INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

Sobre la Reciprocidad Cuadrática, Cúbica y Bicuadrática, y Algunas de sus Aplicaciones

T E S I S
QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FÍSICA Y MATEMÁTICAS

P R E S E N T A

LUIS CASTELLANOS MANZANO

DIRECTOR DE TESIS
DR. PABLO LAM ESTRADA

México, D. F. **Enero de 2009**

A mi familia.

Agradecimientos

Por haberme ayudado en la realización de este trabajo de tesis, agradesco al Dr. Pablo Lam Estrada, Dra. Myriam Rosalía Maldonado Ramírez, M. en C. María Elizabeth de la Cruz Santiago, M. en C. Abelardo Santaella Quintas, Lic. Manuel Robles Bernal y al M. en C. Santiago Marcos Zepeda Martínez.

Índice general

Introducción

Este trabajo es principalmente una revisión sobre reciprocidad cuadrática, cúbica y bicuadrática, empleando la teoría desarrollada sobre los caracteres multiplicativos, las sumas de Gauss y las sumas de Jacobi.

En el primer capítulo se estudiará la reciprocidad cuadrática en $\mathbb{Z}$, iniciando con conceptos básicos como son los residuos cuadráticos, el símbolo de Legendre y extendiendo esta definición al símbolo de Jacobi. Además, se presentará el Lema de Gauss para con ello poder determinar para cuáles primos impares p, -1 y 2 son residuos cuadráticos módulo p. Es un hecho evidente que existe una cantidad infinita de primos de la forma $4k+3$, entonces se planteará la misma pregunta para primos de la forma $4k+1$ y $8k+7$. Se presentará además una demostración analítica de la ley de la reciprocidad cuadrática y más tarde, en las aplicaciones, se observará la flexibilidad que esta ley ofrece para el cálculo del símbolo de Jacobi.

En el segundo capítulo se comenzará con un ligero análisis sobre el campo de números algebraicos y el anillo de enteros algebraicos, después se definirán y estudiarán las sumas cuadráticas de Gauss, las cuales serán de ayuda para dar una segunda demostración de ley de la reciprocidad cuadrática.

En el tercer capítulo se analisarán los caracteres multiplicativos sobre un campo $\mathbb{F}_p$ y, con ayuda de esto, se definirán las sumas de Gauss, las cuales son una generalización de las sumas cuadráticas de Gauss. De forma independiente, se definirán las sumas de Jacobi determinando más tarde la relación que existe entre ambas sumas. También se tratará de calcular el número de soluciones en $\mathbb{F}_p$ de las ecuaciones $X^2+Y^2=1$ y $X^3+Y^3=1$, y finalmente se ampliará la noción sobre las sumas de Jacobi para calcular el número de soluciones en $\mathbb{F}_p$ de la ecuación $X_1^2+X_2^2+\cdots+X_l^2=1$, con $l\in\mathbb{N}$.

A manera de extensión de la reciprocidad cuadrática, en el cuarto capítulo se estudiará la reciprocidad cúbica en el anillo $\mathbb{Z}[\omega]$, con $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$, y la reciprocidad bicuadrática en el anillo $\mathbb{Z}[i]$, introduciendo conceptos análogos al símbolo de Legendre y el de Jacobi, logrando demostrar la ley de la reciprocidad cúbica y bicuadrática sobre elementos primarios.

Se demostrará también el complemento de la ley de la reciprocidad cúbica y, en una sección aparte, se analizará el caracter cúbico de 2, es decir, se establecerá para qué primos p se tiene solución entera para $X^3 \equiv 2 \pmod{p}$. Finalmente, dentro de la teoría de la reciprocidad bicuadrática se presentará una notable ley de reciprocidad descubierta por K.Burde.

Ya que en el primer capítulo una de las interrogantes es deducir el caracter cuadrático de a módulo p, con p primo impar, entonces en el último capítulo se planteará una pregunta similar, es decir, se tratará de deducir el caracter cuadrático de a módulo m, con $(a, m) = 1$. Determinaremos también las condiciones sobre a, b, c y m para que la ecuación Diofantina $aX^2 + bX + c \equiv 0 \pmod{m}$ tenga solución. En este mismo capítulo se verán otras aplicaciones que se enfocan principalmente en la teoría desarrollada sobre la reciprocidad cuadrática.

Capítulo 1

Reciprocidad cuadrática

1.1. Residuos cuadráticos

Definición 1.1.1. *Sean $a, p \in \mathbb{Z}$, con p número primo tal que $p \nmid a$. Decimos que a es un* ***residuo cuadrático módulo*** *p si existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$. En caso contrario, se dice que a* ***no es un residuo cuadrático módulo*** *p.*

De aquí en adelante p y cualquier número primo se supondrá positivo diferente del 2, al menos que se establezca de otra forma.

Definición 1.1.2. *El* ***símbolo de Legendre****, denotado por (a/p) ó $\left(\frac{a}{p}\right)$, adquiere los siguientes valores:*

(a) 1 *si a es un residuo cuadrático módulo p.*

(b) -1 *si a no es un residuo cuadrático módulo p.*

(c) 0 *si $p|a$.*

Proposición 1.1.1. *Sean F es un campo finito con q elementos, $a \in F^*$, $n \in \mathbb{N}$ y $d = (n, q-1)$. Entonces, la ecuación $X^n = a$ es soluble en F^* si, y sólo si $a^{(q-1)/d} = 1$; y en caso de que la ecuación $X^n = a$ sea soluble en F^*, ésta tiene exactamente d soluciones en F^*.*

Demostración: En esta demostración usaremos el hecho de que F^* es un grupo cíclico.

Supongamos primero que $X^n = a$ es soluble en F^*, es decir, existe $b \in F^*$ tal que $b^n = a$. Luego, $a^{(q-1)/d} = b^{n(q-1)/d} = 1$, ya que $d|n$.

Por otro lado, supongamos que $a^{(q-1)/d} = 1$, y tomemos g un generador de F^*. Entonces, existe $l \in \mathbb{N} \cup \{0\}$ tal que $g^l = a$, luego $g^{l(q-1)/d} = a^{(q-1)/d} = 1$, lo cual implica que $d \mid l$, es decir, existe $c \in F^*$ tal que $c^d = a$. Además, debido a que $(n/d, q-1) = 1$, tenemos que $g^{n/d}$ es un generador de F^* y, por lo tanto, existe k tal que $(g^{n/d})^k = c$; así, $(g^{nk/d})^d = c^d = a$, es decir, $g^{nk} = a$, con lo cual demostramos que $X^n = a$ es soluble en F^*.

Falta por demostrar que si la ecuación $X^n = a$ es soluble en F^*, entonces existen exactamente d soluciones en F^*. Una solución es g^k, entonces $g^{k+i(q-1)/d}$, con $i = 1, 2 \ldots, d$ son d soluciones distintas. Supongamos que g^m es solución, entonces $g^{mn} = g^{kn} = a$, lo cual implica que existe r entero tal que $mn - kn = r(q-1)$; por lo tanto, $m - k = \dfrac{r}{n/d} \cdot \dfrac{q-1}{d}$, donde $\dfrac{r}{n/d}$ es entero, debido a que $(n, q-1) = d$, es decir, $m = k + j(q-1)/d$, con j entero. En consecuencia, $g^m = g^{k+j(q-1)/d} = g^{k+i(q-1)/d}$ para algún $i \in \{1, 2 \ldots, d\}$ tal que $j \equiv i \pmod{d}$. □

Proposición 1.1.2. *Sean $a, b \in \mathbb{Z}$, entonces:*

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

(b) $(ab/p) = (a/p)(b/p)$.

(c) Si $a \equiv b \pmod{p}$, *entonces* $(a/p) = (b/p)$.

Demostración: En los tres casos, el resultado se tiene si $p|a$ o $p|b$; así que podemos suponer que $p \nmid a$ y $p \nmid b$.

Para la parte (a) tenemos, $a^{p-1} \equiv 1 \pmod{p}$, luego $(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}$, con lo cual $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ y, por la Proposición 1.1.1, tenemos el resultado.

Para la parte (b) aplicamos el inciso anterior, $(ab)^{(p-1)/2} \equiv (ab/p) \pmod{p}$, luego $a^{(p-1)/2} b^{(p-1)/2} \equiv (ab/p) \pmod{p}$, pero como $a^{(p-1)/2} \equiv (a/p) \pmod{p}$ y $b^{(p-1)/2} \equiv (b/p) \pmod{p}$, entonces $(a/p)(b/p) = (ab/p)$.

La parte (c) se sigue de la definición.

□

Corolario 1.1.1. *Hay tantos residuos como no residuos cuadraticos módulo p.*

Demostración: Por la Proposición 1.1.1, tenemos que $a^{(p-1)/2} \equiv 1 \pmod{p}$ tiene $(p-1)/2$ soluciones, entonces existen $(p-1)/2$ residuos cuadráticos y, por lo tanto, la misma cantidad de no residuos cuadráticos. □

Corolario 1.1.2. $(-1/p) = (-1)^{(p-1)/2}$, *es decir, la ecuación* $X^2 \equiv -1 \pmod{p}$ *tiene solución si, y sólo si* p *es de la forma* $4k+1$.

Demostración: Se obtiene de la parte (a) de la Proposición 1.1.2. □

Corolario 1.1.3. *Existe una cantidad infinita de primos de la forma* $4k+1$.

Demostración: Supongamos que existe una cantidad finita de primos de la forma $4k+1$. Sean $p_1, \ldots, p_l$ dichos primos, y sea p primo impar tal que $p|(p_1 \cdots p_l)^2 + 1$. Entonces, $(-1/p) = 1$ lo cual implica que p es de la forma $4k+1$; además, $p \neq p_i \ \forall i = 1, \ldots, l$, lo cual nos lleva a una contradicción. □

Definición 1.1.3. *Sea* $S = \{-(p-1)/2, -(p-3)/2, \ldots, (p-3)/2, (p-1)/2\}$, *entonces* S *es llamado el* ***conjunto de los residuos principales módulo*** p, *y* μ *denota la cantidad de dichos residuos que sean negativos de los enteros* $a, 2a, \ldots, ((p-3)/2)a, ((p-1)/2)a$.

