frac{p-1}{2}$. Por el teorema Chino de los Restos sabemos que, como p y q son coprimos, para cada par de τ_i, τ_j, existe

un único $y \in \mathcal{U}$ que cumpla esas condiciones, por lo tanto tendremos que

$$|t_1 \cup T_1| = \frac{p-1}{2}\frac{q-1}{2} = r$$

y como t_1 y T_1 son disjuntos llegamos a que

$$|t_1| + |T_1| = r$$

De esta misma manera se comprueba que

$$|t_i| + |T_i| = r, \ \forall i \in \{1, 2, 3, 4\}$$

.

c)

$$\begin{array}{llll} |t_1| = |T_4|, & |t_2| = |T_3|, & |t_3| = |T_2|, & |t_4| = |T_1|, \\ |t_5| = |T_6|, & |t_6| = |T_5|, & |t_7| = |T_8|, & |t_8| = |T_7| \end{array}$$

Probaremos que $|t_1| = |T_4|$: Sea $y \in t_1$. Por una parte tenemos que

$$y \in t \Rightarrow y \leq \frac{pq-1}{2} \Rightarrow pq - y \geq pq - \frac{pq-1}{2} = \frac{pq+1}{2} \Rightarrow pq - y \in T$$

Por otra parte, $y \in t_1 \Leftrightarrow \bar{y}_p \in r_p$ y $\bar{y}_q \in r_q$.

$\bar{y}_p \in r_p$ es lo mismo que decir que $y \equiv \tau_1$ mód p con $\tau_1 \leq \frac{p-1}{2}$, y por lo tanto $pq - y \equiv -\tau_1 \equiv p - \tau_1 \ mod \ p$ con $p - \tau_1 \geq \frac{p-1}{2}$ y por tanto $\overline{(pq-y)}_p \in R_p$.

A partir de que $\overline{y}_q \in r_q$, por el mismo procedimiento se llega a que si $\overline{pq-y} \in R_q$. Ya tenemos probado que $pq - y \in T_4$.

Se observa ahora que la aplicación $y \mapsto pq - y$ es una biyección entre t_1 y T_4 , por lo que $|t_1| = |T_4|$.

Por el mismo procedimiento se comprueban las restantes igualdades.

d) De lo obtenido en b) y c) resulta que

$$|t_1| + |t_4| = |t_1| + |T_1| = r \tag{3.5}$$

$$|t_2| + |t_3| = |t_2| + |T_2| = r \tag{3.6}$$

e) $|t_2|+|t_4|+|t_6| = r$, $|t_3|+|t_4|+|t_8| = r$, $|t_1|+|t_3|+|t_5| = r$, $|t_1|+|t_2|+|t_7| = r$

Observemos que $t_2 \cup t_4 \cup t_6 = \{y \in t : \bar{y}_q \in R_q\}$. Es decir, los elementos de este conjunto cumplen que $y = qx + \tau_1$ con $\tau_1 \in \{\frac{q+1}{2}, ..., q-1\}$ y $0 \leq x < \frac{p-1}{2}$. $x = \frac{p-1}{2}$ no está incluido porque en ese caso tendríamos que

$$y = qx + \tau_1 \geq q\frac{p-1}{2} + \frac{q+1}{2} = q(\frac{p-1}{2} + \frac{1}{2}) + \frac{1}{2} = \frac{qp+1}{2} > \frac{pq-1}{2}$$

.

Hay $\frac{p-1}{2}$ valores posibles para τ_1 y $\frac{q-1}{2}$ valores posibles para x; por lo tanto el número de elementos de $t_2 \cup t_4 \cup t_6$ es r y, como los tres subconjuntos son disjuntos, tenemos que

$$|t_2| + |t_4| + |t_6| = r$$

De la misma manera vemos que $t_3 \cup t_4 \cup t_8 = \{x \in t : \bar{y}_p \in R_p\}$ tiene también r elementos y por tanto

$$|t_3| + |t_4| + |t_8| = r$$

Y lo mismo se cumple para los siguientes:

$$|t_1| + |t_3| + |t_5| = r$$

$$|t_1| + |t_2| + |t_7| = r$$

f) $|t_2| + |t_4| + n = r$ y $|t_3| + |t_4| + m = r$.

Como $|t_6| = n$ y $|t_8| = m$, se deduce de e) que

$$|t_2| + |t_4| + n = r \tag{3.7}$$

$$|t_3| + |t_4| + m = r \tag{3.8}$$

Lo que nos interesa para demostrar el teorema es la paridad de n m y r. Para ello, vamos a realizar algunas operaciones con las ecuaciones que hemos obtenido en (3.5), (3.6), (3.7) y (3.8):

- De la operación
$$2(3{,}5) + (3{,}6) - (3{,}7) - (3{,}8)$$
resulta que $2|t_1| - n - m = r$, de donde
$$2|t_1| = n + m + r$$

- De (3,6) + (3,7) − (3,8) resulta que $2|t_2| + n - m = r$ y

$$2|t_2| = m - n + r$$

- De (3,6) − (3,7) + (3,8) resulta que $2|t_3| - n + m = r$ y

$$2|t_3| = n - m + r$$

- De −(3,6) + (3,7) + (3,8) resulta que $2|t_4| + n + m = r$ y

$$2|t_4| = -m - n + r$$

Al observar las ecuaciones anteriores, se deduce que $(-1)^{n+m} = (-1)^r$. Por tanto, $(-1)^{n+m+r} = 1$ y

$$(-1)^m(-1)^n(-1)^{\frac{(p-1)(q-1)}{4}} = 1$$

Teorema 3.3 (La Ley de Reciprocidad Cuadrática) *Sean p y q dos primos impares distintos.*

1. *Si al menos uno de los dos primos es congruente con 1 módulo 4, entonces o bien uno es residuo cuadrático respecto del otro y viceversa, o ninguno de los dos lo es.*

2. *Si los dos primos p y q son congruentes con 3 módulo 4, entonces solamente y obligatoriamente uno de ellos es residuo cuadrático respecto del otro.*

Demostración
Si al menos uno de los dos primos es congruente con 1 módulo 4, entonces $\frac{(p-1)(q-1)}{4}$ es par, y por el teorema anterior entonces n y m son o bien pares los dos o bien impares los dos, y así, por el lema de Gauss, vemos que si n y m par entonces

$$\left(\frac{p}{q}\right) = 1 \quad \text{y} \quad \left(\frac{q}{p}\right) = 1$$

y por tanto uno residuo cuadrático del otro. Y por el contrario si n y m fueran impares entonces

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

y entonces ninguno sería residuo cuadrático del otro. Y para demostrar la segunda parte del teorema, caso en el que p y q son congruentes con 3 módulo 4, entonces $\frac{(p-1)(q-1)}{4}$ es impar, por lo que solamente o n o m va a ser par, y en ese caso, volviendo a aplicar de la misma manera el lema de Gauss, obtenemos que solamente uno de los dos números primos es residuo cuadrático del otro, y con esto concluimos la demostración.

