Universidad Autónoma del Estado de Hidalgo
Instituto de Ciencias Básicas e Ingeniería
Centro de Investigación en Matemáticas
Licenciatura en Matemáticas Aplicadas

La Ley de Reciprocidad Cuadrática y sus generalizaciones

Tesis que para obtener el título de

Licenciada en Matemáticas Aplicadas

presenta

Angélica Villeda Roldán

bajo la dirección de

Dr. Fernando Barrera Mora

Pachuca de Soto Hidalgo, Abril de 2010.

Resumen

La Ley de Reciprocidad Cuadrática es un resultado fundamental en Teoría de Números. El objetivo de este trabajo es presentar un breve estudio de las demostraciones de esta ley de reciprocidad enfatizando diferentes métodos que conducen a la generalización de tan importante resultado.

Abstract

Quadratic Reciprocity Law is a fundamental result in Number Theory. The aim of this work is to present a short survey of the proofs of this reciprocity law emphasizing different methods that lead to generalizations of such an important result.

A mis Padres,

Gracias por todo lo que me han enseñado.
Por su esfuerzo para ayudarme a seguir adelante
mostrándome el camino correcto. Por ustedes he
logrado una meta más en mi vida.

Índice general

Introducción

La Ley de Reciprocidad Cuadrática es uno de esos resultados que son punto de partida para desarrollar y estructurar teorías importantes. Desde que fue enunciada por Euler en 1754, aunque no demostrada por él, ha sido fuente de investigaciones y desarrollos fructíferos. Después de su formulación por Euler, Legendre en 1785 continuó su estudio, y es considerado el primero en dar una demostración, que después resultaría parcial pues en ella hace uso de un teorema que fue probado hasta 1837 por Dirichlet, relacionado con la existencia de primos en progresiones aritméticas.

Gauss en sus *Disquisitiones Arithmeticae*, publicadas a principios del siglo XIX, presenta por vez primera una demostración completa de la Ley de Reciprocidad Cuadrática. Este resultado, de acuerdo con sus consecuencias que aparecen en esta obra, se convirtió en piedra angular de la teoría sobre formas cuadráticas binarias, razón que llevó a Gauss a "bautizarla" como el *Teorema Aureo*.

Gauss dedicó considerable tiempo a encontrar una demostración y continuó haciéndolo aún después de 1796 cuando encontró la primera; al final de su vida fueron al menos seis las pruebas encontradas en su intento por encontrar una generalización a potencias más altas.

El tratar de encontrar nuevas y diferentes puebas de la Ley de Reciprocidad Cuadrática no sólo fue idea de Gauss, otros matemáticos que también contribuyeron con demostraciones originales son Cauchy, Dedekind, Dirichlet, Kronecker y Eisenstein ([13]), quien de hecho aportó cinco demostraciones distintas. Es de importancia señalar que las diferentes demostraciones que han ido apareciendo, no tienen por finalidad encontrar nuevos métodos de prueba, más bien, las diferentes pruebas que se conocen son consecuencia del

proceso de búsqueda de generalizaciones así como de la búsqueda e identificación de estructura entre los diferentes resultados en teoría de números. Para 1921 se conocían al menos 56 diferentes pruebas y para finales del siglo pasado había más de 150 ([17, pag. 392]).

En este trabajo hacemos un breve estudio de la Ley de Reciprocidad Cuadrática, presentando algunas de sus demostraciones y generalizaciones con la finalidad de identificar algunas rutas que se han seguido en el desarrollo de la teoría de números que tiene a este resultado como punto de partida.

Empezamos el primer capítulo con una serie de definiciones y resultados con el objetivo de que el material presentado sea accesible al mayor número de personas y continuamos en el segundo capítulo con una pequeña discusión sobre un problema de ecuaciones diofantinas que permite motivar la Ley de Reciprocidad Cuadrática; asimismo, enunciamos este importante resultado y presentamos cuatro demostraciones distintas que ilustran sólo una pequeña parte de su diversidad. Finalmente, con el propósito de introducir el tema de las leyes de reciprocidad superiores, en el tercer capítulo se presentan algunos conceptos que permiten enunciar la Ley de Reciprocidad Cúbica, y en la última sección se discute el problema general de reciprocidad, particularmente en el caso cuadrático y ciclotómico.

Capítulo 1

Preliminares

1.1. Preliminares Aritméticos

1.1.1. Divisibilidad

Definición 1.1.1. Si a y b son enteros, con $a \neq 0$, decimos que a *divide* a b, si existe un entero c tal que $b = ac$, y escribimos $a|b$. Si a divide a b también se dice que a es *divisor* o *factor* de b y que b es un *múltiplo* de a.

Si a no divide a b se escribe $a \nmid b$.

Teorema 1.1.2. Sean a, b, c y d números enteros. Entonces se cumple lo siguiente:

i) Si $a|b$ y $b|c$, entonces $a|c$;

ii) Si $a|b$ y $c|d$, entonces $ac|bd$;

iii) Si $d \neq 0$, entonces $a|b$ si y sólo si $da|db$;

iv) Si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$;

v) Si $a|b$ y $b|a$ entonces $a = \pm b$, y viceversa.

Demostración. Si $a|b$ y $b|c$ entonces existen enteros d y e tales que $b = ad$ y $c = eb$, luego $c = eb = e(ad) = a(ed)$, de manera que $a|c$, y el inciso $i)$ queda demostrado. Asimismo, como también $c|d$, existe otro entero e tal que $d = ec$. Luego, $bd = (ad)(ec) = ac(de)$, y, por tanto, $ac|bd$, y $ii)$ se cumple. Para demostrar $iii)$ observemos que si $a|b$ entonces $b = ac$ y $db = dac = (da)c$, por lo que $da|db$. Por otro lado, si $da|db$ entonces existe un entero f tal que

$db = daf$; al ser $d \neq 0$, se sigue que $b = ac$; esto es, $a|b$ y terminamos. Ahora, si $b \neq 0$, al tener que $a|b$, existe un entero $c \neq 0$ tal que $b = ac$. Luego, $|b| = |ac| = |a||c|$, y como $c \neq 0$, entonces $|c| \geq 1$ y, por tanto, $|b| = |a||c| \geq |a|$, de manera que $iv)$ queda probado. Finalmente, si $a|b$ y $b|a$ entonces existen enteros c y d tales que $b = ac$ y $a = bd$. Luego, por $iii)$, $|a| \leq |b|$ y $|b| \leq |a|$; así $|a| = |b|$ y, por tanto, $a = \pm b$. En la otra dirección, se observa claramente que si $a = b$ ó $a = -b$, entonces $a|b$ y $b|a$, por lo que $v)$ se cumple. ■

Teorema 1.1.3. Si c divide a $a_1, a_2, \ldots, a_n$, entonces c divide a $a_1u_1 + a_2u_2 + \cdots + a_nu_n$ para cualesquiera enteros $u_1, u_2, \ldots, u_n$

Demostración. Si c divide a a_i $(i = 1, 2, \ldots, n)$, entonces $a_i = q_ic$ para algunos enteros q_i, de manera que $a_1u_1 + \cdots + a_nu_n = q_1cu_1 + \cdots + q_ncu_n = (q_1u_1 + \cdots + q_nu_n)c$, y al ser $q_1u_1 + \cdots + q_nu_n$ entero (pues q_i y u_i lo son), se sigue que $c|(a_1u_1 + \cdots + a_nu_n)$ ■

Teorema 1.1.4 (Algoritmo de la división)**.** Si a y b son enteros, con $b \neq 0$, entonces existen únicos enteros q y r, llamados *cociente* y *residuo*, respectivamente, tales que

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Demostración. La demostración se hará suponiendo que $b > 0$, el caso negativo se obtiene tomando $-b$.
`Existencia`. Primero, observamos que si $a = 0$, entonces $q = r = 0$, por lo que podemos suponer $a \neq 0$ y definir

$$S = \{a - nb | n \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \ldots\};$$

como S tiene elementos no negativos (tómese $n = -|a|$), entonces $S \cap \mathbb{N} \neq \emptyset$ y por el principio del buen orden, $S \cap \mathbb{N}$ tiene un elemento mínimo de la forma $r = a - qb \geq 0$, para algún entero q. De esta manera, $a = qb + r$ con $r \geq 0$. Si además se tuviera $r \geq b$, entonces S tendría el elemento, no negativo, $a - (q + 1)b = r - b < r$, lo cual contradiría la minimalidad de r. Por lo tanto, necesariamente $0 \leq r < b$.

`Unicidad`. Supongamos que $a = qb + r = q'b + r'$, con $0 \leq r < b$ y $0 \leq r' < b$, de lo anterior se tiene $r - r' = (q' - q)b$; si $q' \neq q$, entonces $|q' - q| \geq 1$ y, por tanto, $|r - r'| \geq |b| = b$, pues b es un divisor de $|r - r'|$, lo cual es imposible debido a que r y r' se encuentran entre 0 y $b - 1$. Así, $q' = q$ y $r' = r$. ■

Definición 1.1.5. Si a y b son enteros, no ambos cero, entonces el entero positivo d es llamado *máximo común divisor* de a y b si se cumple lo siguiente:

i) $d|a$ y $d|b$, y

ii) si $e|a$ y $e|b$ entonces $e|d$.

Denotamos al máximo común divisor de a y b como $\text{mcd}(a, b)$.

Observación 1.1.6. El $mcd(a, b)$ existe y es único.

Demostración. `Existencia`. Consideremos el conjunto S de todas las combinaciones lineales positivas de a y b:

$$S = \{au + bv | au + bv > 0; u, v \in \mathbb{Z}\}.$$

Notemos primero que S es no vacío. Por ejemplo, si $a \neq 0$, entonces el entero $|a| = a \cdot u + b \cdot 0$ está en S, donde hemos escogido $v = 0$ y $u = 1$ ó $u = -1$ dependiendo de si a es positivo o negativo. Por el Principio del Buen Orden, S debe contener a un elemento mínimo d. Así, de la definición de S, existen enteros x y y tales que $d = ax + by$. Afirmamos que $d = \text{mcd}(a, b)$.

Por el algoritmo de la división, existen enteros q y r tales que $a = qd + r$, donde $0 \leq r < d$. Entonces r puede ser escrito en la forma

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy). \end{aligned}$$

Si r fuera positivo, entonces la representación que acabamos de hacer de r implicaría que r está en S, lo cual contradice el hecho de que d es el mínimo entero en S (recordemos que $r < d$). Por lo tanto, $r = 0$, y entonces $a = qd$, es decir, $d|a$. Análogamente, se obtiene que $d|b$, de manera que d es común divisor de a y b.

Ahora, si c es otro común divisor de a y b, entonces por el Teorema 1.1.3, $c|(ax + by)$; esto es, $c|d$. Concluimos así que $d = \text{mcd}(a, b)$.

`Unicidad`. Supongamos que d_1 y d_2 son ambos máximo común divisor de a y b, entonces por $ii)$ de la definición 1.1.5, $d_1|d_2$ y $d_2|d_1$. Luego, como d_1 y d_2 son positivos por definición, por $v)$ del Teorema 1.1.2, se concluye que $d_1 = d_2$. ■

Lema 1.1.7. Si a y b son números enteros no ambos cero y $a = qb + r$ para algunos enteros q y r entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración. Por el Teorema 1.1.3, cualquier común divisor de b y r también divide a $qb+r = a$; similarmente, como $r = a-qb$, se sigue que cualquier divisor de a y b también divide a r. Así, tanto a, b como b, r tienen los mismos divisores y, por tanto, el mismo máximo común divisor. ■

Teorema 1.1.8 (Algoritmo de Euclides)**.** Sean $r_0 = a$ y $r_1 = b$ enteros tales que $a \geq b > 0$. Si aplicamos el algoritmo de la división sucesivamente hasta obtener $r_j = r_{j+1}q_{j+1} + r_{j+2}$, con $0 < r_{j+2} < r_{j+1}$, para $j = 0, 1, \ldots, n-2$ y $r_{n+1} = 0$, entonces $r_n = \text{mcd}(a, b)$, donde r_n es el último residuo distinto de cero.

Demostración. Empezando con $r_0 = a$ y $r_1 = b$ aplicamos sucesivamente el algoritmo de la división dando lugar a

$$\begin{aligned}
r_0 &= r_1q_1 + r_2 && 0 \leq r_2 < r_1, \\
r_1 &= r_2q_2 + r_3 && 0 \leq r_3 < r_2, \\
&\vdots \\
r_{j-2} &= r_{j-1}q_{j-1} + r_j && 0 \leq r_j < r_{j-1}, \\
&\vdots \\
r_{n-4} &= r_{n-3}q_{n-3} + r_{n-2} && 0 \leq r_{n-2} < r_{n-3}, \\
r_{n-3} &= r_{n-2}q_{n-2} + r_{n-1} && 0 \leq r_{n-1} < r_{n-2}, \qquad (1.1) \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n && 0 \leq r_n < r_{n-1}, \qquad (1.2) \\
r_{n-1} &= r_nq_n.
\end{aligned}$$

Podemos asumir entonces que eventualmente se obtendrá un residuo igual a cero, pues la secuencia de residuos $a = r_0 \geq r_1 > r_2 > \cdots \geq 0$ no puede tener más de a términos (ya que cada residuo es entero). Por el lema 1.1.7, se sigue que $\text{mcd}(a, b) = \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \text{mcd}(r_2, r_3) = \cdots = \text{mcd}(r_{n-3}, r_{n-2}) = \text{mcd}(r_{n-2}, r_{n-1}) = \text{mcd}(r_{n-1}, r_n) = \text{mcd}(r_n, 0) = r_n$. Así, $\text{mcd}(a, b) = r_n$, con r_n el último residuo distinto de cero. Nótese que con esta prueba también queda demostrada la existencia del $\text{mcd}(a, b)$. ■

Teorema 1.1.9. Si a y b son enteros (no ambos 0) y $d = \text{mcd}(a, b)$, entonces existen enteros x y y tales que

$$d = ax + by.$$

Demostración. Ver demostración de la Observación 1.1.6. ■

Teorema 1.1.10. Sean a, b y c números enteros, no ambos cero, y $d = \text{mcd}(a, b)$. Entonces la ecuación $ax + by = c$ tiene solución entera si y sólo si c es un múltiplo de d.

Demostración. $\Rightarrow$) Si $c = ax + by$ para algunos enteros x, y, entonces, como $d|a$ y $d|b$, por el Teorema 1.1.3, $d|c$.
$\Leftarrow$) Si $c = de$ para algún entero e, entonces, escribiendo $d = ax_0 + by_0$ (como en el Teorema 1.1.9), se sigue que $c = ax_0e + by_0e = ax + by$, con $x = x_0e$ y $y = y_0e$ enteros.

■

Definición 1.1.11. Si $\text{mcd}(a, b) = 1$ se dice que a y b son *primos relativos* (o *coprimos*).

Corolario 1.1.12. Dos enteros a y b son coprimos si y sólo si existen enteros u y v tales que

$$au + bv = 1.$$

Demostración. Del Teorema 1.1.9, se tiene $\text{mcd}(a, b) = d = au + bv$, para algunos enteros u, v. Si $d = 1$, entonces $1 = au + bv$. Por otro lado, si $1 = au + bv$, por el Teorema anterior, 1 es múltiplo de d, lo cual sólo puede ocurrir para $d = 1$. ■

Corolario 1.1.13. Sean a y b primos relativos.

a) Si $a|c$ y $b|c$, entonces $ab|c$.

b) Si $a|bc$, entonces $a|c$.

Demostración. Dado que a y b son primos relativos, sabemos que existen enteros x, y tales que $ax+by = 1$; asimismo, existen $e, f \in \mathbb{Z}$ tales que $c = ae$ y $c = bf$. Entonces $c = cax+bcy = (bf)ax+(ae)by = ab(fx+ey)$, por lo que $ab|c$, y la primera afirmación queda demostrada. Por otro lado, como se puede escribir $c = cax + cby$ y $a|bc$ y $a|a$, por el Teorema 1.1.3, $a|(cax + cby) = c$, y hemos terminado. ■

1.1.2. Números Primos

Definición 1.1.14. Un entero p es llamado *número primo* si se cumple que

i) $p > 1$, y

ii) los únicos divisores positivos de p son 1 y p mismo.

Si $p > 1$ y no es primo, entonces p es llamado número *compuesto*.

Teorema 1.1.15. Sea p primo y a un entero. Si $p \nmid a$ entonces $\text{mcd}(a, p) = 1$.

Demostración. Sea $d = \text{mcd}(p, a)$, entonces $d|p$, por lo que $d = 1$ ó $d = p$; pero $d|a$, entonces, por la hipótesis, $d \neq p$. Así, $d = 1$. ■

Teorema 1.1.16. Sean a y b enteros y p número primo. Si $p|ab$ entonces $p|a$ o $p|b$.

Demostración. Si $p \nmid a$, por el teorema anterior se tiene que $\text{mcd}(a,p) = 1$; por otro lado, el Teorema 1.1.9 garantiza que $1 = ax + py$, para algunos enteros x, y, por lo que

$$b = axb + pyb.$$

Por hipótesis $p|ab$, entonces p también divide a axb; claramente p divide a pyb, entonces también divide a b, como se quería. ■

Teorema 1.1.17 (Teorema Fundamental de la Aritmética)**.** Todo entero $n > 1$ puede ser representado como producto de números primos de manera única, excepto por el orden de los factores.

Demostración. `Existencia de la factorización`. Por inducción sobre n. Para $n = 2$ el teorema es claramente cierto, pues 2 es primo; supongamos que es cierto para todo entero mayor que 1 y menor que n, y probémoslo para n. Si n es primo no hay nada más que probar. Supongamos que n es compuesto, entonces $n = ab$, con $1 < a < n$ y $1 < b < n$. Por hipótesis de inducción cada uno de a y b se factorizan como producto de primos, entonces $n = ab$ también se factoriza como producto de primos.