Damos un ejemplo para la definición anterior con $p = 7$ y $a = 2$. En este caso, $S = \{-3, -2, -1, 0, 1, 2, 3\}$, además $a = 2 \equiv 2 \pmod{7}$, $2a = 4 \equiv -3 \pmod{7}$ y $3a = 6 \equiv -1 \pmod{7}$, por lo tanto $\mu = 2$.

Lema 1.1.1 (Lema de Gauss). *Si* $p \nmid a$, *entonces* $(a/p) = (-1)^{\mu}$.

Demostración: Sean $\pm m_1, \ldots, \pm m_{(p-1)/2}$ los residuos principales de $a, 2a, \ldots, ((p-1)/2)a$ respectivamente, donde los m_i son positivos. Primero demostremos que $m_k \neq m_l$ si $k \neq l$. Supongamos lo contrario, entonces $m_k = m_l$, luego $ka \equiv \pm la \pmod{p}$, y como $p \nmid a$, entonces $k \equiv \pm l \pmod{p}$, lo cual es una contradicción ya que $|k \pm l| < p$. Multiplicando todas las congruencias $ia \equiv \pm m_i \pmod{p}$ obtenemos, $((p-1)/2)! a^{(p-1)/2} \equiv (-1)^{\mu}((p-1)/2)! \pmod{p}$, luego $a^{(p-1)/2} \equiv (-1)^{\mu} \pmod{p}$. Aplicando la parte (a) de la Proposición 1.1.2 obtenemos $(a/p) = (-1)^{\mu}$. □

Proposición 1.1.3. $(2/p) = (-1)^{(p^2-1)/8}$, *es decir,* $(2/p) = 1$ *si, y sólo si* $p \equiv \pm 1 \pmod{8}$.

Demostración: Calculemos el valor de μ para $p \equiv 1, 3, 5, 7 \pmod 8$. De acuerdo a la notación del lema anterior, tenemos $\{a, 2a, \ldots, ((p-3)/2)a, ((p-1)/2)a\} = \{2, 4, \ldots, (p-3), (p-1)\}$. Sea $0 \leq m < (p-1)/2$ tal que $2m \leq (p-1)/2$ y $2(m+1) > (p-1)/2$, entonces $\mu = (p-1)/2 - m$; de esta forma tenemos los siguientes casos:

(a): Si $p = 8k+1$, se tiene que $(p-1)/2 = 4k$, luego $2k = m$, entonces $\mu = 2k$ y $(2/p) = 1$.

(b): Si $p = 8k+3$, se tiene que $(p-1)/2 = 4k+1$, luego $2k = m$, entonces $\mu = 2k+1$ y $(2/p) = -1$.

(c): Si $p = 8k+5$, se tiene que $(p-1)/2 = 4k+2$, luego $2k+1 = m$, entonces $\mu = 2k+1$ y $(2/p) = -1$.

(d): Si $p = 8k+7$, se tiene que $(p-1)/2 = 4k+3$, luego $2k+1 = m$, entonces $\mu = 2k+2$ y $(2/p) = 1$. □

Corolario 1.1.4. *Existe una cantidad infinita de primos de la forma* $8k+7$.

Demostración: Supongamos que existe una cantidad finita de primos de esta forma; sean $p_1, \ldots, p_l$ dichos primos. Los divisores primos impares de $(4p_1 \cdots p_l)^2 - 2$ son de la forma $8k+1$ y de la forma $8k+7$; pero no todos son de la forma $8k+1$, ya que se contradicería el hecho de que $(4p_1 \cdots p_l)^2 - 2 \equiv -2 \pmod 8$. Por lo tanto existe un primo p de la forma $8k+7$, tal que $p|(4p_1 \cdots p_l)^2 - 2$, con $p \neq p_i \ \forall i$, lo cual lleva a una contradicción. □

1.2. Ley de la reciprocidad cuadrática

En esta sección probaremos el Teorema 1.2.1 que corresponde a las leyes que debe de cumplir el símbolo de Legendre. Para esto, probaremos los siguientes resultados.

Lema 1.2.1. *Sea* $n \in \mathbb{N}$ *impar, entonces*

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

donde $\zeta = e^{2\pi i/n}$ *es una raíz n-ésima primitiva de la unidad.*

Demostración: Tenemos que $z^n - 1 = \prod_{k=0}^{n-1}(z - \zeta^k)$; sustituyendo $z = x/y$ en la ecuación anterior, obtenemos que $x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^k y)$. Además, $-2 + n\mathbb{Z}$ no es un divisor de cero en el anillo $\mathbb{Z}/n\mathbb{Z}$, con $n \geq 3$, por lo que existe una biyección entre $\{\zeta^k | k = 0, \ldots, n-1\}$ y $\{\zeta^{-2k} | k = 0, \ldots, n-1\}$. Por lo tanto,

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

□

Si definimos $f(z) = e^{2\pi i z} - e^{-2\pi i z}$, entonces $f(z + m) = f(z)$, con $m \in \mathbb{Z}$. Además, $f(-z) = -f(z)$.

Proposición 1.2.1. *Si $n \in \mathbb{N}$ impar, $n \geq 3$ y $f(z) = e^{2\pi i z} - e^{-2\pi i z}$, 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: Sustituimos $x = e^{2\pi i z}$ y $y = e^{-2\pi i z}$ en la ecuación del enunciado del Lema 1.2.1 para obtener

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

Además, notemos que $f\left(z + \frac{k}{n}\right) = f\left(z + \frac{k}{n} - 1\right) = f\left(z - \frac{n-k}{n}\right)$. Por lo tanto,

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

□

Proposición 1.2.2. *Sean p número primo y $a \in \mathbb{Z}$ tal que $p \nmid a$. Entonces,*

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

Demostración: Sean $\pm m_k$ los valores dados en la demostración del Lema de Gauss (Lema 1.1.1), entonces $\pm m_k \equiv ak \pmod{p}$, con lo cual

$$f\left(\frac{ka}{p}\right) = f\left(\frac{\pm m_k}{p}\right) = \pm f\left(\frac{m_k}{p}\right).$$

Por lo tanto,

$$\prod_{k=1}^{(p-1)/2} f\left(\frac{ka}{p}\right) = \prod_{k=1}^{(p-1)/2} f\left(\frac{\pm m_k}{p}\right)$$
$$= \left(\frac{a}{p}\right) \prod_{k=1}^{(p-1)/2} f\left(\frac{k}{p}\right) \ .$$

□

Aplicando los resultados anteriores, tenemos el siguiente teorema.

Teorema 1.2.1 (Ley de la Reciprocidad Cuadrática). *Sean p y q números primos impares. Entonces,*

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

(b) $(2/p) = (-1)^{(p^2-1)/8}$.

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

Demostración:
Los incisos (a) y (b) ya han sido probados en la sección anterior (Corolario 1.1.2 y Proposición 1.1.3). Para el inciso (c), aplicamos la Proposición 1.2.1 y Proposición 1.2.2, es decir, utilizando la función f, tenemos que

$$\begin{aligned}\left(\frac{p}{q}\right) &= \prod_{l=1}^{(q-1)/2} \frac{f(pl/q)}{f(l/q)} \\ &= \prod_{m=1}^{(p-1)/2} \prod_{l=1}^{(q-1)/2} f\left(\frac{l}{q}+\frac{m}{p}\right) f\left(\frac{l}{q}-\frac{m}{p}\right) \ ;\end{aligned}$$

de manera similar obtenemos

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

Tomando en cuenta que $f\left(\frac{l}{q}-\frac{m}{p}\right) = -f\left(\frac{m}{p}-\frac{l}{q}\right)$, obtenemos como resultado

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

□

Definición 1.2.1. *Sea $a, b \in \mathbb{Z}$ tales que $(a,b) = 1$ y $b > 2$ impar. Si $b = p_1 p_2 \cdots p_n$, donde los p_i son primos no necesariamente distintos, entonces definimos el* ***símbolo de Jacobi*** *como $(a/b) = \left(\frac{a}{b}\right) := (a/p_1)(a/p_2)\cdots(a/p_n)$.*

Proposición 1.2.3.

(a) $(a_1/b) = (a_2/b)$, *si* $a_1 \equiv a_2 \pmod{b}$.

(b) $(a_1 a_2/b) = (a_1/b)(a_2/b)$.

(c) $(a/b_1 b_2) = (a/b_1)(a/b_2)$.

Demostración: La demostración se sigue de las propiedades del símbolo de Legendre y de la definición anterior. □

Lema 1.2.2. *Sean $r, s \in \mathbb{Z}$ impares. Entonces,*

(*a*) $(rs-1)/2 \equiv (r-1)/2 + (s-1)/2 \pmod 2$.

(*b*) $(r^2s^2-1)/8 \equiv (r^2-1)/8 + (s^2-1)/8 \pmod 2$.

Demostración: Probemos el inciso (*a*). Tenemos que $(r-1)(s-1) \equiv 0 \pmod 4$, luego $rs-1 \equiv (r-1)+(s-1) \pmod 4$, por lo tanto $(rs-1)/2 \equiv (r-1)/2+(s-1)/2 \pmod 2$.

Para el inciso (*b*), se tiene que $(r^2-1)(s^2-1) \equiv 0 \pmod{16}$, luego $r^2s^2-1 \equiv (r^2-1)+(s^2-1) \pmod{16}$, por lo tanto $(r^2s^2-1)/8 \equiv (r^2-1)/8+(s^2-1)/8 \pmod 2$. □

Corolario 1.2.1. *Sean $r_1, r_2, \ldots, r_n \in \mathbb{Z}$ impares. Entonces,*

(*a*) $(r_1r_2\cdots r_n-1)/2 \equiv \sum_{i=1}^{n}(r_i-1)/2 \pmod 2$.

(*b*) $({r_1}^2{r_2}^2\cdots r_n^2-1)/8 \equiv \sum_{i=1}^{n}(r_i^2-1)/8 \pmod 2$.