3.4. Demostración de Eisenstein

Eisenstein trabajó mucho en este resultado. Además de su interesante aportación a la tercera prueba de Gauss que ya hemos comentado en el apartado 3.1.1, obtuvo una ingeniosa prueba, basada en el uso de funciones trigonométricas, que se expone a continuación.

La demostración que vamos a exponer se basa en propiedades de la función $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2isen2\pi z$ entre las cuales tenemos:

a) $f(z+1) = f(z)$ puesto que

$$e^{2\pi i(z+1)} - e^{-2\pi i(z+1)} = e^{2\pi iz}e^{2\pi i} - e^{-2\pi iz}e^{-2\pi i} = e^{2\pi iz} - e^{-2\pi iz}$$

b) $f(-z) = e^{-2\pi iz} - e^{2\pi iz} = -f(z)$.

c) Además, $z \in \mathbb{R}$ es una raíz de $f(z)$ si y sólo si $e^{4\pi iz} = 1$, lo que equivale a que $z = \frac{t}{2}$ para algún entero t.

Lema 3.3 *Si $n > 0$ es impar se cumple 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 Sean 1,ζ, ζ^2,..., ζ^{n-1} las raíces del polinomio $z^n - 1$. Como hay n de ellas y todas son distintas, podemos escribir

$$z^n - 1 = \prod_{k=0}^{n-1}(z - \zeta^k)$$

Haciendo $z = \frac{x}{y}$ y multiplicando toda la ecuación por y^n, se obtiene

$$x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^k y)$$

Como n es impar no importa que cambiemos k por $-2k$, ya que recorreremos igualmente el sistema completo de residuos módulo n, difiriendo únicamente en el orden en el que salen esas raíces. Por lo tanto podemos escribir

$$x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^{-2k} y) = \zeta^{-(1+2+..+n-1)} \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y)$$

Como n es impar, $1 + 2 + .. + (n-1) = n\frac{n-1}{2}$ es múltiplo de n y, por lo tanto, $\zeta^{-(1+2+..+n-1)} = 1$. Entonces finalmente podemos escribir la ecuación

$$x^n - y^n = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y)$$

Probamos ahora una interesante propiedad de la función $f(z)$.

Proposición 3.3 *Si n es un entero positivo impar y $f(z)$ es la anteriormente definida, entonces*

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

Demostración

Sustituyendo $x = e^{2\pi iz}$ e $y = e^{-2\pi iz}$ en el lema anterior, resulta

$$f(nz) = e^{2\pi izn} - e^{-2\pi izn} = \prod_{k=0}^{n-1}(e^{2\pi ik/n} e^{2\pi iz} - e^{-2\pi ik/n} e^{-2\pi iz}) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right)$$

Para dividir este resultado por $f(z)$, unicamente tenemos que eliminar el factor correspondiente a $k = 0$.

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

y, como $f(z+\frac{k}{n}) = f(z+\frac{k}{n}-1) = f(z-\frac{n-k}{n})$, resulta

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

Ahora es claro que cuando k recorre los valores del segundo producto, $n-k$ recorre desde $(n-1)/2$ hasta 1. Por lo tanto finalizamos que

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

Proposición 3.4 *Si p es un primo impar y a es un entero no divisible por p, 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

Para cada $l \in \{1, 2, \ldots, \frac{p-1}{2}\}$, se cumple que $la \equiv \pm m_l$ mód p con $m_l \in \{1, \ldots, \frac{p-1}{2}\}$. Por tanto, $\frac{la}{p} = \pm\frac{m_l}{p} + t$ para algún $t \in \mathbb{Z}$. Entonces, por las propiedades a) y b) anteriores,

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

Multiplicando ahora estas igualdades cuando l recorre el conjunto $\{1, 2, \ldots, \frac{p-1}{2}\}$ y, usando el Lema de Gauss (Lema 2.1), resulta

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

Teniendo ya probadas estas propiedades, vamos a demostrar finalmente la Ley de Reciprocidad Cuadrática.

Sean p y q primos impares. Por la Proposición 3.4

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

y, por Proposición 3.3

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

Veamos que obtenemos de unir las dos ecuaciones anteriores

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

y de la misma manera

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

Como $f(\frac{k}{q}-\frac{l}{p}) = -f(\frac{l}{p}-\frac{k}{q})$, llegamos a que $\frac{\left(\frac{q}{p}\right)}{\left(\frac{p}{q}\right)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ y entonces

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

que es justamente la Ley de Reciprocidad Cuadrática.

3.5. Demostración de Rousseau

Esta demostración se basa en la siguiente versión del Teorema Chino de los Restos:

Teorema 3.4 *Si p, q son primos impares distintos y se representan por $U(\mathbb{Z}_{pq})$, $U(\mathbb{Z}_p)$ y $U(\mathbb{Z}_q)$ los grupos de las unidades de los anillos $\mathbb{Z}_{pq}$, $\mathbb{Z}_p$ y $\mathbb{Z}_q$ respectivamente, la aplicación*

$$\begin{aligned} U(\mathbb{Z}_{pq}) &\to U(\mathbb{Z}_p) \times U(\mathbb{Z}_q) = \mathbb{F}_p^* \times \mathbb{F}_q^* \\ c &\mapsto (c \bmod p, c \bmod q) \end{aligned}$$

es un isomorfismo de grupos.

Consideramos ahora el subgrupo $S =< (-1,-1) >$ del grupo $G = \mathbb{F}_p^* \times \mathbb{F}_q^*$ y el grupo cociente $H = G/S$. Es decir, vamos a realizar una partición de los elementos de G en subconjuntos de la forma $\{(x,y),(-x,-y)\}$.

Como p y q son primos impares, $P = \frac{p-1}{2}$ y $Q = \frac{q-1}{2}$ son enteros y entonces $|H| = \frac{(p-1)(q-1)}{2} = 2PQ$.

Calculamos ahora el producto de los elementos de H de dos formas distintas: para ello determinaremos dos sistemas completos de representantes de las clases de H y realizaremos el producto de los elementos de cada uno de los dos sistemas de representantes. Con esto calcularemos, en ambos casos, un representante de la clase producto, el cual, a la vista de la partición realizada, es único salvo el signo.

- Definimos los dos sistemas de representantes:
  El primer sistema de representantes va a ser

$$R_1 = \{(a,b)/a = 1,...,p-1, b = 1,..., \frac{q-1}{2}\}$$

  Es claro que R_1 tiene $2PQ = |H|$ elementos. Además, es fácil ver que si para cualquier $(x,y) \in R_1$, se cumple que $y \in \{1,..., \frac{q-1}{2}\}$; entonces $-y = p - y \geq q - \frac{q-1}{2} = \frac{q+1}{2}$ y $(-x,-y) \notin R_1$, luego R_1 no contiene dos elementos de la misma clase y es un sistema completo de representantes.