`Unicidad`. Supongamos que n tiene dos factorizaciones, digamos

$$n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r} = {q_1}^{a_1}{q_2}^{a_2}\cdots{q_s}^{a_s},$$

donde p_i y q_j son primos, $p_i \neq p_j$ y $q_i \neq q_j$ si $i \neq j$, y los exponentes e_i, a_j son positivos. Deseamos probar que $r = s$ y que cada p_i es igual a algún q_j. Como p_1 divide a ${q_1}^{a_1}{q_2}^{a_2}\cdots{q_s}^{a_s}$, entonces debe dividir a uno de los factores, por lo que, reordenando de ser necesario, podemos suponer que $p_1|q_1$ y de esto se sigue que $p_1 = q_1$, pues tanto p_1 como q_1 son primos; asimismo, necesariamente $e_1 = a_1$, pues si por ejemplo $e_1 > a_1$, entonces

$$p_1|{q_2}^{a_2}\cdots{q_s}^{a_s},$$

lo cual es imposible, pues $q_j \neq q_k$ para $j \neq k$, $j = 1, 2, \ldots, s$. Continuando con este argumento se muestra que $s = r$, $e_i = a_i$ y $p_i = q_i$, para todo i. ■

Teorema 1.1.18 (Euclides)**.** Existe una infinidad de números primos.

Demostración. Por contradicción, supongamos que existe solamente una colección finita de primos, digamos $p_1, p_2, \ldots, p_n$. Sea

$$m = p_1p_2\cdots p_n + 1.$$

Como $m \in \mathbb{Z}$ y $m > 1$, por el Teorema 1.1.17, m es divisible por algún primo p, el cual debe ser alguno del conjunto $\{p_1, p_2, \ldots, p_n\}$; luego, p divide al producto $p_1 p_2 \cdots p_n$. Así, p divide a m y a $p_1 p_2 \cdots p_n$, y por lo tanto también divide a $m - p_1 p_2 \cdots p_n = 1$, lo cual es imposible. Concluimos entonces que existe una cantidad infinita de primos. ■

1.1.3. Congruencias

Definición 1.1.19. Sea m un entero positivo. Si a y b son enteros, decimos que *a es congruente con b módulo m* si $m|(a-b)$.

Si a es congruente con b módulo m, escribimos $a \equiv b \pmod{m}$. Si $m \nmid (a-b)$, escribimos $a \not\equiv b \pmod{m}$ y decimos que *a y b no son congruentes módulo m.*

El siguiente teorema establece algunas propiedades importantes de las congruencias.

Teorema 1.1.20. Sea m un entero positivo. Las congruencias módulo m satisfacen las siguientes propiedades:

i) *Reflexividad.* Si a es un entero, entonces $a \equiv a \pmod{m}$.

ii) *Simetría.* Si a y b son enteros tales que $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$.

iii) *Transitividad.* Si a, b y c son enteros tales que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$

Demostración. De acuerdo con la definición 1.1.19, claramente $m|(a-a)$, para todo entero a, por lo que se cumple la reflexividad. Por otro lado, si $a \equiv b \pmod{m}$ entonces $m|(a-b)$, pero entonces m también divide a $(b-a)$ y, por tanto, $b \equiv a \pmod{m}$, de manera que hay simetría. Finalmente, si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $m|(a-b)$ y $m|(b-c)$. Luego, $m|(a-b)+(b-c) = a-c$, es decir, $a \equiv c \pmod{m}$, y la transitividad queda demostrada. ■

Observación 1.1.21. Por el Teorema 1.1.20, observamos que para $n > 0$, la congruencia módulo n es una relación de equivalencia en $\mathbb{Z}$.

Definición 1.1.22. Sean a y n números enteros, con $n > 0$. La clase de equivalencia de a, denotada como $[a]$, es llamada la *clase de congruencia* (o *clase residual*) de a módulo n, y se define como

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} \\ &= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}.\end{aligned}$$

Observación 1.1.23. Cada clase corresponde a uno de los posibles residuos $r = 0, 1, \ldots, n$ en la división por n, por lo que hay n diferentes clases de congruencia, a saber

$$\begin{aligned}
[0] &= \{\ldots, 2n, -n, 0, n, 2n, \ldots\}, \\
[1] &= \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, \ldots\}, \\
&\ldots \\
[n-1] &= \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}.
\end{aligned}$$

Asimismo, observamos que no hay más clases de congruencia distintas, pues por ejemplo

$$[n] = \{\ldots, -n, 0, n, 2n, 3n, \ldots\} = [0].$$

De manera más general, tenemos

$$[a] = [b] \quad \text{si y sólo si} \quad a \equiv b \pmod{n}.$$

Observación 1.1.24. Para $n \geq 1$, denotamos al conjunto de n clases de equivalencia mód(n) como $\frac{\mathbb{Z}}{n\mathbb{Z}}$, y lo llamamos el conjunto de enteros mód n.

Definición 1.1.25. Si $[a]$ y $[b]$ son elementos de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (es decir, clases de congruencia mód(n)), definimos a la suma, diferencia y producto como las clases

$$\begin{aligned}
[a] + [b] &= [a+b], \\
[a] - [b] &= [a-b], \\
[a][b] &= [ab]
\end{aligned}$$

que contienen a los enteros $a+b, a-b$ y ab, respectivamente.

Proposición 1.1.26. Si $c > 0$ entonces $a \equiv b \pmod{m}$ si y sólo si $ac \equiv bc \pmod{mc}$.

Demostración. Dado que $c \neq 0$, entonces $m|(b-a)$ si y sólo si $cm|c(b-a)$, por lo que el teorema se concluye inmediatamente. ■

Proposición 1.1.27. Si a, b, c y m son enteros tales que $m > 0, d = \text{mcd}(c, m)$ y $ac \equiv bc \pmod{m}$, entonces $a \equiv b \pmod{\frac{m}{d}}$.

Demostración. Si $ac \equiv bc \pmod{m}$, entonces $m|(ac - bc) = c(a-b)$ y por tanto,

$$\frac{m}{d} \Big| \frac{c}{d}(a-b),$$

pero como $mcd(c, m) = 1$, entonces $(m/d)|(a-b)$; es decir, $a \equiv b \pmod{\frac{m}{d}}$. ■

Corolario 1.1.28. Si a, b, c y m son enteros tales que $m > 0$, $\text{mcd}(c, m) = 1$ y $ac \equiv bc \pmod{m}$, entonces $a \equiv b \pmod{m}$.

Demostración. Hágase $d = 1$ en el teorema anterior. ■

El siguiente teorema es muy útil pues nos muestra la forma en que podemos operar con las congruencias.

Teorema 1.1.29. Si a, b, c, d y m son enteros tales que $m > 0$, $a \equiv b \pmod{m}$, y $c \equiv d \pmod{m}$, entonces

i) $a + c \equiv b + d \pmod{m}$,

ii) $a - c \equiv b - d \pmod{m}$,

iii) $ac \equiv bd \pmod{m}$.

Demostración. Como $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $m|(a - b)$ y $m|(c - d)$. Así, existen enteros k y l tales que $km = a - b$ y $lm = c - d$. Luego, $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = m(k + l)$. De esto, se sigue que $m|[(a + c) - (b + d)]$ y por lo tanto, $a + c \equiv b + d \pmod{m}$.

Por otra parte, $(a-c)-(b-d) = (a-b)-(c-d) = km-lm = m(k-l)$, de manera que $m|[(a - c) - (b - d)]$; esto es, $a - c \equiv b - d \pmod{m}$.

Finalmente, $ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d) = ckm+blm = m(ck + bl)$. Luego, $m|(ac - bd)$ y entonces $ac \equiv bd \pmod{m}$ ■

Teorema 1.1.30. Si a, b, k y m son enteros tales que $k > 0, m > 0$ y $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$.

Demostración. Por *iii*) del teorema anterior, pordemos multiplicar $a \equiv b \pmod{m}$ consigo misma k veces. ■

Presentamos a continuación un importante teorema cuya utilidad no sólo se limita a facilitar el cálculo de congruencias con exponentes, sino que, como se verá en lo sucesivo, es de gran ayuda en la demostración de varios resultados.

Teorema 1.1.31. (Pequeño Teorema de Fermat). Sea p primo y a un entero tal que $p \nmid a$. Entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. Comencemos considerando los primeros $p-1$ múltiplos positivos de a; esto es, los enteros

$$a, 2a, 3a, \ldots, (p-1)a.$$

Ninguno de estos enteros es congruente módulo p con algún otro, y tampoco son congruentes con cero. De hecho, si ocurriera que

$$ra \equiv sa \pmod{p}, \qquad 1 \leq r < s \leq p-1,$$

entonces a podría ser cancelado para tener $r \equiv s \pmod{p}$, lo cual es imposible. Así, el conjunto de múltiplos anteriores debe ser congruente módulo p con $1, 2, 3, \ldots, p-1$, aunque no necesariamente en este orden. Multiplicando todas estas congruencias tenemos,,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p};$$

esto es,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Como $p \nmid (p-1)!$, podemos cancelar $(p-1)!$ en la congruencia anterior y finalmente llegar a

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

■

Teorema 1.1.32. Sea $f(x)$ un polinomio con coeficientes enteros, y sea m un entero positivo. Si $a \equiv b \pmod{m}$, entonces $f(a) \equiv f(b) \pmod{m}$

Demostración. Escribamos $f(x) = c_0 + c_1 x + \cdots + c_k x^k$, donde cada c_i es un entero. Si $a \equiv b \pmod{m}$, entonces por el teorema anterior, $a^i \equiv b^i \pmod{m}$ para todo $i \geq 0$, de manera que entonces $c_i a^i \equiv c_i b^i \pmod{m}$, para todo i, y por lo tanto, $f(a) = \sum c_i a^i \equiv \sum c_i b^i = f(b) \pmod{m}$ ■

Definición 1.1.33. Un *sistema completo de residuos módulo m* es un conjunto de enteros tales que todo entero es congruente módulo m con exactamente uno de los elementos de este conjunto.

Observación 1.1.34. De acuerdo con la definición de clases de congruencia, a un sistema completo de residuos módulo n también lo podemos definir como un conjunto de n enteros que contiene a un representante de cada una de las clases de congruencia en $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Ejemplo 1.1.35. Por el algoritmo de la división, el conjunto de enteros $\{0, 1, 2, \ldots, m-1\}$ es un sistema completo de residuos módulo m y se le conoce como el conjunto de *residuos mínimos no negativos módulo m.*

Ejemplo 1.1.36. Sea m un entero positivo impar. Entonces el conjunto de enteros

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \frac{m-3}{2}, \frac{m-1}{2},$$

es el conjunto de *residuos mínimos absolutos módulo m.*

Lema 1.1.37. Un conjunto de m enteros incongruentes entre sí módulo m forma un sistema completo de residuos módulo m.

Demostración. Supongamos que un conjunto de m enteros incongruentes módulo m no forman un sistema completo de residuos módulo m. Esto implica que existe al menos un entero a que no es congruente con ninguno de los enteros del conjunto. De esta manera, no existe un entero en este conjunto que sea congruente módulo m con el residuo que queda cuando a es dividido por m, por lo que sólo puede haber a lo más $m-1$ residuos diferentes cuando los enteros son divididos por m. De esto se sigue, (por el *principio de las casillas*, el cual señala que si más de n objetos son distribuidos en n casillas, entonces debe haber al menos dos objetos en la misma casilla) que al menos dos enteros en el conjunto tienen el mismo residuo módulo m, lo cual es imposible porque estos enteros son incongruentes módulo m. Así, cualquier conjunto de m enteros incongruentes módulo m forman un sistema completo de residuos módulo m. ■

Teorema 1.1.38. Si $r_1, r_2, \ldots, r_m$ es un sistema completo de residuos módulo m, y si a es un entero positivo tal que $mcd(a, m) = 1$, entonces

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

es un sistema completo de residuos módulo m para cualquier entero b.

Demostración. Basta probar que ningún par de números de los enteros $ar_1 + b$, $ar_2 + b, \ldots, ar_m + b$ son congruentes módulo m. Observamos que si $ar_j + b \equiv ar_k + b \pmod{m}$, entonces $ar_j \equiv ar_k \pmod{m}$, y como $\text{mcd}(a, m) = 1$, por el Corolario 1.1.28 tenemos que $r_j \equiv r_k \pmod{m}$. Dado que $r_j \not\equiv r_k \pmod{m}$ si $j \neq k$, se concluye entonces que $j = k$. La conclusión del teorema queda demostrada observando que entonces $\{r_1, r_2, \ldots, r_m\}$ es un conjunto de m enteros incongruentes módulo m, de manera que por el Lema 1.1.37, estos enteros forman un sistema completo de residuos módulo m. ■

1.1.4. Congruencias Lineales

Definición 1.1.39. Una congruencia de la forma

$$ax \equiv b \pmod{m},$$

donde x es una variable, es llamada *congruencia lineal.*

Observación 1.1.40. Como $ax \equiv b \pmod{n}$ si y sólo si $ax - b$ es múltiplo de n, x será solución de esta congruencia lineal si y sólo si existe un entero y tal que x y y satisfacen la ecuación $ax + ny = b$.

Lema 1.1.41. Si x_0, y_0 es cualquier solución particular de $ax + by = c$, entonces todas las demás soluciones son de la forma

$$x = x_0 + \left(\frac{b}{d}\right) t, \qquad y = y_0 - \left(\frac{a}{d}\right) t,$$

donde t es un entero arbitrario y $d = \text{mcd}(a, b)$.

Demostración. Recordemos del Teorema 1.1.10 que $ax+by = c$ tiene solución si y sólo si $d|c$.

Ahora, supongamos que x_0, y_0 es una solución conocida de $ax + by = c$, es decir,

$$ax_0 + by_0 = c.$$

Si definimos

$$x = x_0 + \frac{bt}{d}, \qquad y = y_0 - \frac{at}{d},$$

donde t es cualquier entero, entonces

$$ax + by = a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) = ax_0 + by_0 = c,$$

por lo que x, y también es solución. Para mostrar que estas son las únicas soluciones, sea x', y' otra solución, es decir, $ax' + by' = c$. Como $ax' + by' = c = ax_0 + by_0$ tenemos

$$a(x' - x_0) + b(y' - y_0) = 0,$$

por lo que dividiendo por d nos queda

$$\frac{a}{d}(x' - x_0) = -\frac{b}{d}(y' - y_0). \tag{1.3}$$

Al ser a y b no ambos cero, sin pérdida de generalidad podemos suponer $b \neq 0$; como $\frac{b}{d}$ divide cada lado de (1.3), y es coprimo con $\frac{a}{d}$, entonces, por el Corolario 1.1.13, divide a $x' - x_0$; es decir, $x' - x_0 = \frac{b}{d}t$, para algún entero t, por lo que

$$x' = x_0 + \frac{b}{d}t.$$

Sustituyendo $x' - x_0$ en (1.3), tenemos

$$-\frac{b}{d}(y' - y_0) = \frac{a}{d}(x' - x_0) = \frac{a}{d} \cdot \frac{b}{d}t,$$

y dividiendo por $\dfrac{b}{d}$ nos queda

$$y' = y_0 - \frac{a}{d}t.$$

■

Teorema 1.1.42. Si $d = \text{mcd}(a, m)$, entonces la congruencia lineal

$$ax \equiv b \pmod{m}$$

tiene solución si y sólo si d divide a b. Si $d|b$, entonces tiene d soluciones mutuamente no congruentes módulo m.

Demostración. Ya hemos observado que la congruencia dada es equivalente a la ecuación $ax + my = b$. Por el Teorema 1.1.10, sabemos también que esta última ecuación tiene solución si y sólo si $d|b$; además, si x_0, y_0 es una solución particular, entonces cualquier otra solución es de la forma

$$x = x_0 + \frac{m}{d}t, \qquad y = y_0 - \frac{a}{d}t,$$

para un entero t arbitrario. De entre los enteros que satisfacen la primera de estas expresiones, consideremos aquellos que ocurren cuando t toma los valores $t = 0, 1, 2, \ldots, d - 1$:

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

Afirmamos que estos enteros son no congruentes módulo m, y cualquier otro entero x de esta forma es congruente con alguno de ellos. Si ocurriera que

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m},$$

donde $0 \leq t_1 < t_2 \leq d - 1$, entonces tendríamos

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}.$$

Como el $\text{mcd}(\frac{m}{d}, m) = \frac{m}{d}$, por la Proposición 1.1.27 el factor $\dfrac{m}{d}$ puede ser cancelado y llegamos a la congruencia

$$t_1 \equiv t_2 \pmod{d},$$

es decir, $d|(t_2 - t_1)$, lo cual es imposible por la desigualdad $0 < t_2 - t_1 < d$.

Nos falta demostrar que cualquier otra solución $x_0 + \frac{m}{d}t$ es congruente módulo m con alguno de los d enteros mencionados anteriormente. Por el algoritmo de la división, existen enteros q, r tales que $t = qd+r$, $0 \leq r \leq d-1$. Entonces,

$$\begin{aligned} x_0 + \frac{m}{d}t &= x_0 + \frac{m}{d}(qd + r) \\ &= x_0 + mq + \frac{m}{d}r \\ &\equiv x_0 + \frac{m}{d}r \pmod{m}, \end{aligned}$$

donde $x_0 + \frac{m}{d}r$ es una de las d soluciones que ya habíamos descrito anteriormente. ■

Una vez considerada una sola congruencia lineal, es natural pensar en el problema de resolver un sistema simultáneo de congruencias lineales:

$$a_1x \equiv b_1 \pmod{m_1}, a_2x \equiv b_2 \pmod{m_2}, \ldots, a_rx \equiv b_r \pmod{m_r}.$$

Es el Teorema Chino del Residuo, presentado a continuación, con lo que se resuelve este problema.