Demostración: La demostración se sigue del Lema 1.2.2 al aplicar inducción. □

Proposición 1.2.4. *Sean $a, b > 2$ enteros impares. Entonces,*

(*a*) $(-1/b) = (-1)^{(b-1)/2}$.

(*b*) $(2/b) = (-1)^{(b^2-1)/8}$.

(*c*) $(a/b)(b/a) = (-1)^{((a-1)/2)((b-1)/2)}$.

Demostración: Supongamos que se tiene la descomposición $b = p_1\cdots p_n$ y $a = q_1\cdots q_m$, donde los p_i y q_k son primos no necesariamente distintos. Entonces, tenemos que

$$\begin{aligned}(-1/b) &= (-1/p_1)\cdots(-1/p_n) = (-1)^{(p_1-1)/2+\cdots+(p_n-1)/2} = (-1)^{(p_1\cdots p_n-1)/2} \\ &= (-1)^{(b-1)/2}\,.\end{aligned}$$

Por lo tanto, se tiene el inciso (*a*). Para (*b*), se tiene que

$$\begin{aligned}(2/b) &= (2/p_1)\cdots(2/p_n) = (-1)^{(p_1^2-1)/8+\cdots+(p_n^2-1)/8} = (-1)^{(p_1^2\cdots p_n^2-1)/8} \\ &= (-1)^{(b^2-1)/8}\,.\end{aligned}$$

Finalmente, para el inciso (c) tenemos

$$\begin{aligned}(a/b)(b/a) &= \prod_{1\leq i\leq n,\ 1\leq k\leq m}(q_k/p_i)(p_i/q_k)\\ &= (-1)^{\sum_{i=1}^{n}\sum_{k=1}^{m}((p_i-1)/2)((q_k-1)/2)}\\ &= (-1)^{(\sum_{i=1}^{n}(p_i-1)/2)(\sum_{k=1}^{m}(q_k-1)/2)}\\ &= (-1)^{(\sum_{i=1}^{n}(p_i-1)/2)((q_1\cdots q_m-1)/2)}\\ &= (-1)^{(\sum_{i=1}^{n}(p_i-1)/2)((a-1)/2)}\\ &= (-1)^{((b-1)/2)((a-1)/2)}.\end{aligned}$$

□

Lema 1.2.3. *Existe una cantidad infinita de primos de la forma* $4k+3$.

Demostración: Supongamos que existe una cantidad finita de primos de esta forma, los cuales son $p_1 = 7, p_2 = 11, \ldots, p_n$, todos ellos diferentes de 3. Entonces existe q primo positivo de la forma $4k+3$ tal que $q|(4p_1p_2\cdots p_n+3)$, donde además $q \neq p_i\ \forall i$. De aquí sigue el resultado. □

Ahora veremos una aplicación para el símbolo de Jacobi.

Teorema 1.2.2. *Sea* $a \in \mathbb{Z}$ *tal que* a *no es un cuadrado, entonces existe una infinidad de primos para los cuales* a *no es un residuo cuadrático.*

Demostración: Por la Ley de Reciprocidad Cuadrática y el Lema 1.2.3, el resultado se tiene para $a = -1$. Por lo tanto, suponemos que $a \neq 0, 1, -1$. Ahora bien, supongamos que $l_1, l_2, \ldots, l_m$ (este conjunto puede ser vacío) son todos los primos para los cuales a no es un residuo cuadrático y $a = \pm 2^e p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ donde los p_i son primos distintos impares, además supongamos que α_n es impar. Por el Teorema Chino del Residuo, podemos hallar $b > 2$ tal que

$$\begin{aligned}b &\equiv 1 \pmod 8,\\ b &\equiv 1 \pmod{l_i}, \text{ para } i = 1, 2, \ldots, m,\\ b &\equiv 1 \pmod{p_j}, \text{ para } j = 1, 2, \ldots, n-1, \text{ y}\\ b &\equiv r \pmod{p_n}, \text{ con } (r/p_n) = -1.\end{aligned}$$

Sea $b = q_1q_2\cdots q_k$ la descomposición en primos de b. Entonces, por la Proposición 1.2.4, tenemos

$$\begin{aligned}(a/b) &= (2^e/b)(p_1/b)^{\alpha_1}(p_2/b)^{\alpha_2}\cdots(p_n/b)^{\alpha_n}\\ &= (b/p_1)^{\alpha_1}(b/p_2)^{\alpha_2}\cdots(b/p_n)^{\alpha_n}\\ &= (1/p_1)^{\alpha_1}(1/p_2)^{\alpha_2}\cdots(r/p_n)^{\alpha_n}\\ &= -1.\end{aligned}$$

Por otro lado, $(a/b) = (a/q_1)(a/q_2)\cdots(a/q_k)$, por lo que existe $1 \leq j \leq k$ tal que $(a/q_j) = -1$, con $q_j \neq l_1, l_2, \ldots, l_m$.

Ahora, supongamos que α_i es par $\forall i$, ó bien, posiblemente se carece de primos impares divisores de a. Cualesquiera que sea el caso, tomemos

$(a) : b = 8l_1\cdots l_m + 7$ con $l_1, \cdots, l_m \neq 7$, si $a < 0$ (notemos que $31 \in \{l_1, \ldots, l_m\}$), y
$(b) : b = 8l_1\cdots l_m + 3$ con $l_1, \cdots, l_m \neq 7$, si $a > 0$ (notemos que $11 \in \{l_1, \ldots, l_m\}$).

Para el inciso (a) tenemos $(a/b) = (-2^e/b) = (-1/b)(2/b)^e = -1$, luego existe $1 \leq j \leq k$ tal que $(a/q_j) = -1$, con $q_j \neq 7, l_1, l_2, \ldots, l_m$. Para el inciso (b) basta notar que e es impar y proceder de forma similar. □

Si p y q son primos positivos impares, entonces $p \equiv q \pmod 4$ ó $p \equiv -q \pmod 4$. En base a esto, daremos una equivalencia para la Ley de la Reciprocidad Cuadrática.

Proposición 1.2.5. *Sean p y q primos distintos impares positivos y $a \geq 1$ un número entero. Entonces, Las siguientes condiciones son equivalentes:*

(a) $(p/q) = (q/p)(-1)^{((p-1)/2)((q-1)/2)}$;

(b) *Si* $p \equiv \pm q \pmod{4a}$, *entonces* $(a/p) = (a/q)$.

Demostración: Supongamos primero que se cumple (a), y tomemos a impar. Si $p \equiv q \pmod{4a}$, entonces $p \equiv q \pmod a$ y $p + q - 2 \equiv 2q - 2 \equiv 0 \pmod 4$, por lo tanto

$$\begin{aligned}(a/p) = (p/a)(-1)^{((a-1)/2)((p-1)/2)} &= (q/a)(-1)^{((a-1)/2)((p-1)/2)}\\ &= (a/q)(-1)^{((a-1)/2)((p+q-2)/2)}\\ &= (a/q).\end{aligned}$$

Si $p \equiv -q \pmod{4a}$, entonces $p \equiv -q \pmod a$ y $p + q \equiv 0 \pmod 4$, por lo tanto

$$\begin{aligned}(a/p) &= (p/a)(-1)^{((a-1)/2)((p-1)/2)} = (-q/a)(-1)^{((a-1)/2)((p-1)/2)} \\ &= (q/a)(-1)^{((a-1)/2)((p+1)/2)} = (a/q)(-1)^{((a-1)/2)((p+q)/2)} \\ &= (a/q).\end{aligned}$$

Si a fuera par, entonces $p \equiv \pm q \pmod 8$, luego $(2/p) = (2/q)$, por lo tanto $(a/p) = (a/q)$.

Supongamos ahora que se cumple (b). Tomemos $p > q$ y a tal que $4a = p \pm q$. Si $4a = p + q$, entonces

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) \\ &= \left(\frac{4a-p}{p}\right) = \left(\frac{q}{p}\right) \ .\end{aligned}$$

Debido a que $p + q \equiv 0 \pmod 4$, se tiene que p ó $q \equiv 1 \pmod 4$, de aquí se tiene el resultado.

Si $4a = p - q$, de forma similar que el caso anterior, obtenemos

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

Debido a que $p - q \equiv 0 \pmod 4$, entonces $p \equiv q \pmod 4$, de aqui se tiene el resultado. □

Para ilustrar este resultado tomemos $p = 223$ y $q = 3$, entonces $223 \equiv 3 \pmod{4(11)}$, luego $(11/223) = (11/3) = (2/3) = -1$.

Capítulo 2

Sumas cuadráticas de Gauss

2.1. Números algebraicos y enteros algebraicos

Definición 2.1.1. *Se dice que un número complejo α es un* ***número algebraico*** *si existe un polinomio $f \in \mathbb{Q}[X]$, no cero, tal que α es raíz de f.*
Se dice que un número complejo ω es un ***entero algebraico*** *si existe un $g \in \mathbb{Z}[X]$ mónico tal que ω es raíz de g.*

Proposición 2.1.1. *Si $r \in \mathbb{Q}$ es un entero algebraico, entonces $r \in \mathbb{Z}$.*

Demostración: Sea $r = \dfrac{c}{d}$ un número racional, con $(c,d) = 1$, y $X^n + b_1 X^{n-1} + \cdots + b_n \in \mathbb{Z}[X]$ tal que $\left(\dfrac{c}{d}\right)^n + b_1 \left(\dfrac{c}{d}\right)^{n-1} + \cdots + b_n = 0$. Multiplicando por d^n la igualdad anterior, obtenemos que $c^n + b_1 c^{n-1} d + \cdots + b_n d^n = 0$, luego $d \mid c^n$, y como $(c,d) = 1$, entonces $d = \pm 1$, por lo tanto $r \in \mathbb{Z}$. □

Definición 2.1.2. *Sea $V \subset \mathbb{C}$ no vacío. Decimos que V es un* ***módulo sobre*** *$\mathbb{Q}$, o simplemente* ***$\mathbb{Q}$-módulo*** *si existen elementos $\gamma_1, \gamma_2, \ldots, \gamma_l \in V$ tales que*

$$V = \left\{ \sum_{i=1}^{l} r_i \gamma_i \mid r_1, r_2, \ldots, r_l \in \mathbb{Q} \right\}.$$

Si V es un $\mathbb{Q}$-módulo generado por los elementos $\gamma_1, \gamma_2, \ldots, \gamma_l$, entonces escribimos esta condición por $V = \langle \gamma_1, \gamma_2, \ldots, \gamma_l \rangle$. Notemos que, en estas condiciones, V es un espacio vectorial sobre $\mathbb{Q}$ de dimensión finita.