  El segundo sistema de representantes es

$$R_2 = \{(c \text{ mód } p, c \text{ mód } q) \in (\mathbb{F}_p)^* \times (\mathbb{F}_q)^* / c \in U(\mathbb{Z}_{pq}), 1 \leq c \leq \frac{pq-1}{2}\}$$

  El número de elementos de R_2 es el número de enteros c tales que $1 \leq c \leq \frac{pq-1}{2}$ y son primos con pq. Los $c \in \{1,\ldots,\frac{pq-1}{2}\}$ que son múltiplo de p son los de la forma $p\frac{q-1}{2}$ y los que son múltiplo de q son los de la forma $q\frac{p-1}{2}$. Por tanto, el número de elementos de R_2 es $\frac{pq-1}{2} - \frac{p-1}{2} - \frac{q-1}{2} = (p-1)\frac{q-1}{2} = 2PQ$.

  Comprobamos ahora que R_2 no contiene dos elementos de la misma clase: si $(c,c),(d,d) \in R_2$ pertenecen a la misma clase, debe ser $cd^{-1} \equiv \pm 1$ mód pq, es decir $c \equiv \pm d$ mód pq pero entonces, por ser $1 \leq c,d \leq \frac{pq-1}{2}$, es $c = d$.

- Calculamos ahora el producto de los elementos de R_1.

Por una parte los elementos de la primera coordenada a, son $1, ..., p-1$, y evidentemente se repiten $\frac{q-1}{2}$ veces cada uno. Y por el otro lado tenemos que los elementos de la segunda coordenada son $1, ..., \frac{q-1}{2}$, y se repite cada uno $p-1$ veces. Por lo tanto,

$$\prod_{(a,b)\in R_1}(a,b) = \left((p-1)!^{\frac{q-1}{2}}, (\frac{q-1}{2})!^{p-1}\right)$$

Por el Teorema de Wilson, se sabe que $(p-1)!^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}}$ mód p.
Por otro lado, calculamos $(\frac{q-1}{2})!^{p-1} = (Q!)^{2P}$ teniendo en cuenta que

$$\begin{aligned}(q-1)! &= 1\cdot 2\cdot \ldots \cdot (q-1) \equiv \\ &\equiv 1\cdot 2\cdot \ldots \cdot Q\cdot(-Q)\cdot ...\cdot(-2)\cdot(-1) \text{ mód } q \\ &= (Q)!(Q)!(-1)^Q\end{aligned}$$

Entonces $(Q!)^2 \equiv (-1)^Q(q-1)!$ mód q y

$$(Q!)^{2P} \equiv (-1)^{PQ}(q-1)!^P \equiv (-1)^{PQ}(-1)^P = (-1)^{P(1+Q)} \text{ mód } q$$

Resulta que

$$\prod_{(a,b)\in R_1}(a,b) = \left((-1)^Q, (-1)^{P(1+Q)}\right)$$

- Vamos a calcular ahora el producto de los elementos de R_2 calculando en primer lugar $M_p = \prod_{c=1,(c,p)=1}^{\frac{pq-1}{2}} c$ mód p y después el producto $M_q = \prod_{c=1}^{\frac{pq-1}{2}} c$ mód q.

$$M_p = \prod_{c=1,(c,p)=1}^{\frac{pq-1}{2}} c = \left(\prod_{c=1}^{p-1} c\right)\left(\prod_{c=p+1}^{2p-1} c\right)\ldots\left(\prod_{c=\frac{q-3}{2}p+1}^{\frac{q-3}{2}p+p-1} c\right)\left(\prod_{c=\frac{q-1}{2}p+1}^{\frac{q-1}{2}p+\frac{p-1}{2}} c\right)$$

Como $\prod_{c=1}^{p-1} c = (p-1)!$ y, para cada $j = 1, \ldots, \frac{q-3}{2}$, se cumple que $\prod_{c=jp+1}^{jp+p-1} c \equiv (p-1)!$ mód p, resulta que

$$M_p \equiv ((p-1)!)^{\frac{q-1}{2}} \prod_{c=\frac{q-1}{2}p+1}^{\frac{q-1}{2}p+\frac{p-1}{2}} c \equiv (p-1)!^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)! \text{ mód } p$$

.

Para calcular ahora $\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \text{ mód } p$ debemos dividir M_p por los múltiplos de q que hay hasta $\frac{pq-1}{2}$.

$$\prod_{r=1}^{\frac{p-1}{2}} rq = q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

y resulta que

$$\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \text{ mód } p \equiv \frac{M_p}{q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!} = \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}$$

Utilizando el Criterio de Euler que asegura que $q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$, se puede escribir

$$\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \text{ mód } p = \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} = (p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

y, teniendo en cuenta el Teorema de Wilson, resulta

$$\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \text{ mód } p$$

Por simetría, cambiando los papeles de p y q, se obtiene el producto de los elementos de la segunda coordenada:

$$\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \text{ mód } q \equiv \frac{M_q}{p^{\frac{q-1}{2}} \left(\frac{q-1}{2}\right)!} = \frac{(q-1)!^{\frac{p-1}{2}}}{p^{\frac{q-1}{2}}} = (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$$

$$\prod_{c=1,(c,pq)=1}^{\frac{pq-1}{2}} c \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \text{ mód } q$$

Resulta ahora que

$$\prod_{(c,c)\in R_2} (c,c) = \left((-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \text{ mód } p, (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \text{ mód } q\right)$$

Finalmente, recordamos que los dos productos que hemos realizado son iguales salvo el signo y resulta que

$$((-1)^Q \text{ mód } p, (-1)^{P(1+Q)} \text{ mód } q) = \pm \left((-1)^Q \left(\frac{q}{p}\right) \text{ mód } p, (-1)^P \left(\frac{p}{q}\right) \text{ mód } q \right)$$

Observando las primeras coordenadas, se concluye que ese factor ± 1 es precisamente $\left(\frac{q}{p}\right)$ y entonces, igualando las segundas coordenadas, obtenemos que

$$(-1)^{P(1+Q)} = (-1)^P \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$$

Y deshaciendo la notación de P y Q obtenemos el resultado

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

3.6. Demostración de Zolotarev

Yegor Ivánovich Zolotarev (1847-1878) fue un matemático ruso, que estudio en la Facultad de Matemáticas de San Petersburgo y en 1867 paso a ser profesor de dicha universidad. En 1872 visitó Berlin donde recibió clases de Kummer y Weierstrass. Defendió su tesis doctoral en 1874, siendo nombrado dos años mas tarde profesor extraordinario de Matemáticas en la facultad de Física y Matemáticas de San Petersburgo. Por desgracia su carrera acabó demasiado pronto con un accidente que provocó su muerte a los 31 años.

En 1872 ([14]), estudiando el signo de una permutación concreta, a la que se ha llamado la "permutación mágica" de Zolotarev, obtuvo una de las demostraciones más interesantes de la Ley de Reciprocidad Cuadrática.

3.6.1. Algunos conceptos sobre permutaciones

Incluimos aquí algunas nociones básicas que utilizaremos en el resto de la sección.