Teorema 1.1.43. (Teorema Chino del Residuo.) Sean $n_1, n_2, \ldots, n_r$ enteros positivos tales que $\text{mcd}(n_i, n_j) = 1$ para $i \neq j$. Entonces el sistema de ecuaciones lineales

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

tiene una solución simultánea, que además es única módulo $n_1n_2 \cdots n_r$.

Demostración. Empezaremos definiendo el producto $n = n_1n_2 \cdots n_r$. Para cada $k = 1, 2, \ldots, r$, sea

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1}n_{k+1} \cdots n_r.$$

Por hipótesis, los n_i son primos relativos a pares, por lo que $\text{mcd}(N_k, n_k) = 1$ y la congruencia $N_kx \equiv 1 \pmod{n_k}$ tiene una única solución $x_k \pmod{n_k}$,

de acuerdo con el teorema anterior. Nuestro propósito ahora será demostrar que el entero

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

es una solución simultánea del sistema dado.

Primero, observamos que $N_i \equiv 0 \pmod{n_k}$, pues en este caso $n_k | N_i$, si $k \neq i$. Así,

$$\overline{x} = a_1 N_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

Pero x_k satisface $N_k x \equiv 1 \pmod{n_k}$, entonces

$$\overline{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k},$$

probando así que existe una solución para el sistema dado.

Para probar la unicidad de la solución, supongamos que x' es cualquier otra solución; entonces,

$$\overline{x} \equiv a_k \equiv x' \pmod{n_k}, \qquad k = 1, 2, \ldots r,$$

es decir, $n_k | \overline{x} - x'$ para cada valor de k. Como $\text{mcd}(n_i, n_j) = 1$, por el Corolario 1.1.13 se sigue que $n_1 n_2 \cdots n_r | \overline{x} - x'$; es decir, $\overline{x} \equiv x' \pmod{n}$. ■

1.1.5. Congruencias Cuadráticas

Ya hemos estudiado la ecuación $ax \equiv b \pmod{n}$, y determinado cuándo tiene o no solución. ¿Qué pasará con las congruencias cuadráticas?

Comencemos considerando la congruencia

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1.4}$$

donde p es primo impar y $a \not\equiv 0 \pmod{p}$; esto es, $\text{mcd}(a, p) = 1$. Como p es primo impar, entonces $\text{mcd}(4a, p) = 1$ y (1.4) es equivalente a $4a(ax^2 + bx + c) \equiv 0 \pmod{p}$ ó $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$. Ahora, haciendo $y = 2ax + b$ y $d = b^2 - 4ac$, tenemos

$$y^2 \equiv d \pmod{p}. \tag{1.5}$$

Si $x \equiv x_0 \pmod{p}$ es solución de (1.4), entonces $y \equiv 2ax_0 + b \pmod{p}$ satisface (1.5); análogamente, si $y \equiv y_0 \pmod{p}$ satisface (1.5), entonces

$2ax \equiv y_0 - b \pmod{p}$ puede resolverse para obtener la solución de (1.4).

Así, el problema de encontrar una solución de (1.4) se reduce a encontrar la solución de una congruencia cuadrática lineal y de una congruencia cuadrática de la forma

$$y^2 \equiv d \pmod{p}.$$

Definición 1.1.44. Sea p un primo impar y $\mcd(a, p) = 1$. Si la congruencia cuadrática $x^2 \equiv a \pmod{p}$ tiene solución, decimos que a es un *residuo cuadrático* de p. De lo contrario, a es un *residuo no cuadrático* de p.

Nótese que si $a \equiv b \pmod{p}$, entonces a es un residuo cuadrático de p si y sólo si b es un residuo cuadrático de p, por lo que, para conocer los residuos cuadráticos módulo p, sólo es necesario calcular los cuadrados de aquellos enteros positivos menores que p.

Ejemplo 1.1.45. Para determinar qué enteros son residuos cuadráticos de 11, calculamos los cuadrados de los enteros $1, 2, 3, \ldots, 10$ y los reducimos módulo p. Tenemos,

$$\begin{array}{ll} 1^2 \equiv 10^2 \equiv 1 \pmod{11} & 4^2 \equiv 7^2 \equiv 5 \pmod{11} \\ 2^2 \equiv 9^2 \equiv 4 \pmod{11} & 5^2 \equiv 6^2 \equiv 3 \pmod{11} \\ 3^2 \equiv 8^2 \equiv 9 \pmod{11} & \end{array}$$

Más aún, como $(p-k)^2 \equiv k^2 \pmod{p}$, la lista de residuos cuadráticos es simétrica alrededor de $p/2$, así que sólo es necesario verificar los cuadrados de 1 a $(p-1)/2$.

Lema 1.1.46. Sea p un primo impar y a un entero no divisible por p. Entonces la congruencia $x^2 \equiv a \pmod{p}$ no tiene soluciones ó tiene exactamente dos soluciones que son incongruentes módulo p.

Demostración. Si $x^2 \equiv a \pmod{p}$ tiene una solución, digamos $x = x_0$, se observa que $x = -x_0$ es una segunda solución, pues $(-x_0)^2 = x_0^2 \equiv a \pmod{p}$. Además, $x_0 \not\equiv -x_0 \pmod{p}$, pues de lo contrario, si $x_0 \equiv -x_0 \pmod{p}$, entonces $2x_0 \equiv 0 \pmod{p}$, lo cual es imposible pues p es impar y $p \nmid x_0$ porque $x_0^2 \equiv a \pmod{p}$ y $p \nmid a$.

Para mostrar que no hay más soluciones incongruentes, supongamos que x_0 y x_1 son ambas soluciones de $x^2 \equiv a \pmod{p}$. Entonces,

$$x_0^2 \equiv x_1^2 \equiv a \pmod{p},$$

por lo que,

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}.$$

Así, $p|(x_0 - x_1)$ o $p|(x_0 + x_1)$; es decir, $x_1 \equiv x_0 \pmod{p}$ o $x_1 \equiv -x_0 \pmod{p}$. ■

Proposición 1.1.47. Si p es un primo impar, entonces hay exactamente $(p-1)/2$ residuos cuadráticos y $(p-1)/2$ residuos no cuadráticos de p entre los enteros $1, 2, \ldots, p-1$.

Demostración. Para encontrar los residuos cuadráticos de p entre los enteros $1, 2, \ldots, p-1$, calculamos los residuos mínimos positivos módulo p de los cuadrados de estos enteros. Como hay $p-1$ cuadrados por considerar y como cada congruencia $x^2 \equiv a \pmod{p}$ tiene o cero o dos soluciones, entonces debe haber exactamente $(p-1)/2$ residuos cuadráticos de p entre los enteros $1, 2, \ldots, p-1$. Los restantes son residuos no cuadráticos. ■

Una notación que simplifica el uso de residuos cuadráticos y que se usará a partir de este momento es la siguiente.

Definición 1.1.48. Sea p un primo impar y sea $\text{mcd}(a, p) = 1$. Definimos el *Símbolo de Legendre* como

$$\left(\frac{a}{p}\right)_{\mathcal{L}} = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático de } p, \\ -1 & \text{si } a \text{ no es residuo cuadrático de } p. \end{cases}$$

El siguiente criterio, debido a Euler, permite decidir cuándo un entero es residuo cuadrático de un número primo.

Teorema 1.1.49. (Criterio de Euler). Sea p un primo impar y sea a un entero positivo no divisible por p. Entonces

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)_{\mathcal{L}} \pmod{p}.$$

Demostración. Primero, supongamos que $\left(\frac{a}{p}\right)_{\mathcal{L}} = 1$. Entonces la congruencia $x^2 \equiv a \pmod{p}$ tiene solución, digamos $x = x_0$. Usando el Pequeño Teorema de Fermat (Teorema 1.1.31), se tiene

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} = x_0^{p-1} \equiv 1 \pmod{p}.$$

Luego, si $\left(\frac{a}{p}\right)_{\mathcal{L}} = 1$, entonces $\left(\frac{a}{p}\right)_{\mathcal{L}} \equiv a^{(p-1)/2} \pmod{p}$.

Ahora, supongamos que $\left(\frac{a}{p}\right)_{\mathcal{L}} = -1$ y consideremos el polinomio $f(x) = x^{(p-1)/2} - 1$. Como $f(x)$ tiene grado $(p-1)/2$, la congruencia $f(x) \equiv 0 \pmod{p}$ tiene a lo más $(p-1)/2$ soluciones. Pero si t es un residuo cuadrático de p entonces existe $x \in \mathbb{Z}$ tal que $x^2 \equiv t \pmod{p}$, por lo que, usando el Pequeño Teorema de Fermat, tenemos

$$t^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}.$$

Así, t es solución de $x^{(p-1)/2}-1$ y por tanto, los $(p-1)/2$ residuos cuadráticos mód p son soluciones de $f(x)$. De esta manera, los residuos no cuadráticos no son soluciones, y entonces

$$a^{(p-1)/2} \not\equiv 1 \pmod{p}, \quad \text{si } \left(\frac{a}{p}\right)_{\mathcal{L}} = -1.$$

Pero, una vez más por el Pequeño Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$, entonces se sigue que

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p};$$

esto es, $p|(a^{(p-1)/2} - 1)$ ó $p|(a^{(p-1)/2} + 1)$, es decir, $a^{(p-1)/2} \equiv 1 \pmod{p}$ ó $a^{(p-1)/2} \equiv -1 \pmod{p}$. Como ya habíamos visto que $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ si $\left(\frac{a}{p}\right)_{\mathcal{L}} = -1$, entonces

$$a^{(p-1)/2} \equiv -1 \pmod{p},$$

como queríamos. ■

Algunas propiedades del símbolo de Legendre son las siguientes:

Teorema 1.1.50. Sea p un primo impar y a y b enteros no divisibles por p. Entonces se tienen las siguientes propiedades:

i) Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right)_{\mathcal{L}} = \left(\frac{b}{p}\right)_{\mathcal{L}}$.

ii) $\left(\frac{a}{p}\right)_{\mathcal{L}} \left(\frac{b}{p}\right)_{\mathcal{L}} = \left(\frac{ab}{p}\right)_{\mathcal{L}}$.

iii) $\left(\frac{a^2}{p}\right)_{\mathcal{L}} = 1$.

Demostración. Si $a \equiv b \pmod{p}$ entonces $x^2 \equiv a \pmod{p}$ tiene solución si y sólo si $x^2 \equiv b \pmod{p}$ tiene solución; por tanto, $\left(\frac{a}{p}\right)_{\mathcal{L}} = \left(\frac{b}{p}\right)_{\mathcal{L}}$, y $i)$ queda demostrado. Ahora, por el criterio de Euler (Teorema 1.1.49) sabemos que $\left(\frac{a}{p}\right)_{\mathcal{L}} \equiv a^{(p-1)/2} \pmod{p}$, $\left(\frac{b}{p}\right)_{\mathcal{L}} \equiv b^{(p-1)/2} \pmod{p}$, y $\left(\frac{ab}{p}\right)_{\mathcal{L}} \equiv (ab)^{(p-1)/2} \pmod{p}$. Luego,

$$\left(\frac{a}{p}\right)_{\mathcal{L}} \left(\frac{b}{p}\right)_{\mathcal{L}} \equiv a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right)_{\mathcal{L}} \pmod{p}.$$

Como los únicos valores posibles del símbolo de Legendre son ± 1, concluimos que

$$\left(\frac{a}{p}\right)_{\mathcal{L}} \left(\frac{b}{p}\right)_{\mathcal{L}} = \left(\frac{ab}{p}\right)_{\mathcal{L}},$$

y $ii)$ se cumple. De esto se sigue, claramente, que $\left(\frac{a^2}{p}\right)_{\mathcal{L}} = \left(\frac{a}{p}\right)_{\mathcal{L}} \left(\frac{a}{p}\right)_{\mathcal{L}} = (\pm 1)^2 = 1$. ■

Teorema 1.1.51. (Lema de Gauss). Consideremos el conjunto de residuos mínimos absolutos módulo p, $S = \{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, 2, \ldots, \frac{p-1}{2}\}$. Si $p \nmid a$, sea μ el número de residuos mínimos absolutos módulo p que son negativos, de los enteros $1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a$. Entonces,

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

Demostración. Sea $\pm m_l$ el residuo mínimo absoluto de $l \cdot a$, donde m_l es positivo. Como l toma valores entre 1 y $\frac{p-1}{2}$, μ es igual al número de signos negativos que acompañan a los m_l.

Afirmamos que $m_l \neq m_k$ si $l \neq k$ y $1 \leq l, k \leq \frac{p-1}{2}$. De otra manera, si $m_l = m_k$, entonces $la \equiv \pm ka \pmod{p}$, y como $p \nmid a$ esto implica que $l \pm k \equiv 0 \pmod{p}$, lo cual es imposible porque $l \neq k$ y $|l \pm k| \leq |l| + |k| \leq p - 1$. Concluimos entonces que los conjuntos $\{1, 2, \ldots, (p-1)/2\}$ y $\{m_1, m_2, \ldots, m_{(p-1)/2}\}$ coinciden. Multiplicando las congruencias $1 \cdot a \equiv \pm m_1 \pmod{p}$, $2 \cdot a \equiv \pm m_2 \pmod{p}, \ldots,$ $((p-1)/2)a \equiv \pm m_{(p-1)/2} \pmod{p}$, obtenemos

$$\left(\frac{p-1}{2}\right)! a^{(p-1)/2} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)! \pmod{p},$$

entonces $a^{(p-1)/2} \equiv (-1)^{\mu} \pmod{p}$. Luego, por el criterio de Euler,

$$\left(\frac{a}{p}\right)_{\mathcal{L}} \equiv (-1)^{\mu} \pmod{p}.$$

■

1.2. Preliminares Algebraicos

Definición 1.2.1. Un grupo $(G, *)$ es un conjunto no vacío de elementos G en el que está definida una operación binaria, denotada por $*$, tal que

1. $a, b, c \in G$ implica que $a * (b * c) = (a * b) * c$ (asociatividad).
2. Existe un elemento $1 \in G$ tal que $a * 1 = 1 * a = a$ para todo $a \in G$ (existencia de elemento neutro en G).
3. Para cada $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a*a^{-1} = a^{-1}*a = 1$ (existencia de inversos en G).

Definición 1.2.2. Un grupo $(G, *)$ se dice que es *abeliano* (o *conmutativo*) si para cualesquier $a, b \in G$ se tiene: $a * b = b * a$.

Definición 1.2.3. Un anillo $(R, +, \cdot)$ es un conjunto R junto con dos operaciones $+$ y $\cdot$, a las que llamamos suma y multiplicación, tal que se cumple lo siguiente:

(i) $(R, +)$ es un grupo abeliano.

(ii) La multiplicación $(\cdot)$ es asociativa.

(iii) Para todo $a, b, c \in R$, $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ y $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$.

Definición 1.2.4. Si la multiplicación de R es tal que $a \cdot b = b \cdot a$ para todo a, b en R, entonces llamamos a R *anillo conmutativo*.

Definición 1.2.5. Si existe un elemento 1 en R tal que $a \cdot 1 = 1 \cdot a$ para todo a en R, diremos que R es un *anillo con unidad*.

Definición 1.2.6. Sea S un subconjunto de un anillo R que es cerrado con respecto a la suma y la multiplicación. Supongamos que $1 \in S$. Supongamos además que con respecto a estas operaciones de suma y multiplicación en S que son inducidas de R, S es por sí mismo un anillo. Decimos en este caso que S es un *subanillo* de R.

Definición 1.2.7. Algunas clases especiales de anillos son las siguientes:

i) Si R es un anillo conmutativo entonces $a \neq 0 \in R$ se dice que es un *divisor de cero* si existe un $b \in R, b \neq 0$, tal que $ab = 0$. Un anillo conmutativo es un *dominio entero* si no tiene divisores de cero. Por ejemplo $\mathbb{Z}$ o el anillo de polinomios en una variable con coeficientes enteros.

ii) Un anillo R se dice que es un *anillo con división* si $R^* = R\backslash\{0\}$ forma un grupo bajo la multiplicación. El anillo de cuaternios es un ejemplo de anillo con división.

iii) Un *campo* es un anillo conmutativo con división; es decir, un campo es un anillo conmutativo con elemento unitario en el que todo elemento distinto de cero tiene inverso multiplicativo. Un ejemplo es el campo de los números racionales $\mathbb{Q}$.

Definición 1.2.8. Sea R un anillo con elemento unitario. Un elemento u en R es una *unidad* de R si tiene un inverso multiplicativo en R; es decir, si existe un elemento $a \in R$ tal que $ua = 1$.

Definición 1.2.9. Sea $p \neq 0$ un elemento del dominio entero R que no es unidad. Si toda factorización de p, digamos $p = ab$, tiene la propiedad de que a o b es una unidad, decimos que p es un elemento *irreducible* de R.

Definición 1.2.10. Dos elementos a y b de R se dice que son asociados si $b = ua$ para alguna unidad u de R.

Definición 1.2.11. Sea R un dominio entero y $p \in R$ distinto de alguna unidad. Decimos que p es primo si $p \neq 0$ y $p|ab$ implica que $p|a$ o $p|b$.

Definición 1.2.12. Un dominio entero R es un *dominio de factorización única* si todo elemento distinto de 0 que no es unidad se puede factorizar como producto de un número finito de elementos irreducibles, y si $p_1 \cdots p_r$ y $q_1 \cdots q_r$ son dos factorizaciones del mismo elemento de R como producto de irreducibles, entonces $r = s$ y los q_j pueden ser renumerados de manera que p_i y q_i son asociados.