Proposición 2.1.2. *Sea $V = \langle \gamma_1, \gamma_2, \ldots, \gamma_l \rangle$ un $\mathbb{Q}$-módulo, y sea $\alpha \in \mathbb{C}$ tal que $\alpha\gamma \in V,\ \forall \gamma \in V$. Entonces, α es un número algebraico.*

Demostración: Como $\alpha\gamma_i \in V,\ \forall i = 1, 2, \ldots, l$, existen $a_{i1}, a_{i2}, \ldots, a_{il} \in \mathbb{Q}$ tales que $\alpha\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$. Luego, $\det(a_{ij} - \delta_{ij}\alpha) = 0$, donde δ_{ij} es la delta de Kronecker. Desarrollando el determinante notamos que α satisface un polinomio mónico de grado l con coeficientes en $\mathbb{Q}$. Por lo tanto, α es un número algebraico. □

La siguiente proposición es un resultado bien conocido.

Proposición 2.1.3. *El conjunto de números algebraicos forma un subcampo de $\mathbb{C}$.*

Demostración: [2], Chapter V, Section 1, Theorem 1.14, pag. 238. □

Exactamente el campo de los números algebraicos es la **cerradura algebraica de $\mathbb{Q}$ en $\mathbb{C}$**.

Definición 2.1.3. *Sea $W \subset \mathbb{C}$ no vacío. Decimos que W es un **módulo sobre** $\mathbb{Z}$, o simplemente $\mathbb{Z}$-**módulo**, si existen elementos $\gamma_1, \gamma_2, \ldots, \gamma_l \in W$ tales que*

$$W = \left\{ \sum_{i=1}^{l} d_i\gamma_i \mid d_1, d_2, \ldots, d_l \in \mathbb{Z} \right\}.$$

Proposición 2.1.4. *Sean W un $\mathbb{Z}$-módulo y $\omega \in \mathbb{C}$ tal que $\omega\gamma \in W,\ \forall \gamma \in W$. Entonces, ω es un entero algebraico.*

Demostración: La demostración es similar a la de la Proposición 2.1.2. □

Proposición 2.1.5. *El conjunto de enteros algebraicos forma un subanillo de $\mathbb{C}$.*

Demostración: Sean α y β enteros algebraicos. Veamos que $\alpha\beta$ y $\alpha+\beta$ son enteros algebraicos. Sean $f, g \in \mathbb{Z}[X]$ polinomios mónicos, con $\text{grad}(f) = n$ y $\text{grad}(g) = m$, tales que $f(\alpha) = 0$ y $g(\beta) = 0$. Si $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, entonces $f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Sea W el $\mathbb{Z}$-módulo generado por los elementos $\alpha^i\beta^j$, con $0 \leq i < n$ y $0 \leq j < m$. Puesto que $\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_0$ (una expresión similar se puede obtener para β^m utilizando el polinomio g), se tiene que $\alpha\beta\alpha^i\beta^j \in W$ y $(\alpha + \beta)\alpha^i\beta^j \in W$. Así pues, tenemos que el resultado sigue de la Proposicion 2.1.4. □

En lo sucesivo, denotaremos por Ω al anillo de enteros algebraicos, el cual es una extensión de $\mathbb{Z}$. Además, si $\omega_1, \omega_2, \gamma \in \Omega$, entonces decimos que ω_1 **es congruente con** ω_2 **módulo** γ, si existe $\alpha \in \Omega$ tal que $\omega_1 - \omega_2 = \alpha\gamma$, lo cual escribiremos $\omega_1 \equiv \omega_2 \pmod{\gamma}$. Es fácil verificar, al aplicar la Proposición 2.1.1, que si $\omega_1, \omega_2, \gamma \in \mathbb{Z}$ y $\gamma \neq 0$, entonces $\alpha \in \mathbb{Z}$.

Proposición 2.1.6. *Sean $\omega_1, \omega_2 \in \Omega$, y sea $p \in \mathbb{Z}$ un número primo. Entonces, $(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \pmod{p}$.*

Demostración: Tenemos que

$$(\omega_1 + \omega_2)^p = \sum_{i=0}^{p} \binom{p}{i} \omega_1^{p-i} \omega_2^i \ .$$

Para obtener el resultado, basta notar que $p | \binom{p}{i}$ para $i = 1, \ldots, p-1$, y que Ω es un anillo. □

2.2. El caracter cuadrático de 2

En el capítulo anterior, demostramos que $(2/p) = (-1)^{(p^2-1)/8}$ con $p \in \mathbb{Z}$ primo impar, en esta parte presentaremos otra demostración de dicha igualdad.

Sean $\zeta = e^{2\pi i/8}$ y $\tau = \zeta + \zeta^{-1}$; notemos que $\zeta = \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$ y $\zeta^{-1} = \dfrac{\sqrt{2}}{2} - \dfrac{\sqrt{2}}{2}i$, entonces $\tau = \sqrt{2}$. Además, podemos expresar

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

Puesto que $\zeta, \zeta^{-1} \in \Omega$, se tiene que

$$\begin{aligned} \zeta^p + \zeta^{-p} &\equiv 2^{(p-1)/2}\tau \pmod{p} \\ &\equiv (2/p)\tau \pmod{p}. \end{aligned}$$

Supóngase que $p \equiv \pm 1 \pmod 8$. Debido a que $\zeta^8 = 1$, se tiene que $\zeta^p + \zeta^{-p} = \tau$. Por otro lado, si $p \equiv \pm 3 \pmod 8$, como $\zeta^3 = -\zeta^{-1}$ y $\zeta^{-3} = -\zeta$, entonces tenemos que $\zeta^p + \zeta^{-p} = -\tau$. Por lo tanto,

$$(-1)^{(p^2-1)/8}\tau \equiv (2/p)\tau \pmod{p},$$

lo cual implica que

$$(-1)^{(p^2-1)/8}\tau^2 \equiv (2/p)\tau^2 \pmod{p},$$

es decir

$$2(-1)^{(p^2-1)/8} \equiv 2(2/p) \pmod{p}$$

y, en consecuencia,

$$(-1)^{(p^2-1)/8} \equiv (2/p) \pmod{p}.$$

2.3. Sumas cuadráticas de Gauss

Hagamos $\zeta = e^{2\pi i/p}$, con p primo impar. Además, todas las sumas consideradas serán de cero a $p-1$.

Lema 2.3.1. *Se tiene que* $\sum_{t=0}^{p-1} \zeta^{at} = p$ *si* $a \equiv 0 \pmod{p}$*, en caso contrario tendremos que* $\sum_{t=0}^{p-1} \zeta^{at} = 0$.

Demostración: Si $a \equiv 0 \pmod{p}$ entonces $\zeta^{at} = 1$ para todo t, luego $\sum_t \zeta^{at} = p$. Por otro lado, si $a \not\equiv 0 \pmod{p}$, entonces $\zeta^a \neq 1$, además $(\zeta^a - 1)\left(\sum_t \zeta^{at}\right) = \zeta^{ap} - 1 = 0$, por lo tanto $\sum_t \zeta^{at} = 0$. □

Lema 2.3.2. *Se tiene que* $\sum_t (t/p) = 0$*, donde* (t/p) *es el símbolo de Legendre.*

Demostración: Se sigue del hecho de que hay tantos residuos como no residuos cuadráticos módulo p (ver Corolario 1.1.1). □

Definición 2.3.1. *Bajo las notaciones anteriores,* $g_a = \sum_{t=0}^{p-1} (t/p)\zeta^{at}$ *es llamada una* ***suma cuadrática de Gauss****. Además denotemos* $g := g_1 = \sum_t (t/p)\zeta^t$.

Proposición 2.3.1. *Tenemos que* $g_a = (a/p)g$.

Demostración: Si $a \equiv 0 \pmod{p}$, entonces $g_a = 0$, por el lema anterior. Por lo tanto, $g_a = (a/p)g$. Si $a \not\equiv 0 \pmod{p}$ entonces at recorre el sistema de residuos mód p, luego $(a/p)g_a = (a/p)\sum_t (t/p)\zeta^{at} = \sum_t (at/p)\zeta^{at} = \sum_x (x/p)\zeta^x = g$. Por lo tanto, $g_a = (a/p)g$. □

Proposición 2.3.2. *Se tiene la relación* $g^2 = (-1)^{(p-1)/2}p$.

Demostración: Para esta demostración tenemos que desarrollar $\sum_a g_a g_{-a}$ de dos formas distintas.

Para el primer desarollo, tenemos que si $a = 0$, entonces $g_a g_{-a} = 0$. En caso contrario, tenemos que $g_a g_{-a} = (a/p)g(-a/p)g = (-1/p)g^2 = (-1)^{(p-1)/2}g^2$, por lo tanto $\sum_a g_a g_{-a} = (-1)^{(p-1)/2}(p-1)g^2$.