Definición 3.3 (Permutación) *Una permutación σ de un conjunto I de n elementos es una aplicación biyectiva de I en I. El conjunto de todas las biyecciones de I tiene estructura de grupo respecto de la composición de aplicaciones. Este grupo se llama grupo simétrico de grado n y se representa por S_n.*

Definición 3.4 *Si σ es una permutación de $I = \{1, 2, \ldots, n\}$, se dice que los elementos $i, j \in I$ forman una inversión de σ si $i < j$ y $\sigma(i) > \sigma(j)$. El número total de inversiones de σ se representa por $\nu(\sigma)$ y se define el signo de la permutación σ mediante la siguiente fórmula:*

$$\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Teorema 3.5 *Para cada $\sigma \in S_n$,*

$$\epsilon(\sigma) = (-1)^{\nu(\sigma)}$$

.

Teorema 3.6 *Asociando a cada $\sigma \in S_n$ su signo, queda definida la aplicación:*

$$\begin{array}{rcl} \epsilon : S_n & \longrightarrow & \{-1, 1\} \\ \sigma & \mapsto & \epsilon(\sigma) = (-1)^{\nu(\sigma)} \end{array}$$

que es un homomorfismo de grupos.

Demostración Utilizando la fórmula del teorema anterior, tenemos que:

$$\epsilon(\sigma \circ \tau) = \prod_{i<j} \frac{\sigma((\tau(j)) - \sigma((\tau(i))}{j - i} = \prod_{i<j} \left(\frac{\sigma((\tau(j)) - \sigma((\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} \right)$$

Haciendo ahora $j' = \tau(j)$ y $i' = \tau(i)$ en la primera fracción, resulta que

$$\epsilon(\sigma \circ \tau) = \prod_{i'<j'} \frac{\sigma(j') - \sigma(i')}{j' - i'} \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} = \epsilon(\sigma)\epsilon(\tau).$$

Lema 3.4 (Lema de Zolotarev) *Si p es un primo impar y a un entero positivo no divisible por p, la aplicación*

$$\begin{array}{rcl} \mu_a : \mathbb{Z}_p^* & \to & \mathbb{Z}_p^* \\ x & \mapsto & ax \text{ mód } p \end{array}$$

es una permutación de $\mathbb{Z}_p^*$ y $\epsilon(\mu_a) = \left(\frac{a}{p}\right)$.

Demostración
Es claro que μ_a es biyectiva. Para probar la segunda parte, observamos en primer lugar que la aplicación

$$\begin{array}{rcl} \epsilon : \mathbb{Z}_p^* & \to & \{\pm 1\} \\ a & \mapsto & \epsilon(\mu_a) \text{ mód } p \end{array}$$

es suprayectiva ya que si a es un elemento de $\mathbb{Z}_p^*$ de orden $p-1$, entonces μ_a es un $(p-1)$-ciclo que es una permutación impar y en consecuencia $\epsilon(\mu_a) = -1$.

Aplicando ahora el Primer Teorema de Isomorfía, tenemos que

$$|Im\ \epsilon| = 2 \Rightarrow |\ker \epsilon| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$$

Como $\mathbb{Z}_p^*$ es cíclico de orden $p-1$, sólo tiene un subgrupo de orden $\frac{p-1}{2}$, que es justamente $\{a^2 /\ a \in \mathbb{Z}_p^*\}$, el conjunto de los residuos cuadráticos. Así, tenemos que

$$\epsilon(\mu_a) = 1 \Leftrightarrow a \in \ker \epsilon \ \Leftrightarrow \left(\frac{a}{p}\right) = 1$$

3.6.2. Demostración de la Ley de Reciprocidad Cuadrática

Para que esta demostración quede mas clara, vamos a introducir un ejemplo, al cual le vamos a ir aplicando los pasos explicados, y veremos sus resultados.

Empezaremos considerando m y n, dos números enteros impares positivos tal que $n > m$, y una baraja de cartas con $m \cdot n$ cartas, numeradas del 0 al $mn-1$. En el ejemplo tendremos que $m = 3$, $n = 7$. Colocaremos las cartas en filas de n cartas cada una, de izquierda a derecha y de arriba a abajo, formando un rectángulo con m filas de n cartas cada una.

$$\begin{array}{ccccc} 0 & 1 & 2 & ... & n-1 \\ n & n+1 & n+2 & ... & 2n-1 \\ 2n & ... & & & \\ ... & & & & \\ (m-1)n & (m-1)n+1 & (m-1)n+2 & ... & mn-1 \end{array}$$

Observemos que en esta matriz, la carta que ocupa la posición (x, y) es la que estaba inicialmente en la posición $nx + y$.

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 14 & 15 & 16 & 17 & 18 & 19 & 20 \end{matrix}$$

Teniendo las cartas así colocadas, las vamos a recoger por columnas, de izquierda a derecha y de arriba a abajo: las m primeras serán

$$0 \quad n \quad 2n \quad ... \quad (m-1)n$$

$$0 \quad 7 \quad 14$$

Después se colocarán las de la segunda columna se colocará y así sucesivamente hasta completar la baraja. Así queda construida una permutación de las cartas que representaremos por $\sigma_{m,n}$.

$$\begin{pmatrix} 0 & 1 & 2 & .. & m-1 & m & m+1 & .. & .. & .. & .. & mn-1 \\ 0 & n & 2n & .. & (m-1)n & 1 & n+1 & .. & (m-1)n+1 & 2 & n+2 & .. & mn-1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & ... & 19 & 20 \\ 0 & 7 & 14 & 1 & 8 & ... & 13 & 20 \end{pmatrix}$$

Es decir, si con el ejemplo colocamos la baraja con el nuevo orden en un rectangulo de las mismas dimensiones que el inicial nos quedaría la matriz:

$$\begin{matrix} 0 & 7 & 14 & 1 & 8 & 15 & 2 \\ 9 & 16 & 3 & 10 & 17 & 4 & 11 \\ 18 & 5 & 12 & 19 & 6 & 13 & 20 \end{matrix}$$

Calcularemos ahora el signo de $\sigma_{m,n}$ de dos formas distintas.

Por una parte, gracias al Teorema 3.6, lo único que tenemos que hacer es contar el número de inversiones de la permutación. Para ello, vamos a ir contando las inversiones que forma cada número, dividiéndolas en bloques de m elementos cada uno.

- 0: por supuesto formará 0 inversiones. Además al contabilizar inversiones lo vamos a obviar, porque es más fácil si empezamos a contar desde el elemento 1 y esto no afectará al resultado final.

- n: como su posición es la 1, formará exactamente $n-1$ inversiones. Es decir, si $n=7$, tenemos $\sigma(1)=7$ forma inversiones con $\sigma(3)=1$, $\sigma(6)=2$, $\sigma(9)=3$, $\sigma(12)=4$, $\sigma(15)=5$, $\sigma(18)=6$. Por lo tanto 6 inversiones.

- $2n$: de los elementos mas pequeños que él únicamente tiene una posición anterior n, por lo que formará $2n-2$ inversiones.