Definición 1.2.13. Un dominio entero R es un *dominio euclideano* si existe una función λ de los elementos distintos de cero de R al conjunto $\{0, 1, 2, 3, \dots\}$ tal que si $a, b, \in R, b \neq 0$, entonces existen $c, d \in R$ con la propiedad de que $a = cb + d$ y $d = 0$ ó $\lambda(d) < \lambda(b)$.

Definición 1.2.14. Un *ideal* en un anillo conmutativo R es un subconjunto I de R tal que

i) $0 \in I$;

ii) si $a, b \in I$, entonces $a + b \in I$;

iii) si $a \in I$ $r \in R$, entonces $ra \in I$.

Definición 1.2.15. Un ideal I en un anillo conmutativo R es un *ideal primo* si es un ideal propio, es decir $I \neq R$, y $ab \in I$ implica $a \in I$ o $b \in I$.

Al igual que con los anillos en los que hemos definido un subanillo, también podemos definir subcampos para un campo dado. Tenemos la siguiente definición:

Definición 1.2.16. Un subconjunto F de K es un *subcampo* de K si F es un subanillo de K y F es por sí mismo un campo. Comunmente, llamamos a K una *extensión* de F y nos referimos al par (F, K) como la extensión K/F.

A lo largo de esta sección, F denotará un campo dado y K una extensión de F.

Definición 1.2.17. Un elemento $\alpha \in K$ se dice que es *algebraico sobre* F si existen elementos $a_0, a_1, \ldots, a_n$ en F, no todos cero, tales que

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0.$$

Si $F[x]$ denota el anillo de los polinomios en x sobre F, entonces $\alpha \in K$ es algebraico sobre F si existe un polinomio distinto de cero $p(x) \in F$ que α satisface, es decir, para el cual $p(\alpha) = 0$.

En el caso especial en que F es el campo de los números racionales y K el campo de lo números complejos, tenemos la siguiente definición.

Definición 1.2.18. Un número complejo se dice que es un *número algebraico* si es algebraico sobre el campo de los números racionales; es decir, un número algebraico es un número complejo α que es raíz de un polinomio $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0$, donde $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q}$ y $a_0 \neq 0$.
Un *entero algebraico* ω es un número complejo que es raíz de un polinomio $x^n + b_1x^{n-1} + \cdots + b_n = 0$, donde $b_1, b_2, \ldots, b_n \in \mathbb{Z}$.

Precisamente sobre los polinomios en $\mathbb{Q}[x]$, cabe mencionar algunas definiciones y resultados que en su mayoría son análogos a los presentados, con números enteros, en la primera sección de este capítulo.

En un polinomio $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$, donde $a_0 \neq 0$, llamamos al entero no negativo n el *grado* de $f(x)$, y a a_0 su *coeficiente principal*. Si $a_0 = 1$, entonces decimos que $f(x)$ es un polinomio *mónico*.

Asimismo, un polinomio $f(x)$ es *divisible* por un polinomio $g(x)$, no idénticamente cero, si existe un polinomio $q(x)$ tal que $f(x) = g(x)q(x)$, y lo denotamos como $g(x)|f(x)$. En este caso, el concepto de divisibilidad no es el mismo que el presentado anteriormente para los números enteros, pues por ejemplo, que 3 divida a 7 es cierto si pensamos a 3 y a 7 como polinomios

de grado cero, mientras que como enteros, $3 \nmid 7$. Un resultado que sí es análogo al de los enteros es el *algoritmo de la división*, el cual presentamos a continuación.

Teorema 1.2.19. Para cualesquiera dos polinomios $f(x)$ y $g(x)$ sobre $\mathbb{Q}$, con $g(x) \neq 0$, existen únicos polinomios $q(x)$, $r(x) \in \mathbb{Q}[x]$ tales que

$$f(x) = g(x)q(x) + r(x),$$

donde $r(x) = 0$ ó el grado de $r(x)$ es menor que el grado de $g(x)$.

Demostración. Si $f(x)$ es idénticamente cero o tiene grado menor que el de $g(x)$, definamos $q(x) = 0$ y $r(x) = f(x)$. De otra manera, dividamos $g(x)$ por $f(x)$ para obtener un cociente $q(x)$ y un residuo $r(x)$. Claramente, $q(x)$ y $r(x)$ son polinomios sobre $\mathbb{Q}$ y $r(x) = 0$ ó el grado de $r(x)$ es menor que el de $g(x)$ si la división se hizo completa. Supongamos ahora que existe otro par de polinomios $q_1(x)$ y $r_1(x)$tales que

$$f(x) = g(x)q_1(x) + r_1(x),$$

entonces $r(x) - r_1(x) = g(x)(q_1(x) - q(x))$. Así, $g(x)$ divide al polinomio $r(x) - r_1(x)$, el cual, a menos que sea idénticamente cero, tiene grado menor que el de $g(x)$. Por lo tanto, $r(x) - r_1(x) = 0$, y de esto se sigue que $q(x) = q_1(x)$. ■

Teorema 1.2.20. Cualesquiera dos polinomios $f(x), g(x) \in \mathbb{Q}[x]$, no ambos idénticamente cero, tienen un divisor común $h(x)$ que se puede escribir como combinación lineal de $f(x)$ y $g(x)$. Esto es, $h(x)|f(x), h(x)|g(x)$, y

$$h(x) = f(x)F(x) + g(x)G(x), \tag{1.6}$$

para algunos polinomios $F(x)$ y $G(x)$ en $\mathbb{Q}[x]$.

Demostración. De todos los polinomios de la forma (1.6), que no son idénticamente cero, escojamos cualquiera que sea del grado mínimo y llamémosle $h(x)$. Si $h(x)$ no fuera divisor de $f(x)$ entonces por el algoritmo de la división, existen polinomios $q(x)$ y $r(x)$ tales que $f(x) = h(x)q(x)+r(x)$, con $r(x) \neq 0$ ó el grado de $r(x)$ menor que el grado de $h(x)$. Pero entonces,

$$\begin{aligned} r(x) &= f(x) - h(x)q(x) \\ &= f(x)[1 - f(x)q(x)] - g(x)[G(x)q(x)], \end{aligned}$$

que es de la forma (1.6), lo cual contradice a la elección de $h(x)$; por lo tanto, $h(x)|f(x)$, y similarmente se prueba que $h(x)|g(x)$. ■

Teorema 1.2.21. Para cualesquiera dos polinomios $f(x)$ y $g(x) \in \mathbb{Q}[x]$, no ambos idénticamente cero, corresponde un único polinomio mónico $d(x)$ con las siguientes propiedades:

i) $d(x)|f(x)$, $d(x)|g(x)$;

ii) $d(x)$ se puede escribir como combinación lineal de $f(x)$ y $g(x)$, igual que en (1.6);

iii) cualquier común divisor de $f(x)$ y $g(x)$ es divisor de $d(x)$, y por tanto, no existe otro común divisor de grado menor que el de $d(x)$.

Demostración. Sea $h(x)$ como en el teorema anterior y definamos $d(x) = c^{-1}h(x)$, donde c es el coeficiente principal de $h(x)$, por lo que $d(x)$ es mónico. Las propiedades i) y ii) se obtienen de la definición de $h(x)$ en el teorema anterior, mientras que la ecuación (1.6) implica que

$$d(x) = c^{-1}f(x)F(x) + c^{-1}g(x)G(x),$$

por lo que si $m(x)$ es un divisor común de $f(x)$ y $g(x)$, entonces $m(x)|d(x)$. Finalmente, para probar que $d(x)$ es único, supongamos que tanto $d(x)$ como $d_1(x)$ satisfacen las propiedades i), ii) y iii). Entonces $d(x)|d_1(x)$ y $d_1(x)|d(x)$, por lo que $d_1(x) = q(x)d(x)$ y $d(x) = q_1(x)d_1(x)$ para algunos polinomios $q(x)$ y $q_1(x)$ en $\mathbb{Q}[x]$. Esto implica que $q(x)q_1(x) = 1$, y entonces $q(x)$ y $q_1(x)$ tiene grado cero. Como tanto $d(x)$ como $d_1(x)$ son mónicos, entonces $q(x) = 1$, y $d_1(x) = d(x)$. ■

Definición 1.2.22. El polinomio $d(x)$ del teorema anterior es llamado el *máximo común divisor* de $f(x)$ y $q(x)$. Se denota como $d(x) = \text{mcd}(f(x), g(x))$.

Definición 1.2.23. Sea $f(x) \in \mathbb{Q}[x]$ un polinomio no idénticamente cero. Decimos que $f(x)$ es *irreducible* sobre $\mathbb{Q}$ si no existe alguna factorización, $f(x) = g(x)h(x)$, de $f(x)$ como producto de dos polinomios $g(x)$ y $h(x)$ de grado positivo.

Teorema 1.2.24. Si α es un número algebraico, entonces α es raíz de un único polinomio mónico irreducible $f(x) \in \mathbb{Q}[x]$. Más aún, si $g(x) \in \mathbb{Q}[x]$, $g(\alpha) = 0$, entonces $f(x)|g(x)$.

Demostración. De todos los polinomios sobre $\mathbb{Q}$ para los cuales α es raíz, tomemos el de menor grado, digamos $G(x)$. Si el coeficiente principal de $G(x)$ es C, definamos el polinomio $H(x)$ como $H(x) = C^{-1}G(x)$. Entonces $H(\alpha) = 0$ y $H(x)$ es mónico. Más aún, $H(x)$ es irreducible, pues si $H(x) = H_1(x)H_2(x)$, entonces al menos unos de sus factores tendría a α de raź, es

decir, $H_1(\alpha) = 0$ ó $H_2(\alpha)$, contrario al hecho de que $G(x) = 0$ y $H(x) = 0$ son polinomios de mínimo grado.

Ahora, sea $f(x)$ cualquier polinomio mónico irreducible con $f(\alpha) = 0$. Probaremos primero la segunda afirmación.
Si $f(x) \nmid g(x)$, entonces $\text{mcd}(f(x), g(x)) = 1$, por lo que existen polinomios $h(x), t(x) \in \mathbb{Q}[x]$ tales que

$$f(x)h(x) + g(x)t(x) = 1.$$

Evaluando en $x = \alpha$, tenemos $1 = f(\alpha)h(\alpha) + g(\alpha)t(\alpha) = 0$, lo cual es una contradicción. Así, $f(x)|g(x)$.

Finalmente, para probar que $f(x)$ es único, supongamos que $f_1(x)$ es un polinomio mónico irreducible tal que $f_1(\alpha) = 0$. Entonces $f(x)|f_1(x)$ por lo demostrado en el párrafo anterior, digamos $f_1(x) = f(x)q(x)$; pero la irreducibilidad de $f_1(x)$ implica que $q(x)$ es una constante, y de hecho, $q(x) = 1$, pues $f_1(x)$ y $f(x)$ son mónicos. De esta manera, $f_1(x) = f(x)$. ■

Un resultado importante que cabe señalar sobre estos números es que el conjunto de los números algebraicos forma un campo, mientras que el de los enteros algebraicos forma un anillo ([16, pags. 417-418]).

Definición 1.2.25. El *polinomio mínimo* de un número algebraico α es el polinomio $f(x)$ descrito en el teorema anterior. El *grado* de un número algebraico es el grado de su polinomio mínimo.

Definición 1.2.26. Un *campo numérico* es una extensión de dimensión finita (con $\mathbb{Q}$ como espacio vectorial) del campo de los números racionales, $\mathbb{Q}$.

Por ejemplo, si α es un número algebraico, entonces se puede verificar ([16, pag. 419]) que la colección de números de la forma $f(\alpha)/h(\alpha)$, $h(\alpha) \neq 0$, f y h polinomios sobre $\mathbb{Q}$, constituye un campo. A este campo lo denotamos por $\mathbb{Q}(\alpha)$ y es una extensión finita de $\mathbb{Q}$, es decir, es un campo numérico.

En particular, cuando K es un campo numérico de dimensión 2 sobre $\mathbb{Q}$, lo llamamos *campo cuadrático* (o *extensión cuadrática*). Todo campo cuadrático es de la forma $K = \mathbb{Q}(\sqrt{d})$, para algún entero d libre de cuadrado[1], donde $d \neq 0, 1$.

[1]Un número entero a es *libre de cuadrado* si el cuadrado (un entero de la forma $x = n^2$) más grande que lo divide es 1.

Teorema 1.2.27. Si α es un número algebraico de grado n, entonces todo número en $\mathbb{Q}(\alpha)$ se puede escribir de manera única como

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \tag{1.7}$$

donde $a_i \in \mathbb{Q}$; consecuentemente, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Demostración. Sea $f(\alpha)/h(\alpha) \in \mathbb{Q}(\alpha)$. Si el polinomio mínimo de α es $g(x)$, entonces $g(x) \nmid h(x)$, pues $h(\alpha) \neq 0$. Pero $g(x)$ es irreducible, por lo que $\text{mcd}(g(x), h(x)) = 1$, y por lo tanto existen polinomios $G(x)$ y $H(x)$ tales que $1 = g(x)G(x) + h(x)H(x)$. Sustituyendo x por α y usando el hecho de que $g(\alpha) = 0$, tenemos que $1/h(\alpha) = H(\alpha)$ y $f(\alpha)/h(\alpha) = f(\alpha)H(\alpha)$. Sea $k(x) = f(x)H(x)$, entonces $f(\alpha)/h(\alpha) = k(\alpha)$. Dividiendo $k(x)$ por $g(x)$ tenemos $k(x) = g(x)q(x) + r(x)$, y así, $f(\alpha)/h(\alpha) = k(\alpha) = r(\alpha)$, donde $r(\alpha)$ es de la forma (1.7).

Para probar que la forma (1.7) es única, supongamos que $r(\alpha)$ y $r_1(\alpha)$ son expresiones de la forma (1.7). Si $r(x) - r_1(\alpha)$ no es idénticamente cero, entonces es un polinomio de grado menor que n. Como el polinomio mínimo de α tiene grado n, entonces $r(\alpha) - r_1(\alpha) \neq 0$, $r(\alpha) \neq r_1(\alpha)$, a menos que $r(x)$ y $r_1(x)$ sean el mismo polinomio. ■

Finalmente, cabe destacar que el campo $\mathbb{Q}(\alpha)$ puede ser visto considerando congruencias módulo el polinomio $f(x)$. Esto es, análogamente al caso de los números enteros, para cualquier polinomio $F(x)$ de grado al menos uno escribimos

$$f_1(x) \equiv f_2(x) \pmod{F(x)}$$

si $F(x)|(f_1(x) - f_2(x))$.

Capítulo 2

Diversas pruebas de la Ley de Reciprocidad Cuadrática

2.1. Introducción

En este capítulo enunciaremos y demostraremos la Ley de Reciprocidad Cuadrática. Primeramente, mostraremos su discusión de manera similar a la que siguieron Euler, Legendre y Gauss con un problema sobre ecuaciones diofánticas.

Sea n un número entero libre de cuadrado, p un primo, y consideremos la ecuación

$$x^2 - ny^2 = p. \tag{2.1}$$

La pregunta que surge inmediatamente es, ¿cuándo tiene soluciones enteras esta ecuación? Es precisamente el estudio de su respuesta lo que ha dado lugar a un gran número de resultados en Teoría de Números, pues resolver la ecuación (2.1) es equivalente a hacerlo cuando el primo p se descompone en el campo $\mathbb{Q}(\sqrt{n})$. El caso particular $n = -1$, lo respondió Fermat en 1640, aunque no proporcionó prueba alguna: un primo p se puede escribir como la suma del cuadrado de dos enteros si y sólo si $p = 2$ o p es congruente con 1 módulo 4. A continuación discutiremos algunas condiciones necesarias para que la ecuación (2.1) tenga solución.

Primero, hacemos notar que si una ecuación con coeficientes enteros tiene solución entera entonces también tendrá solución si la vemos como una congruencia módulo n, para cualquier entero n. De esta manera, una forma de saber si una ecuación tiene soluciones es reducirla módulo n y observar si las

hay. Para intentar esto en este caso, tomemos el caso especial donde $n = q$, y p y q son primos impares distintos, es decir,

$$x^2 - qy^2 = p. \tag{2.2}$$

Para obtener condiciones que garanticen la solución de esta ecuación, hay dos valores de n que pueden considerarse:

1. $n = p$. Si reducimos (2.2) módulo p obtenemos $x^2 \equiv qy^2 \pmod{p}$. Luego, si $y \equiv 0 \pmod{p}$, entonces también $x \equiv 0 \pmod{p}$. Así, $p^2|x^2$ y $p^2|y^2$ y por tanto, $p^2|(x^2 - qy^2) = p$, lo cual es imposible. De esta manera, necesariamente $y \not\equiv 0 \pmod{p}$ y podemos dividir por y para obtener
$$\left(\frac{x}{y}\right)^2 \equiv q \pmod{p}.$$
Luego,

   > La ecuación $x^2 - qy^2 = p$ solamente tiene solución si q es un cuadrado módulo p.

2. $n = q$. Si reducimos módulo q inmediatamente tenemos que $x^2 \equiv p \pmod{q}$. Por lo tanto,

   > La ecuación $x^2 - qy^2 = p$ solamente tiene solución si p es un cuadrado módulo q.

Ahora, tomemos casos particulares para p y q.

Ejemplo 2.1.1. Sea $p = 3$ y $q = 5$. Entonces, como los cuadrados módulo 5 son 1 y 4, se sigue que p no es un cuadrado módulo q. Asimismo, 1 es el único cuadrado módulo 3, mientras que $5 \equiv -1 \pmod{3}$, por lo que q tampoco es un cuadrado módulo p.