Para el segundo desarrollo, tenemos que

$$g_a g_{-a} = \sum_x (x/p)\zeta^{ax} \sum_y (y/p)\zeta^{-ay} = \sum_x \sum_y (x/p)(y/p)\zeta^{a(x-y)},$$

entonces

$$\begin{aligned} \sum_a g_a g_{-a} &= \sum_a \sum_x \sum_y (x/p)(y/p)\zeta^{a(x-y)} \\ &= \sum_x \sum_y (x/p)(y/p) \left[\sum_a \zeta^{a(x-y)} \right] \end{aligned}$$

y debido a que $x - y \equiv 0 \pmod{p}$ si y sólo si $x = y$, se tiene que $\sum_a \zeta^{a(x-y)} = 0$ si $x \neq y$, y $\sum_a \zeta^{a(x-y)} = p$ si $x = y$. Por lo tanto,

$$\sum_a g_a g_{-a} = \sum_t (t^2/p)p = (p-1)p.$$

Igualando ambos desarrollos, tenemos $(-1)^{(p-1)/2}(p-1)g^2 = (p-1)p$, y despejando g^2 obtenemos el resultado. □

Enseguida demostraremos la ley de la reciprocidad cuadrática, la cual asegura que $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$, con p y q primos impares.

$$
\begin{aligned}
(-1)^{((p-1)/2)((q-1)/2)}p^{(q-1)/2}g &\equiv g^{2((q-1)/2)}g \pmod{q} && \text{(Por la Proposición 2.3.2)}\\
&\equiv g^q \pmod{q}\\
&\equiv \left(\sum_t (t/p)\zeta^t\right)^q \pmod{q}\\
&\equiv \sum_t (t/p)^q\zeta^{qt} \pmod{q}\\
&\equiv g_q \pmod{q}\\
&\equiv (q/p)g \pmod{q}, && \text{(Por la Proposición 2.3.1)}
\end{aligned}
$$

con lo cual

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

donde $g^2 = (-1)^{(p-1)/2}p$; luego,

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

en consecuencia,

$$(-1)^{((p-1)/2)((q-1)/2)}(p/q) \equiv (q/p) \pmod{q}.$$

Por lo tanto, $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

2.4. Signo de las sumas cuadráticas de Gauss

Si p es un primo positivo impar, por la Proposición 2.3.2, tenemos $g^2 = (-1)^{(p-1)/2}p$, es decir,

$$g = \begin{cases} -\sqrt{p} \text{ ó } \sqrt{p} & \text{si } p \equiv 1 \pmod{4};\\ -i\sqrt{p} \text{ ó } i\sqrt{p} & \text{si } p \equiv 3 \pmod{4}, \end{cases}$$

por lo que en esta sección determinaremos cuál es el signo de g.

Proposición 2.4.1. *Se tiene que* $\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(p-1)/2}p$, *donde* $\zeta = e^{2\pi i/p}$.

Demostración: Debido a que $X^p - 1 = \prod_{k=0}^{p-1}(X - \zeta^k)$, tenemos que

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{k=1}^{p-1}(X - \zeta^k),$$

el cual es un polinomio irreducible sobre $\mathbb{Q}[X]$. Tomando $X = 1$, se tiene que $p = \prod_{k=1}^{p-1}(1 - \zeta^k)$. Veamos primero que $\{\pm(4k-2) \mid k = 1, 2, \ldots, (p-1)/2\}$ es un conjunto completo de representantes no cero módulo p. Supongamos que $p \mid \pm(4l-2)$ para algún $l \in \{1, 2, \ldots, (p-1)/2\}$; debido a que $(4l-2) < 2p$, se tiene que $p = 4l-2$, es decir, $2|p$ lo cual es una contradicción. Además, si $(4l-2) \equiv \pm(4m-2) \pmod{p}$, tenemos los siguientes dos casos:

(a): $(4l-2) - (4m-2) = 4(l-m) \equiv 0 \pmod{p}$
(b): $(4l-2) + (4m-2) = 4(l+m-1) \equiv 0 \pmod{p}$

Puesto que $|l-m|,\ |l+m-1| < p$, para el primer caso obtenemos que $l = m$, y para el segundo caso surge una contradicción.

Usando lo anteriormente demostrado, obtenemos

$$\begin{aligned} p = \prod_{k=1}^{p-1}(1-\zeta^k) &= \prod_{k=1}^{(p-1)/2}(1-\zeta^{4k-2})(1-\zeta^{-(4k-2)}) \\ &= \prod_{k=1}^{(p-1)/2}(\zeta^{-(2k-1)} - \zeta^{2k-1})(\zeta^{2k-1} - \zeta^{-(2k-1)}) \\ &= (-1)^{(p-1)/2}\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-(2k-1)})^2 \end{aligned}$$

□

Proposición 2.4.2.

$$\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \sqrt{p} & si\ p \equiv 1 \pmod 4; \\ i\sqrt{p} & si\ p \equiv 3 \pmod 4 \end{cases}$$

Demostración: Basta analizar el signo de $\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1} - \zeta^{-(2k-1)})$. Para ello, notemos que

$$\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1}-\zeta^{-(2k-1)}) = i^{(p-1)/2}2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\operatorname{sen}\frac{(4k-2)\pi}{p}\ .$$

Si $p \equiv 1 \pmod 4$, entonces $\pi < \dfrac{4k-2}{p}\pi < 2\pi$ para $k = (p+3)/4, \ldots, (p-1)/2$, luego el signo de $\displaystyle\prod_{k=1}^{(p-1)/2}\operatorname{sen}\frac{(4k-2)\pi}{p}$ es $(-1)^{(p-1)/4}$. Por lo tanto el signo de $i^{(p-1)/2}2^{(p-1)/2}\displaystyle\prod_{k=1}^{(p-1)/2}\operatorname{sen}\frac{(4k-2)\pi}{p}$ es

$$(i)^{2(p-1)/4}(-1)^{(p-1)/4} = (-1)^{(p-1)/2} = 1.$$

Si $p \equiv 3 \pmod 4$, entonces $\pi < \dfrac{4k-2}{p}\pi < 2\pi$ para $k = (p+5)/4, \ldots, (p-1)/2$, luego el signo de $\displaystyle\prod_{k=1}^{(p-1)/2}\operatorname{sen}\frac{(4k-2)\pi}{p}$ es $(-1)^{(p-3)/4}$. Por lo tanto, el signo de $i^{(p-1)/2}2^{(p-1)/2}\displaystyle\prod_{k=1}^{(p-1)/2}\operatorname{sen}\frac{(4k-2)\pi}{p}$ es

$$(i)^{(p-1)/2}(-1)^{(p-3)/4} = i(-1)^{(p-3)/4}(-1)^{(p-3)/4} = i.$$

□

Proposición 2.4.3. *Sean* $f(z) = \displaystyle\sum_{n=0}^{\infty} a_n/n!\ z^n$ *y* $g(z) = \displaystyle\sum_{n=0}^{\infty} b_n/n!\ z^n$ *series de potencias con* a_n *y* b_n *enteros, tales que* $p|a_i$ *para* $i = 1, 2, \ldots, p-1$. *Hagamos* $f(z)g(z) = \displaystyle\sum_{n=0}^{\infty} c_n\ z^n$, *entonces para* $t = 1, 2, \ldots, p-1$, $c_t = p(A_t/B_t)$, *con* A_t *y* B_t *enteros tales que* $p \nmid B_t$.

Demostración: Notemos que $c_t = \displaystyle\sum_{r+s=t}(a_r/r!)(b_s/s!)$, para $t = 0, 1 \ldots$. Debido a que $t < p$, entonces $r < p$ y $s < p$, luego $p|a_r$, pero $p \nmid r!$ y $p \nmid s!$. Por lo tanto existe A_t y B_t enteros tales que $c_t = p(A_t/B_t)$ □

Proposición 2.4.4. *Si* p *es un primo positivo impar, entonces*

$$g = \sum_{t=0}^{p-1}(t/p)\zeta^t = \begin{cases} \sqrt{p} & \text{si } p \equiv 1 \pmod 4; \\ i\sqrt{p} & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Demostración: Definamos $f(x) = \sum_{t=0}^{p-1}(t/p)x^t - \epsilon \prod_{k=1}^{(p-1)/2}(x^{2k-1} - x^{p-(2k-1)})$, donde ϵ es el signo de g. Por lo tanto, basta demostrar que $\epsilon = 1$.

Notemos que $f(1) = 0$ y por la Proposición 2.4.2,$f(\zeta) = 0$. Debido a que $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ es irreducible en $\mathbb{Q}[x]$ y $g(\zeta) = 0$, entonces $g(x)|f(x)$. De igual forma tenemos que $x - 1|f(x)$. Por lo tanto $g(x)(x-1) = x^p - 1|f(x)$, ya que $g(x)$ y $x - 1$ son primos relativos. Luego existe $h(x) \in \mathbb{Q}[x]$ tal que,

$$f(x) = (x^p - 1)h(x); \tag{1}$$

y debido a que $f(x)$, $h(x) \in \mathbb{Z}[x]$ son mónicos, entonces $h(x) \in \mathbb{Z}$. Luego, tomando $x = e^z$ en (1), tenemos

$$\sum_{t=0}^{p-1}(t/p)e^{zt} - \epsilon \prod_{k=1}^{(p-1)/2}(e^{z(2k-1)} - e^{z(p-(2k-1))}) = (e^{zp} - 1)g(e^z). \tag{2}$$

Notemos además que,

$$e^{z(2k-1)} - e^{z(p-(2k-1))} = (4k - p - 2)z + \sum_{n=2}^{\infty} \frac{(2k-1)^n - (p-(2k-1))^n}{n!} z^n.$$

Entonces el coeficiente del término $z^{(p-1)/2}$ del lado derecho de (2) esta dado por,

$$\sum_{t=0}^{p-1}(t/p)\frac{t^{(p-1)/2}}{((p-1)/2)!} - \epsilon \prod_{k=1}^{(p-1)/2}(4k - p - 2),$$

y por la Proposición 2.4.3 tenemos que el coeficiente del término $z^{(p-1)/2}$ del lado izquierdo de (2) esta dado por, $p(A/B)$, con A y B enteros, tal que $p \nmid B$. Entonces,

$$\sum_{t=0}^{p-1}(t/p)\frac{t^{(p-1)/2}}{((p-1)/2)!} - \epsilon \prod_{k=1}^{(p-1)/2}(4k - p - 2) = p(A/B),$$

y multiplicando por $B((p-1)/2)!$, obtenemos

$$\sum_{t=0}^{p-1}(t/p)t^{(p-1)/2} \equiv \epsilon((p-1)/2)! \prod_{k=1}^{(p-1)/2}(4k-p-2) \pmod{p}$$

$$\sum_{t=0}^{p-1}(t/p)(t/p) \equiv \epsilon 2\cdot 4\cdots(p-1) \prod_{k=1}^{(p-1)/2}(2k-1) \pmod{p}$$

$$(p-1) \equiv \epsilon(p-1)! \pmod{p}$$

$$-1 \equiv \epsilon(p-1)! \pmod{p}$$

y finalmente por el Teorema de Wilson tenemos que $-1 \equiv -\epsilon \pmod{p}$, por lo tanto $\epsilon = 1$.