- $3n$: tiene anteriormente a los elementos n y $2n$, por lo que forma $3n-3$ inversiones.

- ...

- $(m-1)n$: formará $(m-1)n-(m-1)$ inversiones por el mismo razonamiento.

Llamemos N_0 a la suma de inversiones que forma este primer bloque:

$$N_0 = (n-1)\sum_{k=1}^{m-1} k$$

Segundo bloque:

- 1: el 1 siempre forma 0 inversiones (hemos excluido el 0).

- $n+1$: se formarán $n-2$ inversiones porque los elementos mas pequeños que han quedado en posiciones anteriores son el 1 y el n.

- $2n+1$: se formarán $2n-4$ inversiones.

- ...

- $(m-1)n+1$: se formarán $(m-1)(n-2)$ inversiones.

Y entonces la suma de todas las inversiones será

$$N_1 = (n-2)\sum_{k=1}^{m-1} k$$

Generalizando esta fórmula $\forall i \in \{0,...,n-1\}$, resulta que

$$N_i = (n-(i+1))\sum_{k=1}^{m-1} k$$

Si volvemos a mirar el teorema 3.5 vemos que lo que realmente nos interesa para saber el signo de la permutación es la paridad del número de inversiones, lo que nos lleva a estudiar la paridad de $\sum_{k=1}^{m-1} k$, común a todos los N_i:

Veamos la paridad de

$$\sum_{k=1}^{m-1} k = 1 + 2 + \ldots + (m-1) = \frac{m(m-1)}{2}$$

Como m es impar, $m-1$ es par y $\frac{m-1}{2} \in \mathbb{Z}$. Por tanto, $\frac{m(m-1)}{2}$ es par si y sólo si lo es $\frac{m-1}{2}$.

Además como m es impar, es $m \equiv 1$ o $3 \bmod 4$ y entonces $m-1 \equiv 0, 2 \bmod 4$. Por tanto,

$$\frac{m(m-1)}{2} \text{ es par } \Leftrightarrow \frac{m-1}{2} \text{ es par } \Leftrightarrow m \equiv 1 \bmod 4$$

Resulta que

- Si $m \equiv 1 \bmod 4$, $\sum_{k=1}^{m-1} k$ es par y, en este caso N_i va a ser siempre un número par.
- Si $m \equiv 3 \bmod 4$, $\sum_{k=1}^{m-1} k$ es impar y aquíes donde nos interesa estudiar la paridad de $n-1-i$. Dicho número será par si y sólo si i es par. Por lo tanto obtenemos que en el único caso en el que N_i será impar es en el caso en que $m \equiv 3 \bmod 4$ y i sea impar.

Por último, determinaremos la paridad del número total de inversiones, $\nu(\sigma_{m,n})$.

$$\nu(\sigma_{m,n}) = N_0 + N_1 + \cdots + N_{n-1} = N_0 + \sum_{i=1,\ i\ par}^{n-1} N_i + \sum_{i=1,\ i\ impar}^{n-1} N_i$$

N_0 siempre es par y N_i es par siempre que i sea par. Por lo tanto la paridad de $\nu(\sigma_{m,n})$ coincide con la paridad del último sumando.

Si i es impar, $(n-(i+1))$ es impar y la paridad de estos N_i depende sólo de m, luego todos ellos son pares o todos son impares.

Si todos son impares, la paridad de la suma coincide con la del número de sumandos: como n es impar, el número de $i's$ impares en $\{1, \ldots, n-1\}$ es $\frac{n-1}{2}$. Por tanto, la suma $\sum_{i=1,\ i\ impar}^{n-1} N_i$ es par en este caso si y sólo si $\frac{n-1}{2}$ lo es.

En resumen, tenemos que

- $\sum_{i=1,\ i\ impar}^{n-1} N_i$ será par si $m \equiv 1$ mód 4 o $n \equiv 1$ mód 4.
- $\sum_{i=1,\ i\ impar}^{n-1} N_i$ será impar si $m \equiv n \equiv 3$ mód 4.

Y por fin llegamos a que el signo de $\sigma_{m,n}$ es

$$\epsilon(\sigma_{m,n}) = \begin{cases} 1 & \text{si } m \equiv 1 \text{ mód } 4 \text{ o } n \equiv 1 \text{ mód } 4 \\ -1 & \text{si } m \equiv n \equiv 3 \text{ mód } 4 \end{cases}$$

En otras palabras,

$$\epsilon(\sigma_{m,n}) = (-1)^{\frac{(m-1)(n-1)}{4}}$$

Hasta ahora hemos estado utilizando n y m como dos enteros impares positivos. A partir de ahora añadiremos otra restricción más: n y m serán coprimos (lo que no influirá en nuestra elección de n y m para el ejemplo). Calcularemos ahora de otra forma el signo de $\sigma_{m,n}$, y esto lo haremos definiendo dos nuevas permutaciones, cuya composición será $\sigma_{m,n}$

Para cada $y \in \{0, \ldots, n-1\}$ definimos α_y

$$\begin{aligned} \alpha_y : \mathbb{Z}_m &\to \mathbb{Z}_m \\ x &\mapsto nx + y \text{ mód } m \end{aligned}$$

y, para cada $x \in \{0, \ldots, m-1\}$, definimos β_x:

$$\begin{aligned} \beta_x : \mathbb{Z}_n &\to \mathbb{Z}_n \\ y &\mapsto x + my \text{ mód } n \end{aligned}$$

Observando que son biyectivas, a partir de estas dos permutaciones, definimos otras dos:

$$\begin{aligned} A = \alpha_y \times 1 : \mathbb{Z}_m \times \mathbb{Z}_n &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ (x, y) &\mapsto (nx + y \text{ mód } m, y \text{ mód } n) \end{aligned}$$

$$\begin{aligned} B = 1 \times \beta_x : \mathbb{Z}_m \times \mathbb{Z}_n &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ (x, y) &\mapsto (x \text{ mód } m, x + my \text{ mód } n) \end{aligned}$$

Vamos a comprobar que $B \circ (A)^{-1} = \sigma_{m,n}$.