Ejemplo 2.1.2. Sea $p = 11$ y $q = 5$. Como $11 \equiv 1 \pmod{5}$, p es un cuadrado módulo q. De la misma manera, $7^2 \equiv 5 \pmod{11}$, por lo que q es un cuadrado módulo p.

Ejemplo 2.1.3. Sea $p = 19$ y $q = 7$. Los cuadrados módulo 7 son $1, 2$ y 4, por lo que $19 \equiv 5 \pmod{7}$ no es un cuadrado. Sin embargo, $8^2 \equiv 7 \pmod{19}$ y por lo tanto, q es un cuadrado módulo p.

Los ejemplos anteriores muestran que hay tres posibilidades:

1. p es congruente con un número cuadrado módulo q y q es congruente con un cuadrado módulo p.

2. p no es congruente con un cuadrado módulo q y q no es congruente con un cuadrado módulo p.

3. p no es congruente con un cuadrado módulo q y q tampoco es congruente con un cuadrado módulo p.

De hecho, con un poco más de ejemplos puede llegarse al punto medular de este trabajo, es decir, a la Ley de Reciprocidad Cuadrática, la cual enunciamos a continuación.

Teorema 2.1.4. (La Ley de Reciprocidad Cuadrática) Sean p y q primos impares distintos. Entonces

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

Mediante este resultado es posible determinar cuándo, dados dos primos impares p y q, uno de ellos, digamos p, es residuo cuadrático de q, una vez que sabemos cuándo q es residuo cuadrático de p.

El estudio que de este teorema se ha hecho a lo largo del tiempo, nos lleva a efectuar un análisis de las diferentes demostraciones que se conocen, sin embargo, no resulta fácil elegir una demostración concreta de este resultado. Algunas de ellas son más conceptuales que otras, pero requiren algunas herramientas más sofisticadas. Otras son más accesibles, pero más largas y técnicas. Ante tal diversidad, decidimos incluir algunas de ellas en el presente capítulo.

2.2. Demostración 1

Iniciamos la discusión presentando una prueba debida a Eisenstein, para lo cual se requieren algunos términos que presentamos en seguida.

Definición 2.2.1. Un número complejo ζ es llamado *raíz n-ésima de la unidad* si $\zeta^n = 1$ para algún entero $n > 0$. Si n es el entero más pequeño con esta propiedad, entonces ζ es una *raíz n-ésima primitiva* de la unidad.

Las n-ésimas raíces de la unidad serán denotadas por: $1, e^{2\pi i/n}, e^{2(2\pi i/n)}, \ldots,$ $e^{(n-1)(2\pi i/n)}$. De entre ellas, las raíces primitivas de la unidad son $e^{(2\pi i/n)k}$, donde $\text{mcd}(k, n) = 1$. Asimismo, si ζ es una raíz n-ésima de la unidad y $m \equiv l \pmod{n}$, entonces $\zeta^m = \zeta^l$; recíprocamente, también se cumple que

si ζ es una n-ésima raíz primitiva de la unidad y $\zeta^m = \zeta^l$, entonces $m \equiv l$ (mód n).

Ahora, consideremos la función $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i\,\mathrm{sen}(2\pi z)$. Esta función satisface $f(z+1) = f(z)$ y $f(-z) = -f(z)$. Igualmente, sus únicos ceros reales son aquellos de la forma $z = n/2,\ n \in \mathbb{Z}$.

Lema 2.2.2. Si $n > 0$ es impar, entonces

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

donde $\zeta = e^{2\pi i/n}$.

Demostración. Los números $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ son todos raíces del polinomio $z^n = 1$. Como hay n de ellos y todos son distintos, entonces

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

Sea $z = x/y$ y multipliquemos ambos lados por y^n. Entonces,

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

Como n es impar y k toma valores sobre todo un sistema completo de residuos módulo n, lo mismo hace $-2k$. Así,

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1}(x - \zeta^{-2k} y) \\ &= \zeta^{-(1+2+\cdots+n-1)} \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y) \\ &= \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y), \end{aligned}$$

pues $1 + 2 + \cdots + (n-1) = n(n-1)/2$, que es divisible por n. ■

Proposición 2.2.3. Si n es un entero positivo impar y $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, entonces

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

Demostración. En el lema anterior, sustituyamos $x = e^{2\pi iz}$ y $y = e^{-2\pi iz}$; entonces

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

Notemos que

$$f\left(z + \frac{k}{n}\right) = f\left(z + \frac{k}{n} - 1\right) = f\left(z - \frac{n-k}{n}\right).$$

Luego,

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

Como k toma valores desde $(n+1)/2$ a $n-1$, entonces $n-k$ irá de $(n-1)/2$ a 1. Así,

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

■

Proposición 2.2.4. Si p es un primo impar, $a \in \mathbb{Z}$, y $p \nmid a$, entonces

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

Demostración. Como en la demostración del lema de Gauss, sea $\pm m_l$ el mínimo residuo de la, donde m_l es positivo, esto es,

$$la \equiv \pm m_l \pmod{p}, \qquad 1 \leq m_l \leq (p-1)/2.$$

Entonces la/p y $\pm m_l/p$ difieren por un entero, por lo que, por las propiedades ya mencionadas de f,

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

Aplicando el lema de Gauss, tenemos

$$\begin{aligned}\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) &= \prod_{l=1}^{(p-1)/2} \left(\pm f\left(\frac{m_l}{p}\right)\right) \\ &= (-1)^{\mu} \prod_{l=1}^{(p-1)/2} f\left(\frac{m_l}{p}\right) \\ &= \left(\frac{a}{p}\right)_{\mathcal{L}} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).\end{aligned}$$

■

Demostración. (Teorema 2.1.4). Por la Proposición 2.2.4,

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

Por la Proposición 2.2.3,

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

Usando estas dos últimas ecuaciones tenemos

$$\begin{aligned}\left(\frac{q}{p}\right)_{\mathcal{L}} &= \frac{\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right)}{\prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)} \\ &= \prod_{l=1}^{(p-1)/2} \frac{f\left(\frac{lq}{p}\right)}{f\left(\frac{l}{p}\right)} \\ &= \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).\end{aligned}$$

Análogamente,

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

Como $f\left(\frac{m}{q}-\frac{l}{p}\right) = -f\left(\frac{l}{p}-\frac{m}{q}\right)$, entonces

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

y por tanto, al multiplicar la cuación anterior en ambos lados por $\left(\frac{q}{p}\right)_{\mathcal{L}}$, y recordando que $\left(\frac{q}{p}\right)_{\mathcal{L}}^2 = 1$, tenemos que

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

■

2.3. Demostración 2

Durante toda esta sección, ζ será utilizada para denotar a $e^{2\pi i/p}$, la p-ésima raíz primitiva de la unidad.

Lema 2.3.1. Sea p un primo impar, entonces

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & \text{si } a \equiv 0 \pmod{p} \\ 0 & \text{de otro modo.} \end{cases}$$

Demostración. Si $a \equiv 0 \pmod{p}$, entonces $\zeta^a = 1$, y por lo tanto, $\sum_{t=0}^{p-1} \zeta^{at} = p$.

Si $a \not\equiv 0 \pmod{p}$, entonces $\zeta^a \neq 1$ y $\sum_{t=0}^{p-1} \zeta^{at} = \frac{(\zeta^{ap}-1)}{(\zeta^a-1)} = 0$. ■

Corolario 2.3.2.

$$p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x,y),$$

donde

$$\delta(x,y) = \begin{cases} 1 & \text{si } x \equiv y \pmod{p}, \text{ y} \\ 0 & \text{si } x \not\equiv y \pmod{p}. \end{cases}$$

Demostración. La prueba es inmediata del lema anterior. ■

Lema 2.3.3.

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right)_{\mathcal{L}} = 0.$$

Demostración. Por definición, $\left(\frac{0}{p}\right)_{\mathcal{L}} = 0$. De los $p-1$ sumandos restantes, la mitad son residuos cuadráticos y la otra no. ■

Definición 2.3.4. La suma cuadrática de Gauss se define como

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)_{\mathcal{L}} \zeta^{at}.$$

Proposición 2.3.5.

$$g_a = \left(\frac{a}{p}\right)_{\mathcal{L}} g_1.$$

Demostración. Si $a \equiv 0 \pmod{p}$, entonces $\zeta^{at} = 1$ para todo t, y $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)_{\mathcal{L}} = 0$ por el lema anterior, lo cual nos da el resultado cuando $a \equiv 0 \pmod{p}$.

Ahora supongamos que $a \not\equiv 0 \pmod{p}$. Entonces,

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

Hemos usado el hecho de que at corre sobre un sistema completo de residuos mód p cuando t lo hace y que $\left(\frac{x}{p}\right)_{\mathcal{L}}$ y ζ^x dependen solamente de las clases

residuales mód p.

Como $\left(\frac{a}{p}\right)_{\mathcal{L}}^2 = 1$ cuando $a \not\equiv 0 \pmod{p}$, nuestro resultado se sigue multiplicando la ecuación $\left(\frac{a}{p}\right)_{\mathcal{L}} g_a = g_1$ por $\left(\frac{a}{p}\right)_{\mathcal{L}}$ en ambos lados. ■

De ahora en adelante, denotaremos g_1 por g. Se sigue de la proposición anterior que $g_a^2 = g^2$ si $a \not\equiv 0 \pmod{p}$.

Proposición 2.3.6.

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

Demostración. La idea de la prueba es evaluar la suma $\sum_{a=0}^{p-1} g_a g_{-a}$ de dos formas distintas.

Si $a \not\equiv 0 \pmod{p}$, entonces por la proposición anterior,

$$g_a g_{-a} = \left(\frac{a}{p}\right)_{\mathcal{L}} \left(\frac{-a}{p}\right)_{\mathcal{L}} g^2 = \left(\frac{-1}{p}\right)_{\mathcal{L}} \left(\frac{a^2}{p}\right)_{\mathcal{L}} = \left(\frac{-1}{p}\right)_{\mathcal{L}} g^2.$$

Se sigue que

$$\sum_{a=0}^{p-1} g_a g_{-a} = \left(\frac{-1}{p}\right)_{\mathcal{L}} (p-1) g^2.$$

Ahora, notemos que

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

Sumando ambos lados sobre a desde 0 hasta $p-1$ y usando el Corolario 2.3.2 tenemos,

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right)_{\mathcal{L}} \left(\frac{y}{p}\right)_{\mathcal{L}} \delta(x,y) p = (p-1)p.$$

Juntando estos resultados obtenemos

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

Así,

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

■

Sea $p^* = (-1)^{(p-1)/2}p$, entonces $g^2 = p^*$. Sea $q \neq p$ otro primo impar. Procedemos a probar la Ley de Reciprocidad Cuadrática trabajando con congruencias módulo q en el anillo formado por el conjunto de enteros algebraicos. Observamos lo siguiente,

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \left(\frac{p^*}{q}\right)_{\mathcal{L}} \pmod{q}.$$

Así,

$$g^q \equiv \left(\frac{p^*}{q}\right)_{\mathcal{L}} g \pmod{q}.$$

Usando el hecho de que dados dos enteros algebraicos cualesquiera ω_1, ω_2 se cumple que $(\omega_1 + \omega_2)^q \equiv \omega_1^q + \omega_2^q \pmod{q}$, se sigue que

$$g^q = \left(\sum_{t=0}^{p-1} \left(\frac{t}{p}\right)_{\mathcal{L}} \zeta^t\right)^q \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)_{\mathcal{L}}^q \zeta^{qt} \equiv g_q \pmod{q}.$$

De lo anterior, $g^q \equiv g_q \equiv \left(\frac{q}{p}\right)_{\mathcal{L}} g \pmod{q}$, y por lo tanto,

$$\left(\frac{q}{p}\right)_{\mathcal{L}} g \equiv \left(\frac{p^*}{q}\right)_{\mathcal{L}} g \pmod{q}.$$

Multiplicando ambos lados por g y usando $g^2 = p^*$, obtenemos

$$\left(\frac{q}{p}\right)_{\mathcal{L}} p^* \equiv \left(\frac{p^*}{q}\right)_{\mathcal{L}} p^* \pmod{q},$$

lo cual implica que

$$\left(\frac{q}{p}\right)_{\mathcal{L}} \equiv \left(\frac{p^*}{q}\right)_{\mathcal{L}} \pmod{q},$$

y finalmente

$$\left(\frac{q}{p}\right)_{\mathcal{L}} = \left(\frac{p^*}{q}\right)_{\mathcal{L}}.$$

Para ver que este resultado es lo que queremos, basta notar que

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

2.4. Demostración 3

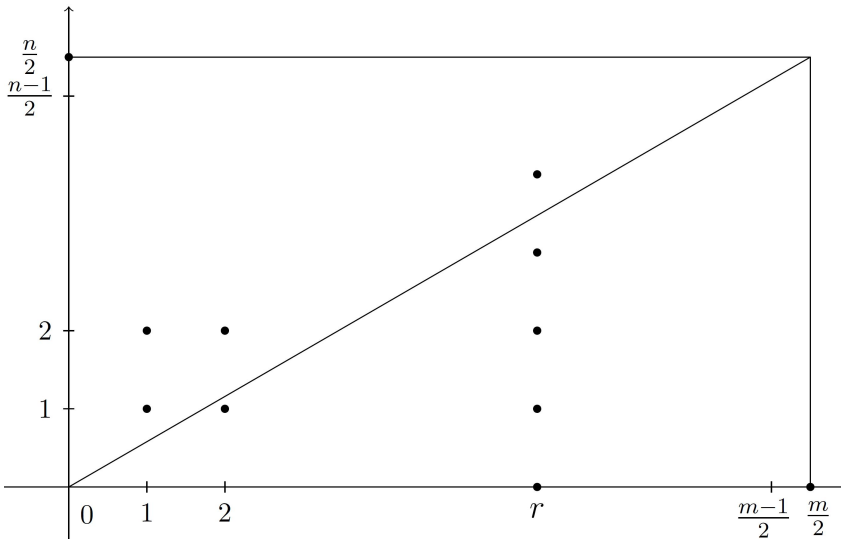
La siguiente demostración es una versión de la tercera prueba de Gauss, debida en parte a Eisenstein, quien demuestra el primero de los lemas que presentamos a continuación.

Lema 2.4.1. Sean m y n enteros coprimos impares, $m \neq 1, n \neq 1$, y sea $m' = \frac{m-1}{2}, n' = \frac{n-1}{2}$, entonces

$$\sum_{r=1}^{m'} \left[\frac{nr}{m}\right] + \sum_{r=1}^{n'} \left[\frac{mr}{n}\right] = m'n',$$

donde $[\bullet]$ denota al entero más grande que no es mayor que $\bullet$.

Demostración. El resultado es geométricamente evidente al darnos cuenta que la suma de la izquierda cuenta los puntos con coordenadas enteras dentro del rectángulo de lados $\frac{m}{2}$ y $\frac{n}{2}$.



De hecho, no hay puntos con coordenadas enteras en la diagonal de este rectángulo. Las coordenads (s, t) de un punto en la diagonal satisfacen $\frac{s}{t} = \frac{m}{n}$, con $s < m, t < n$, y $\frac{m}{n}$ en su forma reducida, pues $\text{mcd}(m, n) = 1$. Así, s y t no pueden ser ambos enteros. En el triángulo inferior del rectángulo, la vertical de abcisa r se encuentra con la diagonal en la ordenada $\frac{rn}{m}$. De esta manera, en dicha vertical hay exactamente $\left[\frac{rn}{m}\right]$ puntos con coordenadas enteras. Si hacemos $r = 1, 2, \ldots, m'$, obtenemos en total $\sum_{r=1}^{m'} \left[\frac{rn}{m}\right]$ puntos con coordenadas enteras dentro del triángulo inferior. Similarmente, hay

$\sum_{r=1}^{n'} \left[\frac{mr}{n}\right]$ puntos con coordenadas enteras en el triángulo superior, mientras que el número total de puntos con coordenas enteras dentro del rectángulo es claramente $m' \cdot n'$. ■

Lema 2.4.2. Sea a un número entero y p un primo impar. Si $p \nmid a$, $p' = \frac{p-1}{2}$ y μ está definida como en el Lema de Gauss, entonces

$$\sum_{m=1}^{p'} \left[\frac{ma}{p}\right] + \frac{1}{8}(a-1)(p^2-1) \equiv \mu \pmod 2.$$

Demostración. Consideremos el conjunto $S = \{r\}$ de residuos mínimos no negativos módulo p, $ma \equiv r \pmod p$, donde $m = 1, 2, \ldots, p$. Dado m, el correspondiente r es la diferencia

$$ma - p\left[\frac{ma}{p}\right].$$

Sumando sobre todos los m tenemos,

$$a\sum_{m=1}^{p'} m - p\sum_{m=1}^{p'} \left[\frac{ma}{p}\right] = \sum_{m=1}^{p'} r;$$

es decir,

$$a\sum_{m=1}^{p'} m = p\sum_{m=1}^{p'} \left[\frac{ma}{p}\right] + \sum_{m=1}^{p'} r. \tag{2.3}$$

Distinguimos ahora entre los $r's$ menores que $\frac{p}{2}$, denotados por $t_1, t_2 \ldots, t_k$, y aquéllos mayores que $\frac{p}{2}$, denotados por $s_1, s_2, \ldots, s_\mu$, pues el número de s_i's es precisamente μ del lema de Gauss. Asimismo, recordemos de la demostración de dicho lema que los conjuntos $\{p - s_i, t_i\}$ y $\{1, 2, \ldots p'\}$ coinciden en algún orden. De esta manera,

$$\begin{aligned} \sum_{i=1}^{\mu}(p - s_i) + \sum_{i=1}^{k} t_i = &\quad \mu p - \textstyle\sum_{i=1}^{\mu} s_i + \sum_{i=1}^{k} t_i \\ = &\quad \textstyle\sum_{m=1}^{p'} m = \frac{\frac{p-1}{2}\cdot\frac{p+1}{2}}{2} = \frac{p^2-1}{8}. \end{aligned} \tag{2.4}$$

Luego, podemos reescribir a (2.3) y (2.4) como sigue,

$$\begin{aligned} a \cdot \frac{p^2-1}{8} = &\quad p\textstyle\sum_{m=1}^{p'} \left[\frac{ma}{p}\right] + \sum_{i=1}^{\mu} s_i + \sum_{i=1}^{k} t_i \\ -\frac{p^2-1}{8} = &\quad -\mu p + \textstyle\sum_{i=1}^{mu} s_i - \sum_{i=1}^{k} t_i. \end{aligned}$$

Sumando las dos ecuaciones anteriores nos queda,

$$(a-1)\cdot\frac{p^2-1}{8} = p\left(\sum_{m=1}^{p'}\left[\frac{ma}{p}\right]-\mu\right)+2\sum_{i=1}^{\mu}s_i.$$

Módulo 2, el lado derecho es congruente con

$$p\left(\sum_{m=1}^{p'}\left[\frac{ma}{p}\right]-\mu\right)\equiv\sum_{m=1}^{p'}\left[\frac{ma}{p}\right]-\mu\equiv\mu-\sum_{m=1}^{p'}\left[\frac{ma}{p}\right],$$

pues $p\equiv 1 \pmod 2$, y el lema queda demostrado. ■

Procedemos ahora a demostrar la Ley de Reciprocidad Cuadrática.