□

Capítulo 3

Sumas de Gauss y sumas de Jacobi

3.1. Caracteres multiplicativos

Denotemos por $\mathbb{F}_p$ al campo finito de p elementos.

Definición 3.1.1. *Un* ***caracter multiplicativo*** *en* $\mathbb{F}_p$ *es una función* $\chi : {\mathbb{F}_p}^* \to \mathbb{C}^*$ *tal que* $\chi(ab) = \chi(a)\chi(b)$.

Un ejemplo de este tipo de funciones es el símbolo de Legendre (a/p), y el **caracter multiplicativo trivial** definido como $\epsilon(a) = 1$ para todo $a \in {\mathbb{F}_p}^*$.

También, podemos extender un caracter multiplicativo a todo $\mathbb{F}_p$ de la siguiente forma: si $\chi \neq \epsilon$, entonces $\chi(0) = 0$, en caso contrario $\epsilon(0) = 1$.

Notemos que $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$, entonces $\chi(1) = 1$. Por otro lado, si $a \in {\mathbb{F}_p}^*$, entonces $a^{p-1} = 1$, y aplicando χ obtenemos que $\chi(a)^{p-1} = \chi(1) = 1$, es decir, $\chi(a)$ es una raíz $p-1$-ésima de la unidad. Además, $1 = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$, luego $\chi(a^{-1}) = \chi(a)^{-1}$. Todo esto se resume en la siguiente proposición.

Proposición 3.1.1. *Sean* χ *un caracter multiplicativo y* $a \in {\mathbb{F}_p}^*$. *Entonces,*

(a) $\chi(1) = 1$.

(b) $\chi(a)$ *es una raíz* $p-1$*-ésima de la unidad.*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$. □

Proposición 3.1.2. *Sea χ un caracter multiplicativo. Si $\chi \neq \epsilon$, entonces* $\sum_t \chi(t) = 0$. *En caso contrario,* $\sum_t \epsilon(t) = p$.

Demostración: Si $\chi \neq \epsilon$, entonces existe $a \in {\mathbb{F}_p}^*$ tal que $\chi(a) \neq 1$. Denotemos por $T = \sum_t \chi(t)$; entonces,

$$\chi(a)T = \sum_t \chi(at) = T,$$

ya que at recorre todo el sistema de residuos mód p. Por lo tanto, $T = 0$. No es difícil demostrar que $\sum_t \epsilon(t) = p$. □

El conjunto de caracteres multiplicativos en $\mathbb{F}_p$ forma un grupo con la siguiente operación: si χ y λ son caracteres multiplicativos en $\mathbb{F}_p$, entonces $\chi\lambda$ es tal que $\chi\lambda(a) = \chi(a)\lambda(a)$. Además, la identidad es ϵ y χ^{-1} es tal que $\chi^{-1}(a) = \chi(a)^{-1}$.

Proposición 3.1.3. *El grupo de caracteres multiplicativos en $\mathbb{F}_p$ es cíclico de orden $p-1$. Además, si $a \in {\mathbb{F}_p}^*$ y $a \neq 1$, entonces existe un caracter multiplicativo χ tal que $\chi(a) \neq 1$.*

Demostración: Sea $g \in {\mathbb{F}_p}^*$ un generador de ${\mathbb{F}_p}^*$, entonces definimos el caracter multiplicativo λ tal que $\lambda(g^k) = e^{2\pi ik/(p-1)}$ para $k = 1, 2, \ldots, p-1$. Así, notemos que cualquier caracter χ está únicamente determinado por la imagen de g.

Demostremos primero que λ es el generador del grupo de caracteres multiplicativos. Si χ es un caracter arbitrario, entonces existe $l \in \{1, \ldots, p-1\}$ tal que $\chi(g) = e^{2\pi il/(p-1)}$ y, como $\lambda^l(g) = \lambda(g^l) = e^{2\pi il/(p-1)}$, tenemos que $\chi = \lambda^l$; además, es fácil notar que λ es de orden $p-1$.

Ahora, demostremos la segunda parte de la proposición. Como $a \neq 1$, entonces existe $l \in \{1, \ldots, p-2\}$ tal que $a = g^l$, por lo tanto $\lambda(a) = \lambda(g^l) = e^{2\pi il/(p-1)} \neq 1$. □

Corolario 3.1.1. *Si $a \in {\mathbb{F}_p}^*$, con $a \neq 1$, entonces* $\sum_\chi \chi(a) = 0$, *donde la suma es sobre todos los caracteres en $\mathbb{F}_p$.*

Demostración: Denotemos $T = \sum_\chi \chi(a)$ y tomemos λ dado en la demostración de la Proposición 3.1.3, entonces $\lambda(a) \neq 1$ y $\lambda(a)T = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a) = T$. Por lo tanto, $T = 0$. □

Proposición 3.1.4. *Si $a \in \mathbb{F}_p{}^*$, $n \mid (p-1)$ y la ecuación $X^n = a$ no es soluble, entonces existe un caracter multiplicativo χ tal que $\chi(a) \neq 1$ y $\chi^n = \epsilon$.*

Demostración: De nuevo, sean g y λ dados en la demostración de la Proposición 3.1.3, entonces existe $l \in \{1, \ldots, p-2\}$ tal que $a = g^l$; además, $n \nmid l$ ya que de lo contrario la ecuación $X^n = a$ sería soluble. Demostremos que $\lambda^{(p-1)/n}$ es el caracter que estamos buscando. Notemos que $\lambda^{(p-1)/n}$ es de orden n y, además, $\lambda^{(p-1)/n}(a) = \lambda^{(p-1)/n}(g^l) = e^{2\pi i l/n} \neq 1$ ya que $n \nmid l$.

□

Si $a \in \mathbb{F}_p$ y $m \in \mathbb{N}$, denotemos por $N(X^m = a)$ al número de soluciones de la ecuación $X^m = a$.

Proposición 3.1.5. *Si $a \in \mathbb{F}_p$ y $n \mid (p-1)$, entonces $N(X^n = a) = \sum_{\chi^n = \epsilon} \chi(a)$, donde la suma es sobre todos los caracteres tales que $\chi^n = \epsilon$.*

Demostración: Denotemos por $T = \sum_{\chi^n = \epsilon} \chi(a)$ y sea $\chi = \lambda^{(p-1)/n}$. Entonces, $\epsilon, \chi, \chi^2, \ldots, \chi^{n-1}$ son todos los caracteres de orden dividiendo a n. Para el caso $a = 0$, el resultado el fácil de obtener. Para el caso $a \neq 0$, y suponiendo que $X^n = a$ es soluble, se tiene que existe $b \in \mathbb{F}_p{}^*$ tal que $b^n = a$, luego $T = \sum_{k=1}^{n} \chi^k(a) = \sum_{k=1}^{n} \chi^k(b^n) = n$, por lo tanto $T = N(X^n = a)$. Ahora, supongamos que $X^n = a$ no es soluble, entonces $a \neq 1$; luego, por la Proposición 3.1.4, sabemos que $\chi(a) \neq 1$ y $\chi^n = \epsilon$, entonces $\chi(a)T = \chi(a)\sum_{k=1}^{n} \chi^k(a) = \sum_{k=1}^{n} \chi(a)\chi^k(a) = \sum_{k=2}^{n+1} \chi^k(a) = T$, por lo tanto $T = 0$. □

Como caso especial, notemos que $2 \mid (p-1)$ y los únicos dos caracteres de orden diviendo a 2 son ϵ y (a/p) (símbolo de Legendre). Por lo tanto, $N(X^2 = a) = 1 + (a/p)$.

3.2. Sumas de Gauss

Enseguida daremos una generalización de las sumas cuadráticas de Gauss. Recordemos que las sumas son de 0 a $p-1$, y que $\zeta = e^{2\pi i/p}$ con p primo impar.

Definición 3.2.1. *Sean χ un caracter multiplicativo y $a \in \mathbb{F}_p$. Entonces, definimos $g_a(\chi) = \sum_t \chi(t)\zeta^{at}$ la cual es llamada* ***suma de Gauss en*** $\mathbb{F}_p$ ***perteneciente al caracter*** χ.

Denotemos $g_1(\chi) = \sum_t \chi(t)\zeta^t$ por $g(\chi)$.

Proposición 3.2.1. *Sean χ un caracter multiplicativo y $a \in \mathbb{F}_p$. Entonces,*
(a) $g_a(\chi) = p$ *si* $\chi = \epsilon$ *y* $a = 0$.
(b) $g_a(\chi) = 0$ *si* $\chi = \epsilon$ *y* $a \neq 0$.
(c) $g_a(\chi) = 0$ *si* $\chi \neq \epsilon$ *y* $a = 0$.
(e) $g_a(\chi) = \chi(a^{-1})g(\chi)$ *si* $\chi \neq \epsilon$ *y* $a \neq 0$.

Demostración: No es difícil demostrar los primeros tres incisos. Así que nos enfocaremos en el último inciso. Tenemos que

$$\begin{aligned}\chi(a)g_a(\chi) &= \chi(a)\sum_t \chi(t)\zeta^{at} \\ &= \sum_t \chi(at)\zeta^{at} \\ &= \sum_y \chi(y)\zeta^y \\ &= g(\chi)\end{aligned}$$

Por lo tanto, $g_a(\chi) = \chi(a^{-1})g(\chi)$. □

Proposición 3.2.2. *Si $\chi \neq \epsilon$, entonces $|g(\chi)| = \sqrt{p}$.*

Demostración: Para esta demostración, tenemos que desarrollar $\sum_a g_a(\chi)\overline{g_a(\chi)}$ de dos formas distintas.

Para el primer desarollo tenemos que si $a = 0$, entonces $g_0(\chi)\overline{g_0(\chi)} = 0$. En caso contrario, tenemos que $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} = g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. Por lo tanto, $\sum_a g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2$.