Tal y como están definidas las permutaciones, vemos que lo que permuta son posiciones de la matriz, por lo que primero vamos a ver como es esa permutación de posiciones en el ejemplo, y después escribiremos la matriz ya sabiendo que a cada posición (x, y) está asociado el entero $nx + y$. Por lo tanto la permutación A^{-1} quedará:

$$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (0,4) & (0,5) & ... & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\ (0,0) & (2,1) & (1,2) & (0,3) & (2,4) & (1,5) & ... & (1,1) & (0,2) & (2,3) & (1,4) & (0,5) & (2,6) \end{pmatrix}$$

Por tanto la matriz, escribiéndola ya con la transformación de cada posición asociada a su entero, nos queda

$$\begin{matrix} 0 & 8 & 16 & 3 & 11 & 19 & 6 \\ 7 & 15 & 2 & 10 & 18 & 5 & 13 \\ 14 & 1 & 9 & 17 & 4 & 12 & 20 \end{matrix}$$

Solamente nos queda aplicar β_x a esta matriz. Y hacemos lo mismo, primero escribiremos la permutación de los elementos escritos como posiciones de la matriz,y después escribiremos la matriz resultante de los enteros $nx + y$.

$$\begin{pmatrix} (0,0) & (2,1) & (1,2) & (0,3) & (2,4) & (1,5) & ... & (1,1) & (0,2) & (2,3) & (1,4) & (0,5) & (2,6) \\ (0,0) & (0,3) & (0,6) & (0,2) & (0,5) & (0,1) & ... & (2,5) & (2,1) & (2,4) & (2,0) & (2,3) & (2,6) \end{pmatrix}$$

$$\begin{matrix} 0 & 7 & 14 & 1 & 8 & 15 & 2 \\ 9 & 16 & 3 & 10 & 17 & 4 & 11 \\ 18 & 5 & 12 & 19 & 6 & 13 & 20 \end{matrix}$$

Vemos que la matriz resultante es la misma que la matriz obtenida al aplicar $\sigma_{m,n}$. Esta composición ha sido fácil de ver para el ejemplo, pero para el caso general no se ve tan claro. Para poder comparar $\sigma_{m,n}$ con la composición de A y B, tenemos que ver primero como se comporta $\sigma_{m,n}$ en el caso general. Miremos de nuevo el rectángulo de cartas inicial:

- 1ª ordenación: Tomamos las cartas por filas. Esto quiere decir, estiramos esa matriz de forma que en las primeras posiciones tendremos los elementos de la primera fila, seguidos de estos irán los de la segunda, etc. Esta ordenación es muy fácil de ver, porque es la ordenación natural. Entonces en la posición (i, j) tendremos la carta con el elemento $ni + j$.

- 2ª ordenación: Es el caso en que tomamos las cartas por columnas. Esto quiere decir que en las primeras posiciones tendremos los elementos de la primera columna ordenados de arriba a abajo, seguidos de la segunda etc. Por tanto en esta ordenación vemos que en la posición (i,j) tendremos el elemento $mj + i$.

Vemos que entonces la permutación $\sigma_{m,n}$ lo que hace es pasar de una ordenación a otra. En otras palabras, relaciona el elemento en la posición (i, j) de la primera ordenación con el elemento en la posición (i, j) de la segunda ordenación, por lo tanto, siendo $i \in 1, ..., m-1$ y $j \in 1, ..., n-1$:

$$\begin{aligned} \sigma_{m,n} : \mathbb{Z}_{mn} &\to \mathbb{Z}_{mn} \\ ni + j &\mapsto mj + i \end{aligned}$$

Una de las cosas que nos va a facilitar mucho el trabajo es no tener que utilizar la inversa de la permutación A. Esto lo vamos a hacer considerando el isomorfismo

$$\begin{aligned} \pi : \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ a &\mapsto (a \text{ mód } m, a \text{ mód } n) \end{aligned}$$

la cual no nos va a influir en ningun momento para calcular el signo de las permutaciones. Vemos claramente que $\pi(nx+y) = (nx+y \text{ mód } m, y \text{ mód } n)$, y que $\pi(x + my) = (x \text{ mód } m, x + my \text{ mód } n)$. La aplicación π únicamente la utilizaremos para pasar de $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$. Entonces comprobemos la siguiente igualdad que, si nos fijamos, realmente es la misma que hemos utilizado para el ejemplo: $\pi \circ \sigma_{mn} \circ \pi^{-1} \circ A = B$. Veamos fácilmente que esta igualdad se cumple:

$$\pi(\sigma(\pi^{-1}(A(x, y)))) = \pi(\sigma(\pi^{-1}(nx + y, y))) =$$

$$= \pi(\sigma(nx + y)) = \pi(x + my) = (x, x + my) = B(x, y)$$

Ya hemos comprobado la igualdad entre nuestra permutación $\sigma_{m,n}$ y la composición de A y B. Estudiemos su signo para poder igualarlo al signo de $\sigma_{m,n}$ que hemos calculado anteriormente. Tomando las permutaciones μ_n, y μ_m, tal y como hemos definido μ_a en la demostración del lema de Zolotarev (Lema 3.4), tenemos que

$$\begin{aligned} \mu_n : \mathbb{Z}_m &\to \mathbb{Z}_m \\ x &\mapsto nx \text{ mód } p \end{aligned}$$

$$\begin{aligned} \mu_m : \mathbb{Z}_n &\to \mathbb{Z}_n \\ x &\mapsto mx \text{ mód } p \end{aligned}$$

Vemos que la permutación α_y es la composición de μ_n con la traslación $(x \mapsto x + y \text{ mód } m)$. Es evidente que la traslación formará un m-ciclo por lo que el signo de ella será 1, y entonces vemos que el signo de α_y es el mismo que el de μ_n, y por lo tanto el mismo también para $\alpha_y \times 1$, que es el que nos interesa. Por lo tanto, $\epsilon(A) = \epsilon(\mu_n)$. De la misma manera tenemos que $\epsilon(B) = \epsilon(\mu_m)$.

Ahora, para probar la Ley de Reciprocidad Cuadrática, aplicaremos el Lema de Zolotarev a las dos permutaciones μ_n y μ_m, que nos obliga a añadir la restricción de tomar tanto m como n primos impares; entonces podremos asegurar que $\epsilon(A) = \left(\frac{n}{m}\right)$, y que $\epsilon(B) = \left(\frac{m}{n}\right)$.

Por último, sabemos que $\epsilon(\pi \circ \sigma_{mn} \circ \pi) = \epsilon(\sigma_{mn})$ ya que vamos a tener el mismo número de inversiones. Además, como hemos asegurado en el Teorema 3.6, la aplicación signo es un homomorfismo, por lo tanto si $B \circ A^{-1} = \sigma_{m,n} = (-1)^{\frac{(m-1)(n-1)}{4}}$,

$$\epsilon(\sigma_{mn})\epsilon(A) = \epsilon(B)$$

Y por fin hemos demostrado la Ley de Reciprocidad Cuadrática

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

Bibliografía

[1] Baker, Matt, "Zolotarev's Magical Proof of the Lay of Quadratic Reciprocity". (2011) http://www.numdam.org/item?id=NAM_1872_2_11__354_0

[2] Baumgart, O. "The Quadratic Reciprocity Law: A

[3] Cardenal, Edwin León , "La Gema de la Reina: Una breve revisión histórica de la ley de reciprocidad cuadrática", Lecturas Matemáticas, Volúmen 30, p. 17-27. https://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html http://studylib.es/doc/214793/reciprocidad-cuadratica

[4] Edwards H.M. "Euler and quadratic reciprocity", Math. Mag. 56 (5)(1983), 285-291. https://proofwiki.org/wiki/Second_Supplement_to_Law_of_Quadratic_Reciprocity

[5] Elvidge, Sean "The History of the Law of Quadratic Reciprocity".