Demostración. (Del Teorema 2.1.4) Por el Lema de Gauss, sabemos cómo definir enteros m y n de manera que $\left(\frac{p}{q}\right)_{\mathcal{L}}=(-1)^n$ y $\left(\frac{q}{p}\right)_{\mathcal{L}}=(-1)^m$, por lo que

$$\left(\frac{p}{q}\right)_{\mathcal{L}}\left(\frac{q}{p}\right)_{\mathcal{L}}=(-1)^{n+m}.$$

Por el Lema 2.4.2,

$$\begin{aligned} n &\equiv \textstyle\sum_{r=1}^{p'}\left[\frac{rq}{p}\right]+\frac{(q-1)(p^2-1)}{8} \\ &\equiv \textstyle\sum_{r=1}^{p'}\left[\frac{rq}{p}\right] \pmod 2, \end{aligned}$$

pues p y q son impares. Análogamente,

$$m\equiv\sum_{r=1}^{q'}\left[\frac{rp}{q}\right] \pmod 2,$$

donde $q'=\frac{q-1}{2}$. De esta manera,

$$m+n\equiv\sum_{r=1}^{q'}\left[\frac{rp}{q}\right]+\sum_{r=1}^{p'}\left[\frac{rq}{p}\right] \pmod 2.$$

Por el Lema 2.4.1, $m+n\equiv p'\cdot q' \pmod 2$, por lo que el Teorema 2.1.4 queda demostrado. ■

2.5. Demostración 4

Un aspecto de gran importancia en las ideas y resultados de las matemáticas, es la forma en que estructuran o dan origen a teorías completas. La Ley de Reciprocidad Cuadrática es uno de esos resultados que ha dado origen al gran desarrollo de la teoría algebraica de números; precisamente en el proceso de su generalización tuvo lugar el estudio del anillo de enteros del campo ciclotómico $\mathbb{Q}(\zeta)$, lo que a su vez motivó el estudio de los anillos de enteros, trabajo desarrollado por Kummer y Dedekind, entre otros ([12, pag. ix]). Al respecto, Hecke citado en [12, pag. v], argumenta:

> La teoría moderna de números se remonta al descubrimiento de la ley de reciprocidad. Pero su forma aún pertenece a la teoría de los números racionales, pues ésta puede ser formulada enteramente como una relación simple entre números racionales; sin embargo, su contenido apunta más allá de los números racionales. [...] El desarrollo de la teoría algebraica de números ha demostrado de hecho, que el contenido de la Ley de Reciprocidad Cuadrática solamente resulta entendible si uno pasa a números algebraicos generales y que una demostración apropiada a la naturaleza del problema puede ser mejor desarrollada con esos métodos superiores.

Tomando esto como referente y después de haber presentado tres pruebas de la Ley de Reciprocidad Cuadrática, que siguen más o menos las ideas originales de Gauss, Eisenstein y otros, presentamos una cuarta prueba que tiene por finalidad ilustrar la forma en que se usan varias ideas centrales en la teoría de números algebraicos, que permiten identificar la relación que hay entre la Ley de Reciprocidad Cuadrática y su conexión con varias ideas en teoría algebraica de números.

La demostración que presentamos aparece en [9, pags. 59-61]; algunos de los detalles no los presentamos para evitar hacer la exposición más extensa; estos pueden encontrarse en la referencia citada.

Definición 2.5.1. Si ζ es una raíz n-ésima primitiva de la unidad, llamamos a $\mathbb{Q}(\zeta)$ el *n-ésimo campo ciclotómico*, o simplemente *campo ciclotómico*.

Teorema 2.5.2. Sea p un primo impar. El p-ésimo campo ciclotómico contiene una única extensión cuadrática de $\mathbb{Q}$, que es $\mathbb{Q}(\sqrt{\varepsilon(p)p})$, donde $\varepsilon(p) = (-1)^{\frac{p-1}{2}}$.

Lema 2.5.3. Sea a un entero libre de cuadrado y q un primo impar. Entonces q se puede escribir como producto de dos ideales primos distintos en $\mathbb{Q}(\sqrt{a})$ si y sólo si q no divide a a y $\left(\frac{a}{q}\right)_{\mathcal{L}} = 1$.

Lema 2.5.4. Sean p y q primos impares distintos. Entonces q se factoriza como producto de dos primos en $\mathbb{Q}(\sqrt{\varepsilon(p)p})$ si y sólo si $\left(\frac{q}{p}\right)_{\mathcal{L}} = 1$.

Procedemos ahora a demostrar la Ley de Reciprocidad Cuadrática:

Por el Lema 2.5.4, $\left(\frac{q}{p}\right)_{\mathcal{L}} = 1$ si y sólo si q se factoriza como producto de dos primos en $\mathbb{Q}(\sqrt{\varepsilon(p)p})$, y esto sucede si y sólo si $\left(\frac{\varepsilon(p)p}{q}\right)_{\mathcal{L}} = 1$, por el Lema 2.5.3. Por otro lado, recordando que $\varepsilon(p) = (-1)^{\frac{p-1}{2}}$, tenemos,

$$\begin{aligned}\left(\frac{\varepsilon(p)p}{q}\right)_{\mathcal{L}} &= \left(\frac{\varepsilon(p)}{q}\right)_{\mathcal{L}} \left(\frac{p}{q}\right)_{\mathcal{L}} \\ &= \left(\frac{-1}{q}\right)_{\mathcal{L}}^{\frac{p-1}{2}} \left(\frac{p}{q}\right)_{\mathcal{L}} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)_{\mathcal{L}}.\end{aligned}$$

Por lo anterior,

$$\left(\frac{q}{p}\right)_{\mathcal{L}} = 1 \Leftrightarrow (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \left(\frac{p}{q}\right)_{\mathcal{L}} = 1.$$

Es importante señalar que la Ley de Reciprocidad Cuadrática tiene varias aplicaciones. Por mencionar algunas de ellas están la validez de la llamada Prueba de Primalidad de Pepin para números de Fermat, y los teoremas, enunciados por éste último, para un número primo impar p, según los cuales:

$$\begin{array}{lllll} p = x^2 + y^2 & x, y \in \mathbb{Z} & \Leftrightarrow & p \equiv 1 \pmod 4 \\ p = x^2 + 2y^2 & x, y \in \mathbb{Z} & \Leftrightarrow & p \equiv 1, 3 \pmod 8 \\ p = x^2 + 3y^2 & x, y \in \mathbb{Z} & \Leftrightarrow & p = 3 \text{ ó } p \equiv 1 \pmod 3. \end{array}$$

2.6. Leyes suplementarias

Aunque el Teorema 2.1.4 es reconocido mayor y comúnmente como la Ley de Reciprocidad Cuadrática, algunos autores incluyen la evaluación de $\left(\frac{-1}{p}\right)_{\mathcal{L}}$ y $\left(\frac{2}{p}\right)_{\mathcal{L}}$. Estos casos se conocen como la $1a.$ y $2da.$ leyes suplementarias, respectivamente, y a continuación presentamos su demostración.

Proposición 2.6.1 (1a. Ley Suplementaria)**.** Sea p un número primo impar. Entonces

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

Demostración. Por el Criterio de Euler,

$$\left(\frac{-1}{p}\right)_{\mathcal{L}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Como los únicos valores posibles de $\left(\frac{-1}{p}\right)_{\mathcal{L}}$ y $(-1)^{\frac{p-1}{2}}$ son 1 y -1, y p es impar, entonces,

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

■

Proposición 2.6.2 (2da. Ley Suplementaria)**.** Sea p un número primo impar. Entonces

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

Demostración. En esta demostración haremos uso de la notación y resultados de la Demostración 4 presentada en la sección anterior. Primero, observamos que aplicando el lema 2.5.4, se sigue que $\left(\frac{2}{p}\right)_{\mathcal{L}} = 1$ si y sólo si el primo 2 tiene dos divisores primos distintos en $E = \mathbb{Q}(\sqrt{\varepsilon(p)p})$.

Pero el siguiente paso que sería análogo a la Demostración 4, no se puede aplicar para $p = 2$, pues en este caso la factorización de $2R_E$, donde R_E representa a los enteros algebraicos en E, no está determinada por la factorización del polinomio $x^2 - \varepsilon(p)p$. En su lugar, tenemos $R_E = \mathbb{Z}[\omega]$, con

$$\omega = \frac{1 + \sqrt{\varepsilon(p)p}}{2},$$

y cuyo polinomio mínimo es

$$g(x) = x^2 - x + \frac{1 - \varepsilon(p)p}{4}.$$

De esta manera, $2R_E$ tendrá dos factores primos si y sólo si $g(x)$ se escribe como producto de dos factores de grado 1 módulo 2. Ahora, $g(0) \equiv g(1) \equiv 0 \pmod{2}$ se cumple si y sólo si $\frac{1-\varepsilon(p)p}{4}$ es par, y esto ocurre si y sólo si

$1 + 8t = \varepsilon(p)p$; es decir, $(-1)^{\frac{p-1}{2}}p = 8t + 1$.

Para concluir la demostración, probaremos lo siguiente:

$$\frac{p^2 - 1}{2} = 2l \Leftrightarrow (-1)^{\frac{p-1}{2}}p = 8t + 1.$$

Veamos, si $(-1)^{\frac{p-1}{2}}p = 8t + 1$, elevando al cuadrado tenemos

$$p^2 = (8t + 1)^2,$$

pues p es impar. Luego, $p^2 = 64t^2 + 16t + 1$, y entonces $\frac{p^2-1}{8} = 8t^2 + 2t = 2l$, para $l = 4t^2 + t$.

Para demostrar la otra dirección, observamos que p es de la forma $8m+r$, para $r = 1, 3, 5$,ó 7. Si $p = 8m + 1$, entonces $(-1)^{\frac{p-1}{2}} = 1$, por lo que $(-1)^{\frac{p-1}{2}}p = 8m + 1$. Ahora, $p \neq 8m + 3$, pues de lo contrario,

$$\begin{aligned} p^2 &= (2(4m + 1) + 1)^2 \\ &= 4(4m + 1)^2 + 4(4m + 1) + 1. \end{aligned}$$

Entonces, $p^2 - 1 = 4(4m+1)(4m+2) = 8(4m+1)(2m+1)$; luego, $\frac{p^2-1}{8}$ sería impar, lo cual es imposible. El caso $p = 8m + 5$ es análogo al anterior y si $p = 8m + 7$, entonces $(-1)^{\frac{p-1}{2}} = -1$ y $-p \equiv 1 \pmod 8$, por lo cual

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

■

Capítulo 3

Leyes de Reciprocidad Superiores

En el capítulo anterior vimos que la Ley de Reciprocidad Cuadrática responde a la pregunta, ¿para qué primos p la congruencia $x^2 \equiv q \pmod{p}$ tiene solución? Si hacemos la pregunta para congruencias $x^n \equiv q \pmod{p}$, llegamos a lo que se conoce como Leyes de Reciprocidad Superiores. En particular, cuando $n = 3$ y 4 las llamamos leyes de reciprocidad cúbica y bicuadrática, respectivamente.

Aunque Gauss descubrió y reformuló la Ley de Reciprocidad Bicuadrática, no logró demostrarla completamente. Las primeras pruebas completas publicadas de las leyes de reciprocidad cúbica y bicuadrática se deben a Eisenstein.

En este capítulo enunciaremos la ley de reciprocidad cúbica; una demostración puede encontrarse en [8, pags. 115-118]. Asimismo, se presentan algunas ideas de la forma general de las leyes de reciprocidad. Al respecto, Lemmermeyer considera que "La historia de las leyes de reciprocidad es una historia de la teoría de números algebraicos" ([12, pag. v]).

3.1. La Ley de Reciprocidad Cúbica

Como hemos mencionado, las leyes de reciprocidad superiores surgen al intentar resolver la congruencia $x^n \equiv q \pmod{p}$. El estudio de n's cada vez más grandes llevó a Gauss a formular las leyes de reciprocidad cúbica y bicuadrática en 1814, pero no fue sino hasta 1844 que Eisenstein publicó la primera demostración de estos teoremas. En esta sección presentamos

un bosquejo sobre la formulación de la Ley de Reciprocidad Cúbica, y los detalles de su demostración pueden encontrarse en [8, pag. 115].

Consideremos la ecuación $x^3 = 1$. Como

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

las raíces de la ecuación son 1, $\dfrac{-1 \pm \sqrt{-3}}{2}$. Sea $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, y consideremos el conjunto $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$. $\mathbb{Z}[\omega]$ es cerrado bajo la suma y la resta; más aún,

$$\begin{aligned}(a + b\omega)(c + d\omega) &= ac + (ad + bc)\omega + bd\omega^2 \\ &= (ac - bd) + (ad + bc - bd)\omega,\end{aligned}$$

pues $\omega^2 = -(1 + \omega)$. Así, $\mathbb{Z}[\omega]$ es un anillo, y como es subconjunto de los números complejos, es un dominio entero.

Observamos también que $\mathbb{Z}[\omega]$ es cerrado bajo la conjugación compleja. De hecho, como $\overline{\sqrt{-3}} = \overline{\sqrt{3}i} = -\sqrt{3}i = -\sqrt{-3}$, vemos que $\overline{\omega} = \omega^2$. Luego, si $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, entonces $\overline{\alpha} = a + b\overline{\omega} = a + b\omega^2 = (a - b) - b\omega \in \mathbb{Z}[\omega]$.

Otra observación que se puede verificar es que $\mathbb{Z}[\omega]$ es un dominio euclidiano y de factorización única ([8, pag. 13]).

Definición 3.1.1. Si $\alpha = a + b\omega \in \mathbb{Z}[\omega]$. Definimos la norma de α, denotada $N\alpha$, como $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$.

Proposición 3.1.2. Si $\alpha = a + b\omega, \beta = c + d\omega \in \mathbb{Z}[\omega]$, entonces

$$N\alpha\beta = N\alpha N\beta.$$

Demostración. Veamos, $\alpha\beta = (a + b\omega)(c + d\omega) = (ac - bd) + (ad + bc - bd)\omega$, por lo que

$$\begin{aligned}N\alpha\beta &= (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 \\ &= a^2c^2 + acbd + b^2d^2 - a^2cd - abc^2 - abd^2 - b^2cd + a^2d^2 + b^2c^2 \\ &= a^2(c^2 - cd + d^2) - ab(c^2 - cd + d^2) + b^2(c^2 - cd + d^2) \\ &= (a^2 - ab + b^2)(c^2 - cd + d^2) \\ &= N\alpha N\beta.\end{aligned}$$

■

Nuestro propósito por el momento será descubrir las unidades y los elementos primos (o irreducibles) en $\mathbb{Z}[\omega]$.

Proposición 3.1.3. $\alpha \in \mathbb{Z}[\omega]$ es una unidad si y sólo si $N\alpha = 1$. Las unidades en $\mathbb{Z}[\omega]$ son $1, -1, \omega, -\omega, \omega^2$ y $-\omega^2$.

Demostración. Si $N\alpha = 1$, $\alpha\overline{\alpha} = 1$, lo cual implica que α es una unidad, pues $\overline{\alpha} \in \mathbb{Z}[\omega]$.

Si α es una unidad, entonces existe $\beta \in \mathbb{Z}[\omega]$ tal que $\alpha\beta = 1$. Así, $N\alpha N\beta = 1$. Como $N\alpha$ y $N\beta$ son enteros positivos, esto implica que $N\alpha = 1$.

Ahora supongamos que $\alpha = a + b\omega$ es una unidad. Entonces $N\alpha = 1$ y por tanto, $1 = a^2 - ab + b^2$ ó $4 = (2a - b)^2 + 3b^2$. Hay dos posibilidades:

a) $2a - b = \pm 1$, $b = \pm 1$,

b) $2a - b = \pm 2$, $b = 0$.

Resolviendo estos seis pares de ecuaciones llegamos al resultado $1, -1, \omega, -\omega$, $-1 - \omega$ y $1 + \omega$. Como $\omega^2 + \omega + 1 = 0$, los últimos dos elementos son ω^2 y $-\omega^2$. ■

Para encontrar los primos de $\mathbb{Z}[\omega]$ es importante notar que primos en $\mathbb{Z}$ no necesariamente son primos en $\mathbb{Z}[\omega]$. Por ejemplo, $7 = (3 + \omega)(2 - \omega)$. Por esta razón, hablaremos de primos en $\mathbb{Z}$ como *primos racionales* y nos referiremos a los primos en $\mathbb{Z}[\omega]$ simplemente como primos.