Para el segundo desarrollo tenemos que

$$g_a(\chi)\overline{g_a(\chi)} = \sum_x \chi(x)\zeta^{ax} \sum_y \overline{\chi(y)}\zeta^{-ay} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{a(x-y)},$$

con lo cual

$$\begin{aligned}\sum_a g_a(\chi)\overline{g_a(\chi)} &= \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{a(x-y)} \\ &= \sum_x \sum_y \chi(x)\overline{\chi(y)} \left[\sum_a \zeta^{a(x-y)}\right].\end{aligned}$$

Debido a que $x - y \equiv 0 \pmod{p}$ si y sólo si $x = y$, entonces $\sum_a \zeta^{a(x-y)} = 0$ si $x \neq y$, y $\sum_a \zeta^{a(x-y)} = p$ si $x = y$. Por lo tanto,

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_t \chi(t)\overline{\chi(t)}p = (p-1)p.$$

Igualando ambos desarrollos, tenemos que $(p-1)|g(\chi)|^2 = (p-1)p$, y despejando $|g(\chi)|$ obtenemos el resultado. □

A manera de observación tenemos:

$$\begin{aligned}p &= g(\chi)\overline{g(\chi)} \\ &= g(\chi)\overline{\sum_t \chi(t)\zeta^t} \\ &= g(\chi)\sum_t \chi^{-1}(t)\zeta^{-t} \\ &= g(\chi)\chi(-1)\sum_t \chi^{-1}(-t)\zeta^{-t} \text{(ya que } \chi(-1) = \chi^{-1}(-1) = \pm 1) \\ &= \chi(-1)g(\chi)g(\chi^{-1}).\end{aligned}$$

Es decir, $g(\chi)g(\chi^{-1}) = \chi(-1)p$. Además, si tomamos χ que sea el símbolo de Legendre, tenemos que $g^2 = (-1)^{(p-1)/2}p$, el cual ha sido probado con anterioridad.

3.3. Sumas de Jacobi

Definición 3.3.1. *Sean χ y λ caracteres multiplicativos en $\mathbb{F}_p$. Entonces, definimos $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$, la cual es llamada* ***suma de Jacobi****.*

Teorema 3.3.1. *Si χ y λ son caracteres multiplicativos no triviales, entonces*
(a) $J(\epsilon,\epsilon)=p$.
(b) $J(\epsilon,\chi)=0$.
(c) $J(\chi,\chi^{-1})=-\chi(-1)$.
(d) Si $\chi\lambda\neq\epsilon$, *entonces* $J(\chi,\lambda)=\dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Demostración: No es difícil demostrar los primeros dos incisos. Para el inciso (c) tenemos que

$$\begin{aligned} J(\chi,\chi^{-1}) &= \sum_{a+b=1}\chi(a)\chi^{-1}(b)=\sum_{a}\chi(a)\chi^{-1}(1-a) \\ &= \sum_{a,\ a\neq 1}\chi(a)\chi\left(\frac{1}{1-a}\right) \\ &= \sum_{a,\ a\neq 1}\chi\left(\frac{a}{1-a}\right). \end{aligned}$$

Además, si $c\in\mathbb{F}_p$, $c\neq -1$ y definimos $a=\dfrac{c}{1+c}$, entonces $\dfrac{a}{1-a}=c$, por lo tanto $\displaystyle\sum_{a,\ a\neq 1}\chi\left(\frac{a}{1-a}\right)=\sum_{c,\ c\neq -1}\chi(c)=-\chi(-1)$.

Para el inciso (d), tenemos que

$$g(\chi)g(\lambda)=\sum_{x}\chi(x)\zeta^{x}\sum_{y}\lambda(y)\zeta^{y}=\sum_{x,y}\chi(x)\lambda(y)\zeta^{x+y}=\sum_{t}\sum_{x+y=t}\chi(x)\lambda(y)\zeta^{t}.$$

Para $t=0$,

$$\sum_{x+y=t}\chi(x)\lambda(y)\zeta^{t}=\sum_{x+y=0}\chi(x)\lambda(y)=\sum_{x}\chi(x)\lambda(-x)=\lambda(-1)\sum_{x}\chi\lambda(x)=0.$$

Para $t\neq 0$, existen x' y y' tales que $x't=x$ y $y't=y$, luego

$$\begin{aligned} \sum_{x+y=t}\chi(x)\lambda(y)\zeta^{t} &= \sum_{x't+y't=t}\chi(x't)\lambda(y't)\zeta^{t}=\chi\lambda(t)\zeta^{t}\sum_{x'+y'=1}\chi(x')\lambda('t) \\ &= \chi\lambda(t)\zeta^{t}J(\chi,\lambda). \end{aligned}$$

Por lo tanto, $g(\chi)g(\lambda) = \sum_t \chi\lambda(t)\zeta^t J(\chi,\lambda) = g(\chi\lambda)J(\chi,\lambda)$. □

Corolario 3.3.1. *Si χ y λ son caracteres multiplicativos tales que $\chi\lambda \neq \epsilon$, entonces $|J(\chi,\lambda)| = \sqrt{p}$.*

Demostración: Del inciso (d) del Teorema 3.3.1, tenemos

$$|J(\chi,\lambda)| = \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} = \sqrt{p}\ .$$

□

Consideremos la ecuación $X^2 + Y^2 = 1$ en $\mathbb{F}_p$. Entonces,

$$\begin{aligned} N(X^2+Y^2=1) &= \sum_{a+b=1} N(X^2=a)N(Y^2=b) \\ &= \sum_{a+b=1} (1+(a/p))(1+(b/p)) \\ &= p + \sum_a (a/p) + \sum_b (b/p) + \sum_{a+b=1} (a/p)(b/p) \\ &= p + J(\chi,\chi) \ \text{ (donde } \chi \text{ es el símbolo de Legendre)} \\ &= p - \chi(-1) \ \text{ (ya que } \chi = \chi^{-1}) \\ &= p - (-1/p) \\ &= p - (-1)^{(p-1)/2} \end{aligned}$$

es decir, si $p \equiv 1 \pmod 4$, entonces $N(X^2+Y^2=1) = p-1$, y si $p \equiv 3 \pmod 4$, entonces $N(X^2+Y^2=1) = p+1$.

Ahora, consideremos la ecuación $X^3 + Y^3 = 1$ en $\mathbb{F}_p$. Entonces

$$N(X^3+Y^3=1) = \sum_{a+b=1} N(X^3=a)N(Y^3=b).$$

Si $p \equiv 2 \pmod 3$, entonces $N(X^3=a) = 1$ para toda $a \in \mathbb{F}_p$, ya que $(3, p-1) = 1$; por lo tanto, $N(X^3+Y^3=1) = p$. Si $p \equiv 1 \pmod 3$, entonces $3 \mid (p-1)$. Sea χ un caracter multiplicativo de orden 3, entonces ϵ, χ, χ^2 son todos los caracteres multiplicativos de orden diviendo a 3. Por lo tanto,

$$\begin{aligned}
N(x^3+y^3=1) &= \sum_{a+b=1}(1+\chi(a)+\chi^2(a))N(1+\chi(b)+\chi^2(b)) \\
&= p+\sum_{a+b=1}\chi(a)\chi(b)+\sum_{a+b=1}\chi^2(a)\chi(b) \\
&\quad +\sum_{a+b=1}\chi(a)\chi^2(b)+\sum_{a+b=1}\chi^2(a)\chi^2(b) \\
&= p+J(\chi,\chi)+J(\chi^2,\chi)+J(\chi,\chi^2)+J(\chi^2,\chi^2) \\
&= p+J(\chi,\chi)-\chi^2(-1)-\chi(-1)+J(\chi^2,\chi^2) \\
&= p+J(\chi,\chi)-2+J(\chi^2,\chi^2),
\end{aligned}$$

ya que $\chi(-1)=\chi(-1)^3=\chi^3(-1)=\epsilon(-1)=1$; pero como $\chi^2=\chi^{-1}=\overline{\chi}$, se tiene que

$$N(X^3+Y^3=1)=p+J(\chi,\chi)-2+J(\chi^2,\chi^2)=p-2+2\mathrm{Re}J(\chi,\chi).$$

Por lo tanto $|N(X^3+Y^3=1)-(p-2)|\leq 2|J(\chi,\chi)|=2\sqrt{p}$, lo cual nos indica que para valores muy grandes de p tendremos muchas soluciones de la ecuación. De hecho, siempre se tienen al menos seis soluciones debido a que $N(X^3=1)=3$ y $N(x^3=0)=1$.

Para $p\geq 19$, se tienen más de seis soluciones, ya que $N(X^3+Y^3=1)\geq p-2-2\sqrt{p}=(\sqrt{p}-1)^2-3>6$. Más adelante demostraremos que para $p=7$ ó $p=13$ sólo se tienen seis soluciones.

Proposición 3.3.1. *Si* $p\equiv 1 \pmod 4$*, entonces existen enteros* a *y* b *tales que* $a^2+b^2=p$*. Si* $p\equiv 1 \pmod 3$*, entonces existen enteros* a *y* b *tales que* $a^2-ab+b^2=p$*.*

Demostración: Para el primer caso, tenemos que $4\mid(p-1)$, luego existe un caracter multiplicativo χ en $\mathbb{F}_p$ de orden cuatro, es decir, $\chi(\mathbb{F}_p)=\{0,1,-1,i,-i\}$, así que existen enteros a y b tales que $J(\chi,\chi)=a+bi$. Por lo tanto, aplicando el Corolario 3.3.1, tenemos que $|J(\chi,\chi)|^2=a^2+b^2=p$. Para el segundo caso, tenemos que $3\mid(p-1)$, entonces existe un caracter multiplicativo χ en $\mathbb{F}_p$ de orden tres, es decir, $\chi(\mathbb{F}_p)=\{0,1,\omega,\omega^2\}$ donde $\omega=e^{2\pi i/3}=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$ y, tomando en cuenta que $\omega^2=-1-\omega$, entonces existen enteros a y b tales que $J(\chi,\chi)=a+b\omega$. Por lo tanto, $|J(\chi,\chi)|^2=a^2-ab+b^2=p$. □

Proposición 3.3.2. *Si $n \mid (p-1)$ y χ es un caracter multiplicativo de orden n, entonces*

$$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

Demostración: Por el Teorema 3.3.1, tenemos que $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$ y, multiplicando esta última igualdad por $g(\chi)$ y empleando de nuevo el Teorema 3.3.1, tenemos que $g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi) = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$.