[6] Eisenstein, G. "Geometrischer Beweis des Fundamental Theorems für die quadratischen Reste". J. Reine und Angew. Math. 28 (1844) 246-248.

[7] Fernando, José F; Gamboa, J. Manuel. "Ecuaciones Algebraicas: Extensiones de Cuerpos y Teoría de Galois". Ed. Sanz y Torres (2015)

Collection of Classical Proofs". Birkhäuser (2010)

[8] C.F. Gauss, "Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplicationes novae", 1818; Werke II, 47-64, in particular p. 51;

[9] Ireland, K.; Rosen, M. "A Classical Introduction to Modern Number Theory" Springer GTM 84 (1990)

[10] Kronecker, L. "Der dritte Gausssche Beweis des Reciprocitätsgesetzes für die quadratischen Reste, in vereinfachter Darstellung" J. Reine Angew. Math. 97 (1885) 93-94. Werke II, 533-536.

[11] Lemmermeyer, F. "Reciprocity Laws: from Euler to Eisenstein" Springer. Monographs in Mathematics (1991)

[12] G. Rousseau, On the Quadratic Reciprocity Law, J. Austral. Math. Soc. Ser. A 51 (1991), no. 3, 423-425. https://math.stackexchange.com/questions/180002/legendre-symbol-second-supplementary-law

[13] Weintraub, Steven H. "Gauss's Fifth Proof of the Law of Quadratic Reciprocity".http://www.lehigh.edu/~shw2/q-recip/gauss5.pdf (2000)

[14] Zolotarev, "Nouvelle démonstration de la loi de réciprocité de Legendre". Nouvelles annales de mathématiques, 2^e série, tome 11 (1872), p.354-362

Apéndice

A continuación incluimos una lista de todas las demostraciones de la Ley de Reciprocidad Cuadrática, desde Gauss hasta la actualidad.

Autor	Año	Método
1. Legendre	1788	Quadratic forms; incomplete
2. Gauß 1	1801	Induction; April 8, 1796
3. Gauß 2	1801	Quadratic forms; June 27, 1796
4. Gauß 3	1808	Gauß's Lemma; May 6, 1807
5. Gauß 4	1811	Cyclotomy; May 1801
6. Gauß 5	1818	Gauß's Lemma; 1807/08
7. Gauß 6	1818	Gauß sums; 1807/08
8. Cauchy	1829	Gauß 6
9. Jacobi	1830	Gauß 6
10. Dirichlet 1	1835	Gauß 4
11. Lebesgue 1	1838	$N(x_1^2 + ... + x_q^2 = 1 mod p)$
12. Schönemann	1839	quadratic period equation
13. Cauchy	1840	Gauss 4
14. Eisenstein 1	1844	generalized Jacobi sums
15. Eisenstein 2	1844	Gauß 6
16. Eisenstein 3	1844	Gauß's Lemma
17. Eisenstein 4	1845	Sine
18. Eisenstein 5	1845	infinite products
19. Kummer 1	1846	period equation
20. Liouville	1847	Cyclotomy
21. Lebesgue 2	1847	Lebesgue 1
22. Schaar	1847	Gauß's Lemma
23. Plana 1	1851	Gauß sums
24. Genocchi 1	1852	Gauß's Lemma

25. Schaar 2 2	1854	Gauß 4
26. Dirichlet 2	1854	Gauß 1
27. Genocchi 2	1854	Liouville
28. Schaar 3 3	1860	Gauß 4
29. Lebesgue 3	1860	Gauß 7, 8
30. Kummer 2	1862	Quadratic forms
31. Kummer 3	1862	Quadratic forms
32. Dedekind 1	1863	Quadratic forms
33. Gauß 7	1863	quadratic periods; Sept. 1796
34. Gauß 8	1863	quadratic periods; Sept. 1796
35. Mathieu	1867	Cyclotomy
36. von Staudt	1867	Cyclotomy
37. Bouniakowski	1869	Gauß's Lemma
38. Stern	1870	Gauß's Lemma
39. Zeller	1872	Gauß's Lemma
40. Zolotarev	1872	Permutations
41. Kronecker 1	1872	Zeller
42. Schering 1	1875	Gauß 3
43. Kronecker 2	1876	Induction
44. Mansion 1	1876	Gauß's Lemma
45. Dedekind 2	1877	Gauß 6
46. Dedekind 3	1877	Dedekind Sums
47. Pellet 1	1878	Stickelberger-Voronoi
48. Pépin 1	1878	Cyclotomy
49. Sochocki	1878	Theta functions
50. Schering 2	1879	Gauß's Lemma
51. Petersen	1879	Gauß's Lemma
52. Genocchi 2	1880	Gauß's Lemma
53. Kronecker 3	1880	Gauß 4
54. Kronecker 4	1880	quadratic period
55. Voigt	1881	Gauß's Lemma
56. Pellet 2	1882	Mathieu 1867
57. Busche 1	1883	Gauß's Lemma
58. Gegenbauer 1	1884	Gauß's Lemma
59. Kronecker 5	1884	Gauß's Lemma
60. Kronecker 6	1885	Gauß 3
61. Kronecker 7	1885	Gauß's Lemma
62. Bock	1886	Gauß's Lemma
63. Lerch 1	1887	Gauß 3
64. Busche 2	1888	Gauß's Lemma
65. Hacks	1889	Schering
66. Hermes	1889	Induction
67. Kronecker 8	1889	Gauß's Lemma
68. Tafelmacher 1	1889	Stern
69. Tafelmacher 2	1889	Stern/Schering
70. Tafelmacher 3	1889	Schering

71. Busche 3	1890	Gauß's Lemma
72. Franklin	1890	Gauß's Lemma
73. Lucas	1890	Gauß's Lemma
74. Pépin 2	1890	Gauß 2
75. Fields	1891	Gauß's Lemma
76. Gegenbauer 2	1891	Gauß's Lemma
77. Gegenbauer 3	1893	Gauß's Lemma
78. Schmidt 1	1893	Gauß's Lemma
79. Schmidt 2	1893	Gauß's Lemma
80. Schmidt 3	1893	Induction
81. Heinitz	1893	Gauß's Lemma
82. Gegenbauer 4	1894	Gauß's Lemma
83. Bang	1894	Induction
84. Mertens 1	1894	Gauß's Lemma
85. Mertens 2	1894	Gauß sums
86. Busche 4	1896	Gauss's Lemma
87. Lange 1	1896	Gauß's Lemma
88. Mansion 2	1896	Gauss 2
89. de la Vallée Poussin	1896	Gauß 2
90. Lange 2	1897	Gauß's Lemma
91. Hilbert	1897	Cyclotomy
92. Alexejewsky	1898	Schering
93. Pépin 3	1898	Legendre
94. Pépin 4	1898	Gauß 5
96. Fischer	1900	Resultants
97. Takagi	1903	Zeller
98. Lerch 2	1903	Gauß 5
99. Mertens 3	1904	Eisenstein 4
100. Mirimanoff & Hensel	1905	Stickelber ger-Voronoi
101. Cornacchia 5	1909	
102. Busche 5	1909	Zeller
103. Busche 6	1909	Eisenstein
107. Pépin 5	1911	Gauss 2
108. Petr 1	1911	Mertens 3
109. Pocklington	1911	Gauß 3
110. Dedekind 3	1912	Zeller
111. Heawood	1913	Geometric
112. Frobenius 1	1914	Zeller
113. Frobenius 2	1914	Geometric (Eisenstein)
114. Lasker	1916	Stickelberger-Voronoi
115. Cerone	1917	Eisenstein 4
116. Bartelds & Schuh	1918	Gauß's Lemm
117. Stieltjes	1918	Lattice points
118. Teege 1	1920	Legendre
119. Teege 2	1921	Cyclotomy