Proposición 3.1.4. Si π es un primo en $\mathbb{Z}[\omega]$, entonces existe un primo racional p tal que $N\pi = p$ ó p^2. En el primer caso, π no es asociado de algún primo racional; en el segundo caso, π es asociado de p.

Demostración. Sabemos que $N\pi = n$ para algún $n > 1$; esto es, $\pi\overline{\pi} = n$, y n es producto de primos racionales, por lo que $\pi | p$ para algún primo racional p. Si $p = \pi\gamma$, $\gamma \in \mathbb{Z}[\omega]$ entonces

$$N\pi N\gamma = (\pi\overline{\pi})(\gamma\overline{\gamma}) = (\pi\gamma)(\overline{\pi\gamma}) = Np = p\overline{p} = p^2.$$

Así, ó $N\pi = p^2$ y $N\gamma = 1$, ó $N\pi = p$. En el primer caso, γ es una unidad y por lo tanto π está asociado con p, pues $p = \pi\gamma$. En el segundo caso, si $\pi = uq$, donde u es una unidad y q un primo racional, entonces $p = N\pi = NuNq = q^2$, lo cual es imposible. Así, π no es asociado de ningún primo racional. ■

Proposición 3.1.5. Si $\pi \in \mathbb{Z}[\omega]$ es tal que $N\pi = p$, p primo racional, entonces π es primo en $\mathbb{Z}[\omega]$.

Demostración. Supongamos que π no es primo en $\mathbb{Z}[\omega]$; entonces $\pi = \rho\gamma$, donde $N\rho, N\gamma > 1$. Así, $p = N\pi = N\rho N\gamma$, lo cual no puede ser pues p es primo en $\mathbb{Z}$. Entonces π es primo en $\mathbb{Z}[\omega]$. ■

El siguiente resultado clasifica los primos en $\mathbb{Z}[\omega]$

Proposición 3.1.6. Sean p y q primos racionales. Si $q \equiv 2 \pmod 3$, entonces q es primo en $\mathbb{Z}[\omega]$. Si $p \equiv 1 \pmod 3$, entonces $p = \pi\overline{\pi}$, donde π es primo en $\mathbb{Z}[\omega]$. Finalmente, $3 = -\omega^2(1-\omega)^2$, y $1-\omega$ es primo en $\mathbb{Z}[\omega]$.

Demostración. Supongamos que q no es primo en $\mathbb{Z}[\omega]$. Entonces $q = \pi\gamma$, con $N\pi > 1$, $N\gamma > 1$. Así,

$$Nq = q^2 = N\pi N\gamma \quad y \quad N\pi = q,$$

pues q es primo racional. Sea $\pi = a + b\omega$, entonces $q = a^2 - ab + b^2$, ó $4q = (2a-b)^2 + 3b^2$. Luego, $q \equiv (2a-b)^2 \pmod 3$.

Si $3 \nmid q$ tenemos que $q \equiv 1 \pmod 3$, pues 1 es el único cuadrado distinto de cero módulo 3, lo cual es una contradicción pues $q \equiv 2 \pmod 3$. Por lo tanto, si $q \equiv 2 \pmod 3$, entonces q es primo en $\mathbb{Z}[\omega]$.

Ahora, supongamos que $p \equiv 1 \pmod 3$. Por la Ley de Reciprocidad Cuadrática,

$$\begin{aligned}\left(\frac{-3}{p}\right)_{\mathcal{L}} &= \left(\frac{-1}{p}\right)_{\mathcal{L}}\left(\frac{3}{p}\right)_{\mathcal{L}} \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)_{\mathcal{L}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \\ &= \left(\frac{p}{3}\right)_{\mathcal{L}} = \left(\frac{1}{3}\right)_{\mathcal{L}} \\ &= 1.\end{aligned}$$

Luego, existe un entero a tal que $a^2 \equiv -3 \pmod p$, ó $pb = a^2 + 3$, para algún $b \in \mathbb{Z}$. Así,

$$p|(a+\sqrt{-3})(a-\sqrt{-3}) = (a+1+2\omega)(a-1-2\omega).$$

Si p fuera primo en $\mathbb{Z}[\omega]$, tendría que dividir a uno de los factores. De esta manera, $p = \pi\gamma$, donde π y γ no son unidades. Tomando normas, tenemos

que $Np = N\pi\gamma$; es decir, $p^2 = N\pi N\gamma$ y por tanto, $p = N\pi = \pi\overline{\pi}$.

Finalmente, para demostrar el último enunciado de la demostración, procedemos como sigue:

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) \\ &= (x-1)(x^2+x+1), \end{aligned}$$

entonces $x^2 + x + 1 = (x - \omega)(x - \omega^2)$. Haciendo $x = 1$ tenemos:

$$\begin{aligned} 3 &= (1-\omega)(1-\omega^2) \\ &= (1+\omega)(1-\omega)^2 \\ &= -\omega^2(1-\omega)^2, \end{aligned}$$

pues $\omega^2 + \omega + 1 = 0$. Tomando normas, tenemos que $9 = N(1-\omega)^2$, ya que $-\omega^2$ es unidad en $\mathbb{Z}[\omega]$. Luego $3 = N(1-\omega)$, por lo que, por la Proposición 3.1.5, $1 - \omega$ es primo. ■

Así, los primos en $\mathbb{Z}[\omega]$ consisten en aquellos primos racionales positivos que son congruentes con 2 módulo 3 y sus asociados, los primos complejos de la forma $a + b\omega$ cuya norma es un primo racional congruente con 1 módulo 3, y $1 - \omega$ y sus asociados.

Definición 3.1.7. Sea π un primo en $\mathbb{Z}[\omega]$ tal que $N\pi \neq 3$. Si $\alpha \in \mathbb{Z}[\omega]$, definimos el *caracter residual cúbico de* α módulo π como:

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{si } \alpha \equiv 0 \pmod{\pi} \\ \omega^r & \text{si } \alpha \not\equiv 0 \pmod{\pi} \text{ y } \alpha^{\frac{N\pi-1}{3}} \equiv \omega^r \pmod{\pi},\ r = 0,1,2. \end{cases}$$

Este caracter puede considerarse como el análogo del símbolo de Legendre definido para residuos cuadráticos. Algunas de sus propiedades son las siguientes: si $\alpha, \beta \in \mathbb{Z}[\omega]$, entonces

i) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^{\,2} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$,

ii) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$,

iii) $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$ si $\alpha \equiv \beta \pmod{\pi}$,

iv) $\left(\frac{-1}{\pi}\right)_3 = 1$,

v) $\left(\frac{\omega}{\pi}\right)_3 = \omega^{\frac{N\pi-1}{3}}$.

Definición 3.1.8.
Un primo π de $\mathbb{Z}[\omega]$ es *primario* si $\pi \equiv 2 \pmod 3$.

Una vez establecidos los preliminares anteriores, procedemos a enunciar la Ley de Reciprocidad Cúbica, demostrada en 1844 por Ferdinand Eisenstein.

Teorema 3.1.9 (Ley de Reciprocidad Cúbica)**.** Si π y λ son primos primarios de $\mathbb{Z}[\omega]$ entonces

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

Como es posible notar, este enunciado ha requerido de herramientas más sofisticadas que la Ley de Reciprocidad Cuadática, y las otras generalizaciones requieren de conceptos aún más avanzados. Por esta razón, nos limitamos a mencionar que, entre otras generalizaciones, se encuentran la ley de reciprocidad bicuadrática, la ley de reciprocida racional (propuesta por Eisenstein en 1850), y la generalización a extensiones abelianas finitas, debida a Artin.

3.2. Leyes generales de reciprocidad

Una vez enunciada y demostrada la Ley de Reciprocidad Cuadrática así como dado un bosquejo de la Ley de Reciprocidad Cúbica, presentamos a continuación un enfoque más general sobre ellas. En particular, discutiremos el *Problema general de Reciprocidad*, que envuelve a todas las leyes de reciprocidad, y para el cual requeriremos de la siguiente notación:

Sea $f(x)$ un polinomio mónico irreducible con coeficientes enteros, y p un primo impar. Reduciendo los coeficientes de $f(x)$ módulo p obtenemos un nuevo polinomio $f_p(x)$ con coeficientes en el campo $\mathbb{F}_p$. Aún cuando el polinomio original $f(x)$ es irreducible, puede ser que $f_p(x)$ sea reducible. Si esto ocurre y podemos factorizar el polinomio $f_p(x)$ sobre $\mathbb{F}_p$ como producto de factores lineales distintos, decimos que $f(x)$ *se factoriza completamente módulo* p, y definimos a $\mathbf{Fac}(\mathbf{f})$ como el conjunto de todos los números primos tales que $f(x)$ se factoriza completamente módulo p. De esta manera, el problema general de reciprocidad se enuncia como sigue:

Problema General de Reciprocidad. Dado $f(x)$ un polinomio mónico irreducible con coeficientes enteros y p un primo impar, describir la factorización de $f_p(x)$ como función de p. En particular, determinar los primos que pertenecen a $\mathbf{Fac}(\mathbf{f})$.

Al método para describir la factorización de $f_p(x)$, o en su caso, a la determinación de los primos en $\mathbf{Fac}(\mathbf{f})$ es a lo que llamaremos una *ley de reciprocidad*. Como veremos más adelante, para polinomios cuadráticos el problema se resuelve eficientemente y es precisamente la Ley de Reciprocidad Cuadrática la que nos da, valga la redundancia, una ley de reciprocidad. En general, para polinomios con grupo de Galois abeliano el problema general de reciprocidad tiene solución, pero muy poco se sabe de aquellos polinomios cuyo grupo de Galois no es abeliano ([15]).

3.2.1. Polinomios Cuadráticos.

Supongamos que $f(x)$ es un polinomio cuadrático irreducible con coeficientes enteros. Si p es un número primo impar, entonces hay tres posibilidades en la factorización de $f_p(x)$:

1. $f_p(x) = l(x)^2$, donde $l(x)$ es lineal.

2. $f_p(x) = l_1(x) \cdot l_2(x)$, con $l_1(x)$ y $l_2(x)$ dos polinomios lineales distintos. En este caso, $f(x)$ se factoriza completamente módulo p.

3. $f_p(x)$ es irreducible en $\mathbb{F}_p[x]$.

Para este caso cuadrático, trabajaremos con polinomios de la forma x^2-q, con q un número primo. Si $f(x) = x^2 - q$, entonces el caso 1 ocurre módulo p cuando $p = q$, y también cuando $p = 2$. Para distinguir los casos 2 y 3, necesitamos determinar cuándo q es un residuo cuadrático módulo p, pues si q es un residuo cuadrático y $q^2 \equiv a^2 \pmod{p}$, entonces

$$x^2 - q \equiv (x + a)(x - a) \pmod{p}.$$

Lo anterior nos indica que estamos en el caso 2, mientras que si q no es un residuo cuadrático, entonces caemos en el caso 3.

En términos del símbolo de Legendre y dejando de lado el caso 1, tenemos lo siguiente:

- $x^2 - q$ se factoriza completamente módulo p si y sólo si $\left(\frac{q}{p}\right)_{\mathcal{L}} = 1$.

- $x^2 - q$ es irreducible módulo p si y sólo si $\left(\frac{q}{p}\right)_{\mathcal{L}} = -1$.

Recordemos que para resolver el problema de reciprocidad necesitamos determinar al conjunto $\mathbf{Fac(x^2 - q)}$ y por el momento lo que sabemos es que p está en $\mathbf{Fac(x^2 - q)}$ si y sólo si $\left(\frac{q}{p}\right)_{\mathcal{L}} = 1$. Una forma de aproximarse a este problema es a través de conceptos de densidad de subconjuntos de números primos (ver [9, pag. 162]). Por otro lado, este problema también se puede abordar usando $\left(\frac{p}{q}\right)_{\mathcal{L}}$ en lugar de $\left(\frac{q}{p}\right)_{\mathcal{L}}$ pues, al haber solamente q clases residuales, únicamente tendríamos que calcular q símbolos de Legendre. Es en este punto cuando aparece la Ley de Reciprocidad Cuadrática. Recordemos su enunciado:

Ley de Reciprocidad Cuadrática. Sean p y q primos impares distintos. Entonces,

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

Una inmediata consecuencia de este enunciado es el siguiente corolario.

Corolario 3.2.1. Sean p y q primos impares distintos. Entonces,

$$\left(\frac{p}{q}\right)_{\mathcal{L}} = \begin{cases} \left(\frac{q}{p}\right)_{\mathcal{L}} & \text{si } p \equiv 1 \pmod 4 \text{ ó } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right)_{\mathcal{L}} & \text{si } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Demostración. El número $\frac{p-1}{2} \cdot \frac{q-1}{2}$ es par si y sólo si al menos uno de los enteros p y q es de la forma $4k+1$; si ambos son de la forma $4k+3$, entonces el producto es impar, por lo que

$$\left(\frac{p}{q}\right)_{\mathcal{L}} \left(\frac{q}{p}\right)_{\mathcal{L}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \text{ ó } q \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Multiplicando ambos lados de la ecuación anterior por $\left(\frac{q}{p}\right)_{\mathcal{L}}$, y usando el hecho de que $\left(\frac{q}{p}\right)_{\mathcal{L}}^2 = 1$, llegamos al resultado deseado. ■

Con la ayuda de este corolario, podemos calcular $\left(\frac{q}{p}\right)_{\mathcal{L}}$ para q fijo y p variable: primero, hay que calcular $\left(\frac{b}{q}\right)_{\mathcal{L}}$ para todos los enteros b tales que $1 \leq b \leq q-1$. En segundo lugar, dado p, se debe encontrar b tal que $1 \leq b \leq q-1$ y $b \equiv p \pmod q$. Luego, por las propiedades del símbolo de Legendre, $\left(\frac{b}{q}\right)_{\mathcal{L}} = \left(\frac{p}{q}\right)_{\mathcal{L}}$. Finalmente, tendremos que usar el corolario anterior para convertir $\left(\frac{p}{q}\right)_{\mathcal{L}}$ en $\left(\frac{q}{p}\right)_{\mathcal{L}}$.

Así, con este algoritmo es posible resolver el problema general de reciprocidad para polinomios cuadráticos. El caso q impar se resuelve usando la Ley de Reciprocidad Cuadrática; el caso $q = 2$ requiere un tratamiento diferente, pues el polinomio $x^2 - 2$ tiene raíces dobles módulo 2. De hecho, en el tratamiento de este caso se considera el polinomio $p(x) = x^2 - x + \frac{1-\varepsilon(p)p}{4}$, con $\varepsilon(p) = (-1)^{\frac{p-1}{2}}$.

El siguiente teorema resuelve el problema general de reciprocidad para el caso cuadrático.

Teorema 3.2.2. Si q es un primo impar, entonces el conjunto $\mathbf{Fac(x^2 - q)}$ puede ser determinado bajo condiciones de congruencia módulo q si $q \equiv 1$ (mód 4), y módulo $4q$ si $q \equiv 3$ (mód 4). Más aún, $\mathbf{Fac(p(x))}$ puede ser descrito bajo condiciones de congruencia módulo 8.

La primera parte de este teorema se obtiene del corolario de la Ley de Reciprocidad Cuadrática, mientras que la segunda parte proviene de la segunda ley suplementaria. Los detalles se ilustran mediante ejemplos en [15, pags. 573-574].

3.2.2. Polinomios ciclotómicos

El teorema 3.2.2 muestra que la Ley de Reciprocidad Cuadrática da una "ley de reciprocidad" en el sentido que describimos en el problema general de reciprocidad; esto es, mediante este teorema obtenemos una descripción completa de $\mathbf{Fac(f)}$ para polinomios cuadráticos. Ahora centraremos la atención en polinomios ciclotómicos.

Sea ζ una raíz n-ésima primitiva de la unidad, denotada por ζ_n. Denotamos al polinomio mínimo de ζ_n sobre $\mathbb{Q}$ como $\Phi_n(x)$ y lo llamamos el *n-ésimo polinomio ciclotómico*. Damos por hecho que $\Phi_n(x)$ tiene coeficientes enteros, grado $\phi(n)$ y es irreducible sobre $\mathbb{Q}$, donde ϕ es la función de Euler, y tiene lugar la factorización

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

donde el producto es sobre todos los divisores de n. Por ejemplo, $\Phi_1(x) = x - 1$, y si p es primo, entonces $x^p - 1 = (x - 1) \cdot \Phi_p(x)$, y por tanto,

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Demostraciones de estas afirmaciones pueden encontrarse en [11].

Nuestro propósito es encontrar una "ley de reciprocidad" para estos polinomios ciclotómicos; es decir, describir el conjunto $\mathbf{Fac}(\phi_{\mathbf{n}}(\mathbf{x}))$. Para ello, tenemos el siguiente teorema.

Teorema 3.2.3. Ley de Reciprocidad Ciclotómica. El polinomio ciclotómico $\Phi_n(x)$ se factoriza completamente módulo p si y sólo si $p \equiv 1 \pmod{n}$.

Primero demostraremos el siguiente lema sobre campos finitos para después utilizarlo en la demostración de este teorema.

Lema 3.2.4. Sea p un primo impar y a un elemento de $\mathbb{F}_p$ tal que $a^n = 1$. Si $a^d \neq 1$ para todos los divisores propios d de n, entonces $(x-a)|\Phi_n(x)$ en $\mathbb{F}_p[x]$.