120. Arwin	1924	Quadratic forms
121. Rédei 1	1925	Gauß's Lemma
122. Rédei 2	1926	Gauß's Lemma
123. Whitehead	1927	Genus theory (Kummer)
124. Petr 2	1927	theta functions
125. Skolem 1	1928	Genus theory
126. Petr 3	1934	Kronecker (signs)
127. van Veen	1934	Geometric (Eisenstein)
128. Fueter	1935	quaternion algebras
129. Whiteman	1935	Gauß's Lemma
130. Dockeray	1938	Eisenstein 3
131. Scholz	1938	Gauss 3
132. Kapferer	1939	Liouville
133. Dörge	1942	Gauß's Lemma
134. Rédei 3	1944	Gauß 5
135. Lewy	1946	Cyclotomy
136. Petr 4	1946	Cyclotomy
137. Skolem 2	1948	Gauß 2
138. Barbilian	1950	Eisenstein 1
139. J. Delsarte	1950	Vandermonde determinants
140. Rédei 4	1951	Gauß 3
141. Brandt 1	1951	Gauß 2
142. Brandt 2	1951	Gauß sums
143. Brewer	1951	Mathieu, Pellet
144. Furquim de Almeida	1951	Finite fields
145. Zassenhaus	1952	Finite fields
146. Riesz	1953	Permutations
147. Fröhlich	1954	Class Field Theory
148. Ankeny	1955	Cyclotomy
149. D.H. Lehmer	1957	Gauß's Lemma
150. C. Meyer	1957	Dedekind sums
151. Holzer	1958	Gauß sums
152. Rédei 5	1958	Cyclotomic polynomial
153. Reichardt	1958	Gauß 3
154. Carlitz	1960	Gauß 1
155. Kubota 1	1961	Cyclotomy
156. Kubota 2	1961	Gauß sums (sign)
157. Skolem 3	1961	Cyclotomy
158. Skolem 4	1961	finite fields
159. Hausner	1961	Gauß sums
160. Swan 1	1962	Stickelberger-Voronoi
161. Gerstenhaber	1963	Eisenstein, sine
162. Koschmieder	1963	Eisenstein, sine
163. Rademacher	1964	Finite Fourier analysis

164. Weil	1964	Theta functions
165. Kloosterman	1965	Holzer
166. Chowla	1966	Finite fields
167. Burde	1967	Gauß's Lemma
168. Kaplan 1	1969	Eisenstein
169. Kaplan 2	1969	quadratic congruences
170. Birch	1971	K-groups (Tate)
171. Reshetukha	1971	Gauß sums
172. Agou	1972	finite fields
173. Brenner	1973	Zolotarev
174. Honda	1973	Gauß sums
175. Milnor & Husemöller	1973	Weil 1964
176. Zagier	1973	Dedekind sums
177. Allander	1974	Gauß's Lemma
178. Berndt & Evans	1974	Gauß's Lemma
179. Hirzebruch & Zagier	1974	Dedekind Sums
180. Rogers	1974	Legendre
181. Castaldo	1976	Gauß's Lemma
182. Springer	1976	Gauss sums
183. Frame	1978	Kronecker (signs)
184. Hurrelbrink	1978	K-theory
185. Auslander & Tolimieri	1979	Fourier transform
186. Corro	1980	Gauß sums
187. Brown	1981	Gauß 1
188. Goldschmidt	1981	cyclotomy
189. Kac	1981	Eisenstein, sine
190. Barcanescu	1981	Zolotarev
191. Zantema	1983	Brauer groups
192. Ely	1984	Lebesgue 1
193. Eichler	1985	Theta function
194. Barrucand & Laubie	1987	Stickelberger-Voronoi
195. Peklar	1989	Gauß's Lemma
196. Barnes	1990	Zolotarev
197. Swan 2	1990	Cyclotomy
198. Rousseau 1	1990	Exterior algebras
199. Rousseau 2	1991	Permutations
200. Keune	1991	Finite fields
201. Kubota 3	1992	geometry
202. Russinoff	1992	Gauß's Lemma
203. Garrett	1992	Weil 1964
204. Motose	1993	group algebras
205. Rousseau 3	1994	Zolotarev
206. Young	1995	Gauß sums
207. Brylinski	1997	group actions
208. Merindol	1997	Eisenstein, sine

209. Watanabe	1997	Zolotarev
210. Ishii	1998	Gauß 4
211. Motose	1999	group algebras
212. Zahidi	2000	Stickelberger-Voronoi
213. Lemmermeyer	2000	Lebesgue 1, Ely
214. Meyer	2000	Dedekind sums
215. Tangedal	2000	Eisenstein, geometric
216. Chapman	2001	recurring sequences
217. Hammick	2001	Rousseau 2
218. Girstmair	2001	Eichler
219. Murty	2001	Schur
220. Luo	2003	Rousseau
221. Motose 2	2003	Schur
222. Motose 3	2003	Schur
223. Sey Yoon Kim	2004	Rousseau 2
224. Sun	2004	Gauß' Lemma
225. Duke & Spears	2005	groups
226. Murty & Pacelli	2005	theta functions
227. Szyjewski	2005	Zolotarev
228. Arkhipova	2006	Gauss 4
229. Castryck	2007	Zolotarev
230. Verdure	2008	elliptic curves
231. Gurevich, Hadani, Howe	2008	Schur, Weil
232. Jakimczuk	2009	Lebesgue 1
233. Steiner	2009	Rousseau 2
234. Steiner	2009	Rousseau 2
235. Hambleton & Scharaschkin	2010	resultants (Swan 2)
236. Jerabek	2010	Gauss 3
237. Brunyate & Clark	2010	Zolotarev
238. Szyjewski	2	2012 Zolotarev
239. Dicker	2012	determinants
240. Hambleton & Scharaschkin	2012	Pell conics
241. Karlsson	2012	Gauss sums
242. Zver	2012	Dedekind sums
243. Baker & Shurman	2012	Zolotarev
244. Demchenko & Gurevich	2013	formal groups
245. Caldero & Germoni	2010	Lebesgue 1
246. Burda & Kadets	2013	quadratic periods

Referencia:https://www.rzuser.uni-heidelberg.de/ hb3/rchrono.html