Demostración. La ecuación $x^n - 1 = \prod_{d|n} \Phi_d(x)$ sigue siendo válida en $\mathbb{F}_p$, por lo que $a^n - 1 = 0 = \prod_{d|n} \Phi_d(a)$. Como $\mathbb{F}_p$ es un campo, se sigue que $\Phi_m(a) = 0$ para algún divisor m de n. Por lo tanto,

$$a^m - 1 = \prod_{d|m} \Phi_d(a) = 0.$$

De lo anterior se sigue que $a^m = 1$, lo cual sólo puede ocurrir si $m = n$ por la hipótesis, por lo que $\Phi_n(a) = 0$, y $x - a$ divide a $\Phi_n(x)$. ■

Demostración. Del teorema. Recordemos que el grupo multiplicativo $\mathbb{F}_p^*$ formado por los elementos distintos de cero de $\mathbb{F}_p$ es cíclico de orden $p-1$. Así, ${\mathbb{F}_p}^*$ tiene un subgrupo cíclico de orden n si y sólo si n divide a $p-1$. Tal subgrupo tiene $\phi(n)$ generadores, por lo que ${\mathbb{F}_p}^*$ contiene $\phi(n)$ raíces primitivas n-ésimas distintas (los generadores) si y sólo si contiene una, y esto sucede exactamente cuando $p \equiv 1 \pmod{n}$.

Ahora supongamos que $p \equiv 1 \pmod{n}$ y por tanto, que $\mathbb{F}_p$ contiene $\phi(n)$ raíces primitivas distintas de 1. Por el lema anterior, estas deben ser raíces de $\Phi_n(x)$, de manera que $\Phi_n(x)$ se escribe como producto de factores lineales distintos.

En la otra dirección, supongamos que $\Phi_n(x)$ se factoriza como producto de factores lineales distintos módulo p. Si estos factores son distintos, entonces p no puede dividir a n, y por lo tanto, $x^n - 1$ también tiene raíces distintas módulo p. Sea a una raíz de $\Phi_n(x)$ en $\mathbb{F}_p$; entonces $a^n = 1$. Si d es el mínimo divisor de n tal que $a^d = 1$, entonces $\Phi_d(a) = 0$, por el lema anterior. Si $d \neq n$, la relación $x^n - 1 = \prod_{d|n} \Phi_d(x)$ muestra que a es al menos una raíz

doble de $x^n - 1$, lo cual es una contradicción. Así, a genera un subgrupo cíclico de orden n en ${\mathbb{F}_p}^*$, y $p|n-1$. Esto completa la prueba de la "ley ciclotómica de reciprocidad". ■

En esta última sección hemos visto que si $f(x)$ es un polinomio cuadrático o ciclotómico, entonces el conjunto $\mathbf{Fac(x)}$ puede ser descrito mediante congruencias respecto a ciertos módulos, lo cual da solución particular al problema de reciprocidad.

Uno de los problemas más difíciles en teoría de números es la descripción de $\mathbf{Fac(f(x))}$. Para el caso en que el grupo de Galois de $f(x)$ es abeliano, el problema se resuelve con la llamada Teoría de Campos de Clase ([9, pag. 130]). El caso no abeliano no ha sido resuelto satisfactoriamente y sólo se conocen resultados muy parciales ([12, pag. xi]). La discusión de los resultados concernientes a la descripción de $\mathbf{Fac(f(x))}$ queda fuera del alcance del presente trabajo, pues se requieren resultados profundos de la teoría de números algebraicos.

Conclusiones

Durante el desarrollo de este trabajo, pudimos conocer una pequeña parte del vasto y extenso tema de las leyes de reciprocidad. Empezamos con los preliminares necesarios para adentrarnos en el tema, y continuar con la Ley de Reciprocidad Cuadrática. Enseguida presentamos cuatro de sus demostraciones con el propósito de lograr un mejor entendimiento y mostrar la diversidad de los métodos que se han usado en ellas. Finalmente, enunciamos la Ley de Reciprocidad Cúbica y culminamos con el Problema General de Reciprocidad.

Desde el punto de vista personal, el haber escrito el presente trabajo me ha permitido iniciarme en el estudio de esta rama tan apasionante de las matemáticas, que es la Teoría de Números. Conocí y aprendí diversos métodos e ideas tanto en la investigación como durante su realización.

Mi propósito es continuar con el estudio, a mayor profundidad, de las distintas pruebas que aquí se presentaron, en particular, lo referente a los métodos algebraicos que se usan en la Demostración 4. Asimismo, seguir estudiando otras demostraciones, y por supuesto, adentrarme en los preliminares necesarios para el entendimiento de sus generalizaciones.

Apéndice A

Cronología de Demostraciones de la Ley de Reciprocidad Cuadrática

Presentamos a continuación una amplia lista de las pruebas que han sido publicadas, desde 1788, de la Ley de Reciprocidad Cuadrática. A pesar de su longitud, la lista no está completa; para un listado más completo y actualizado, así como referencias bibliográficas de cada una de ellas puede encontrarse en [12] y [13].

♯	Autor	Año	Método/Comentarios
1	Legendre	1788	Formas Cuadráticas; incompleta
2	Gauss 1	1801	Inducción; Abril 8, 1796
3	Gauss 2	1801	Formas Cuadráticas; Junio 27, 1796
4	Gauss 3	1808	Lema de Gauss; Mayo 6, 1807
5	Gauss 4	1811	Ciclotomía; Mayo 1801
6	Gauss 5	1818	Lema de Gauss; 1807/08
7	Gauss 6	1818	Sumas de Gauss; 1807/08
8	Cauchy	1829	Gauss 6
9	Jacobi	1830	Gauss 6
10	Dirichlet	1835	Gauss 4
11	Lebesgue 1	1838	$N({x_1}^2 + \cdots + {x_q}^2) \equiv 1 \pmod{p}$)
12	Schöneman	1839	Ecuación periódica cuadrática
13	Eisenstein 1	1844	Sumas de Jacobi generalizadas
14	Eisenstein 2	1844	Gauss 6
15	Eisenstein 3	1844	Lema de Gauss

♯	Autor	Año	Método/Comentarios
16	Eisenstein 4	1845	Seno
17	Eisenstein 5	1845	Productos infinitos
18	Liouville	1847	Ciclotomía
19	Lebesgue 2	1847	Lebesgue 1
20	Schar	1847	Lema de Gauss
21	Genocchi	1852	Lema de Gauss
22	Dirichlet	1854	Gauss 1
23	Lebesgue 3	1860	Gauss 7,8
24	Kummer 1	1862	Formas Cuadráticas
25	Kummer 2	1862	Formas Cuadráticas
26	Dedekind 1	1863	Formas Cuadráticas
27	Gauss 7	1863	Períodos Cuadráticos; Sept. 1796
28	Gauss 8	1863	Períodos Cuadráticos; Sept. 1796
29	Mathieu	1867	Ciclotomía
30	von Staudt	1867	Ciclotomía
31	Bouniakowski	1869	Lema de Gauss
32	Stern	1870	Lema de Gauss
33	Zeller	1872	Lema de Gauss
34	Zolotarev	1872	Permutaciones
35	Kronecker 1	1872	Zeller
36	Schering	1875	Gauss 3
37	Kronecker 2	1876	Inducción
38	Mansion	1876	Lema de Gauss
39	Dedekind 2	1877	Gauss 6
40	Dedekind 3	1877	Sumas de Dedekind
41	Pellet 1	1878	Stickelberger-Voronoi
42	Pépin 1	1878	Ciclotomía
43	Schering	1879	Lema de Gauss
44	Petersen	1879	Lema de Gauss
45	Genocchi	1880	Lema de Gauss
46	Kronecker 3	1880	Gauss 4
47	Kronecker 4	1880	Período Cuadrático
48	Voigt	1881	Lema de Gauss
49	Pellet 2	1882	Mathieu 1867
50	Busche 1	1883	Lema de Gauss
51	Gegenbauer 1	1884	Lema de Gauss
52	Kronecker 5	1884	Lema de Gauss
53	Kronecker 6	1885	Gauss 3
54	Kronecker 7	1885	Lema de Gauss
55	Bock	1886	Lema de Gauss
56	Lerch	1887	Gauss 3
57	Busche 2	1888	Lema de Gauss
58	Hacks	1889	Schering

♯	Autor	Año	Método/Comentarios
59	Hermes	1889	Inducción
60	Kronecker 8	1889	Lema de Gauss
61	Tafelmacher 1	1889	Stern
62	Tafelmacher 2	1889	Stern/Schering
63	Tafelmacher 3	1889	Schering
64	Busche 3	1890	Lemade Gauss
65	Franklin	1890	Lema de Gauss
66	Lucas	1890	Lema de Gauss
67	Pépin 2	1890	Gauss 2
68	Fields	1891	Lema de Gauss
69	Gegenbauer 2	1891	Lema de Gauss
70	Gegenbauer 3	1893	Lema de Gauss
71	Schmidt 1	1893	Lema de Gauss
72	Schmidt 2	1893	Lema de Gauss
73	Schmidt 3	1893	Inducción
74	Gegenbauer 4	1894	Lema de Gauss
75	Bang	1894	Inducción
76	Mertens 1	1894	Lema de Gauss
77	Mertens 2	1894	Sumas de Gauss
78	Bushce 4	1896	Lema de Gauss
79	Lange 1	1896	Lema de Gauss
80	de la Vallée Poussin	1896	Gauss 2
81	Lange 2	1897	Lema de Gauss
82	Hilbert	1897	Ciclotomía
83	Alexejewsky	1898	Schering
84	Pépin 3	1898	Legendre
85	Pépin 4	1898	Gauss 5
86	König	1899	Inducción
87	Fischer	1900	Resultantes
88	Takagi	1903	Zeller
89	Lerch	1903	Gauss 5
90	Mertens 3	1904	Eisentein 4
91	Mirimanoff & Hensel	1905	Stickelberger-Voroni
92	Busche 5	1909	Zeller
93	Busche 6	1909	Eisenstein
94	Petr 1	1911	Mertens 3
95	Pocklington	1911	Gauss 3
96	Dedekind 4	1912	Zeller
97	Frobenius 1	1914	Zeller
98	Frobenius 2	1914	Eisenstein 3
99	Lasker	1916	Stickelberger-Voroni
100	Cerone	1917	Eisenstein 4
101	Barstelds & Schuh	1918	Lema de Gauss

♯	Autor	Año	Método/Comentarios
102	Stieltjes	1918	Puntos en el plano entero
103	Teege 1	1920	Legendre
104	Teege 2	1921	Ciclotomía
105	Arwin	1924	Formas Cuadráticas
106	Rédei 1	1925	Lema de Gauss
107	Rédei 2	1926	Lema de Gauss
108	Whitehead	1927	Kummer
109	Petr 2	1927	Funciones Teta
110	Petr 3	1934	Kronecker (signos)
111	van Veen	1934	Eisenstein 3
112	Fueter	1935	Álgebras de cuaterniones
113	Whiteman	1935	Lema de Gauss
114	Dockeray	1938	Eisenstein 3
115	Dörge	1942	Lema de Gauss
116	Rédei 3	1944	Gauss 5
117	Lewy	1946	Ciclotomía
118	Petr 4	1946	Ciclotomía
119	Skolem 2	1948	Gauss 2
120	Barbilian	1950	Eisenstein 1
121	Rédei 4	1951	Gauss 3
122	Brandt 1	1951	Gauss 2
123	Brandt 2	1951	Sumas de Gauss
124	Brewer	1951	Mathieu, Pellet
125	Furquim de Almeida	1951	Campos Finitos
126	Zassenhaus	1952	Campos Finitos
127	Riesz	1953	Permutaciones
128	Frölich	1954	Teoría de Campos de Clase
129	Ankeny	1955	Ciclotomía
130	D. H. Lehmer	1957	Lema de Gauss
131	C. Meyer	1957	Sumas de Dedekind
132	Holzer	1958	Sumas de Gauss
133	Rédei 5	1958	Polinomios Ciclotómicos
134	Reichardt	1958	Gauss 3
135	Carlitz	1960	Gauss 1
136	Kubota 1	1961	Ciclotomía
137	Kubota 2	1961	Sumas de Gauss
138	Skolem 3	1961	Ciclotomía
139	Skolem 4	1961	Campos Finitos
140	Hausner	1961	Sumas de Gauss
142	Swan 1	1962	Stickelberger-Voronoi
143	Koschmieder	1963	Eisenstein, seno
144	Gerstenhaber	1963	Eisesntein, seno
145	Rademacher	1964	Análisis de Fourier Finito

♯	Autor	Año	Método/Comentarios
146	Weil	1964	Funciones Teta
147	Kloosterman	1965	Holzer
148	Chowla	1966	Campos Finitos
149	Burde	1967	Lema de Gauss
150	Kaplan 1	1969	Eisenstein
151	Kaplan 2	1969	Conguencias Cuadráticas
152	Birch	1971	Teoría-K (Tate)
153	Reshetujha	1971	Sumas de Gauss
154	Agou	1972	Campos Finitos
155	Brenner	1973	Zolotarev
156	Honda	1973	Sumas de Gauss
157	Milnor & Husemöller	1973	Weil 1964
158	Allander	1974	Lema de Gauss
159	Berndt & Evans	1974	Lema de Gauss
160	Hirzebrucht & Zagier	1974	Sumas de Dedekind
161	Rogers	1974	Legendre
162	Castaldo	1976	Lema de Gauss
163	Frame	1978	Kronecker
164	Hurrelbrink	1978	Teoría-K
165	Auslander & Tolimeri	1979	Transformada de Fourier
166	Brown	1981	Gauss 1
167	Goldschmidt	1981	Ciclotomía
168	Kac	1981	Eisenstein, seno
169	Barcanescu	1983	Zolotarev
170	Zantema	1983	Grupos de Brauer
171	Ely	1984	Lebesgue 1
172	Eichler	1985	Función Teta
173	Barrucand & Laubie	1987	Stickelberger-Voronoi
174	Peklar	1989	Lema de Gauss
175	Barnes	1990	Zolotarev
176	Swan 2	1990	Ciclotomía
177	Rousseau 1	1990	Álgebras exteriores
178	Rousseau 2	1991	Permutaciones
179	Keune	1991	Campos Finitos
180	Kubota	1992	Geometría
181	Russinoff	1992	Lema de Gauss
182	Garret	1992	Weil 1964
183	Motose	1993	Álgebras de grupo
184	Rousseau	1994	Zolotarev
185	Young	1995	Sumas de Gauss
186	Brylinski	1997	Acciones de grupo
187	Merindol	1997	Eisenstein, seno
188	Watanabe	1997	Zolotarev

♯	Autor	Año	Método/Comentarios
189	Ishii	1998	Gauss 4
190	Motose	1999	Álgebras de grupo
191	Lemmermeyer	2000	Lebesgue 1, Ely
192	Meyer	2000	Sumas de Dedekind
193	Chapman	2001	Secuencias recurrentes
194	Hammick	2001	Rousseau 2
195	Girstmair	2001	Eichler
196	Murty	2001	Schur
197	Luo	2003	Rousseau
198	Motose 2	2003	Schur
199	Sey Yoon Kim 3	2004	Rousseau 2
200	Sun	2004	Lema de Gauss
201	Duke & Spears	2005	Grupos
202	Murty & Pacelli	2005	Funciones Teta
203	Szvjewski	2005	Zolotarev
204	Arkhipova	2006	Gauss 4
205	Castryck	2007	Zolotarev
206	Verdure	2008	Curvas Elípticas
207	Gurevich, Hadani, Howe	2008	Schur, Weil
208	Jakimczuk	2009	Lebesgue 1
209	Steiner	2009	Rousseau 2
210	Hambleton & Scharaschkin	2009	Resultantes (Swan 2)
211	Hambleton & Scharaschkin	2009	Cónicas de Pell

Bibliografía

[1] S. D. Adhikari. *The Early Reciprocity Laws: From Gauss to Eisenstein.* Cyclotomic Fields and Related Topics, Bhaskaracharya Pratishthana, Pune, 55-74, (2000).

[2] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, Nueva York, 1919.

[3] E.T. Bell. *Historia de las Matemáticas.* Fondo de Cultura Económica, México, D.F., 1949.

[4] D. M. Burton. *Elementary Number Theory.* Mc Graw-Hill, EUA, 2007.

[5] L.E. Dickson. *History of the Theory of Numbers.* American Mathematical Society, 1999.

[6] John B. Fraleigh. *A First Course in Abstract Algebra,* 7ma. edición, Addison Wesley, 2002.

[7] I.N. Herstein. *Álgebra Moderna.* Trillas, México, 2006.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* 2^{da} edición. Graduate texts in Mathematics 84, Springer-Verlag, 1990.

[9] Gerald J. Janusz. *Algebraic Number Fields.* 2^{da} edición., Graduate Studies in Mathematics 7, American Mathematical Society, Providence, RI, 1996.

[10] G.A. Jones and M.J. Jones. *Elementary Number Theory*, Springer-Verlag, Londres, 1999.

[11] S. Lang. *Algebra*, Graduate Texts in Mathematics, 211 (Revised third edition), Springer-Verlag, Nueva York, 2002.

[12] F. Lemmermeyer. *Reciprocity Laws.* Springer Monographs in Mathematics, Springer-Verlag, Berlín, 2000.

[13] Proofs of the Quadratic Reciprocity Law `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`

[14] J. J. Rotman. *A First Course in Abstract Algebra,* Prentice Hall, Upper Saddle River, NJ, 1996.

[15] B. F. Wyman. *What is a Reciprocity Law?* American Mathematical Monthly 79, 571-586, 1972.

[16] I. Niven, H.L. Montgomery and H. S. Zuckerman *An Introduction to the Theory of Numbers.* John Wiley & Sons, EUA, 1991.

[17] K. H. Rosen. *Elementary Number Theory and its applications*, Addison-Wesley, EUA, 1986.