Continuando con el proceso anterior, obtenemos que

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1});$$

multiplicando por $g(\chi)$ y tomando en cuenta que $\chi^{n-1} = \chi^{-1}$, concluimos que

$$\begin{aligned} g(\chi)^n &= J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1})g(\chi) \\ &= \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}). \end{aligned}$$

La última igualdad es debido a que anteriormente demostramos que si $\lambda \neq \epsilon$ es un caracter multiplicativo, entonces $g(\lambda)g(\lambda^{-1}) = \lambda(-1)p$. □

Corolario 3.3.2. *Si χ es un caracter multiplicativo cúbico , es decir, un caracter de orden tres, entonces $g(\chi)^3 = pJ(\chi,\chi)$.*

Demostración: Basta reducir el resultado de la Proposición 3.3.2 para el caso $n = 3$, y tomar en cuenta que

$$\chi(-1) = \chi((-1)^3) = \chi^3(-1) = 1.$$

□

Proposición 3.3.3. *Si $p \equiv 1 \pmod 3$, χ es un caracter multiplicativo cúbico y $J(\chi,\chi) = a + b\omega$, con a y b enteros, entonces $a \equiv -1 \pmod 3$ y $b \equiv 0 \pmod 3$.*

Demostración: Empleando congruencias en el anillo de enteros algebraicos obtenemos,

$$g(\chi)^3 = \left[\sum_t \chi(t)\zeta^t\right]^3 \equiv \sum_{t\neq 0} \chi(t)^3\zeta^{3t} \equiv \sum_{t\neq 0} \epsilon(t)\zeta^{3t} \equiv -1 \pmod 3.$$

Entonces, $g(\chi)^3 = pJ(\chi,\chi) \equiv J(\chi,\chi) \equiv -1 \pmod 3$, es decir,

$$a + b\omega \equiv -1 \pmod 3.$$

De forma análoga, se demuestra que $g(\chi^{-1})^3 \equiv -1 \pmod 3$, luego $g(\chi^{-1})^3 = pJ(\chi^{-1},\chi^{-1}) \equiv \overline{J(\chi,\chi)} \equiv -1 \pmod 3$, es decir,

$$a + b\overline{\omega} \equiv -1 \pmod 3.$$

Restando las dos congruencias, obtenemos $b(\omega - \overline{\omega}) \equiv 0 \pmod 3$, luego $b\sqrt{-3} \equiv 0 \pmod 3$; elevando al cuadrado obtenemos, $-3b^2 \equiv 0 \pmod 9$, por lo tanto $3 \mid b$ y, del hecho que $a + b\omega \equiv -1 \pmod 3$, obtenemos que $a \equiv -1 \pmod 3$. □

Corolario 3.3.3. *Sean $A = 2a - b$ y $B = b/3$. Entonces, $A \equiv 1 \pmod 3$ y $4p = A^2 + 27B^2$.*

Demostración: Debido a que $a \equiv -1 \pmod 3$ y $b \equiv 0 \pmod 3$, se tiene que $2a - b \equiv 1 \pmod 3$.

Para la segunda parte, tenemos que $p = |J(\chi,\chi)|^2 = a^2 - 2ab + b^2$, luego $4p = (2a-b)^2 + 3b^2 = A^2 + 27B^2$. □

Teorema 3.3.2. *Si $p \equiv 1 \pmod 3$, entonces existen enteros A y B tales que $4p = A^2 + 27B^2$, y si pedimos que $A \equiv 1 \pmod 3$, entonces A está determinado de forma única. Además, $N(X^3 + Y^3 = 1) = p - 2 + A$.*

Demostración: La existencia se desprende de la Proposición 3.3.3 y del Corolario 3.3.3. Si $A \equiv 1 \pmod 3$, entonces la unicidad de A esta determinada por la Proposición 4.2.7, por lo tanto $A = 2a - b$.

Además, previamente establecimos que $N(X^3 + Y^3 = 1) = p - 2 + 2ReJ(\chi,\chi)$, con χ caracter cúbico en $\mathbb{F}_p$. Entonces $2ReJ(\chi,\chi) = 2a - b = A$, por lo tanto $N(X^3 + Y^3 = 1) = p - 2 + A$. □

Debido a que $4 \cdot 7 = 1^2 + 27 \cdot 1^2$, y que $4 \cdot 13 = (-5)^2 + 27 \cdot 1^3$, por el Teorema 3.3.2, concluimos que $N(X^3 + Y^3 = 1) = 6$ para $p = 7$ ó $p = 13$. Además, previamente demostramos que $N(X^3 + Y^3 = 1) > 6$ para $p \geq 19$.

Ilustremos el teorema anterior con otro ejemplo. Debido a que $4 \cdot 31 = 4^2 + 27 \cdot 2^2$, entonces $N(X^3 + Y^3 = 1) = 33$ para $p = 31$.

3.4. Más sobre sumas de Jacobi

A manera de genaralizar las sumas de Jacobi, se tiene la siguiente definición.

Definición 3.4.1. *Sean $\chi_1, \chi_2, \ldots, \chi_l$ caracteres multiplicativos en $\mathbb{F}_p$. Definimos la **suma de Jacobi (generalizada)** como:*

$$J(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1+t_2+\cdot+t_l=1} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l).$$

Además, definimos

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_{t_1+t_2+\cdot+t_l=0} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l).$$

Proposición 3.4.1. *Se tienen las siguientes propiedades:*

(*a*) $J_0(\epsilon, \epsilon, \ldots, \epsilon) = J(\epsilon, \epsilon, \ldots, \epsilon) = p^{l-1}$.

(*b*) *Si algunos pero no todos de los χ_i son triviales, entonces*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) = 0.$$

(*c*) *Si $\chi_l \neq \epsilon$, entonces*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \begin{cases} 0, & si \;\; \chi_1\cdots\chi_l \neq \epsilon; \\ \chi_l(-1)(p-1)J(\chi_1, \chi_2\ldots, \chi_{l-1}), & si \;\; \chi_1\cdots\chi_l = \epsilon. \end{cases}$$

Demostración: Para la parte (*a*), si tomamos $t_1, t_2, \ldots, t_{l-1}$ de forma arbitraria, entonces t_l está únicamente determinado bajo la relación $t_1 + t_2 \cdots + t_l = 0$, por lo tanto $J_0(\epsilon, \epsilon, \ldots, \epsilon) = p^{l-1}$.

Para la parte (*b*), supongamos que $\chi_l = \epsilon$, entonces

$$\begin{aligned} J_0(\chi_1, \chi_2, \ldots, \epsilon) &= \sum_{t_1+\cdots+t_l=0} \chi_1(t_1)\cdots\chi_{l-1}(t_{l-1})\epsilon(t_l) \\ &= \sum_{t_1,\ldots,t_{l-1}} \chi_1(t_1)\cdots\chi_{l-1}(t_{l-1}) \\ &= \left(\sum_{t_1}\chi_1(t_1)\right)\left(\sum_{t_2}\chi_2(t_2)\right)\cdots\left(\sum_{t_{l-1}}\chi_{l-1}(t_{l-1})\right) \\ &= 0, \end{aligned}$$

ya que no todos los χ_i son triviales. De forma análoga, se puede demostrar que $J(\chi_1, \chi_2, \ldots, \chi_l) = 0$.

Para la última parte, tenemos que

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_s \chi_l(s) \left(\sum_{t_1+t_2+\cdots+t_{l-1}=-s} \chi_1(t_1) \cdots \chi_{l-1}(t_{l-1}) \right) .$$

Como $\chi_l(0) = 0$, el primer término de la suma anterior se anula. Tomemos $s \neq 0$, luego existe t_i' tal que $t_i = -st_i'$ con $i = 1, 2, \ldots, l-1$. Entonces

$$\begin{aligned} \sum_{t_1+t_2+\cdots+t_{l-1}=-s} \chi_1(t_1) \cdots \chi_{l-1}(t_{l-1}) &= \chi_1 \cdots \chi_{l-1}(-s) \sum_{t_1'+t_2'+\cdots+t_{l-1}'=1} \chi_1(t_1') \cdots \chi_{l-1}(t_{l-1}') \\ &= \chi_1 \cdots \chi_{l-1}(-1)\chi_1 \cdots \chi_{l-1}(s) J(\chi_1, \ldots, \chi_{l-1}). \end{aligned}$$

Por lo tanto

$$\begin{aligned} J_0(\chi_1, \chi_2, \ldots, \chi_l) &= \sum_{s \neq 0} \chi_l(s)\chi_1 \cdots \chi_{l-1}(-1)\chi_1 \cdots \chi_{l-1}(s) J(\chi_1, \ldots, \chi_{l-1}) \\ &= \chi_1 \cdots \chi_{l-1}(-1) J(\chi_1, \ldots, \chi_{l-1}) \sum_{s \neq 0} \chi_1 \cdots \chi_{l-1}\chi_l(s). \end{aligned}$$

Si $\chi_1 \cdots \chi_l \neq \epsilon$, entonces $\sum_{s \neq 0} \chi_1 \cdots \chi_{l-1}\chi_l(s) = 0$, por lo tanto $J_0(\chi_1, \chi_2, \ldots, \chi_l) = 0$.

Si $\chi_1 \cdots \chi_l = \epsilon$, entonces $\chi_1 \cdots \chi_{l-1}(-1) = \chi_l(-1)$ y $\sum_{s \neq 0} \chi_1 \cdots \chi_{l-1}\chi_l(s) = p - 1$, de aquí se sigue el resultado. □

Teorema 3.4.1. *Sean $\chi_1, \chi_2, \ldots, \chi_l$ caracteres multiplicativos no triviales tales que $\chi_1\chi_2 \cdots \chi_l \neq \epsilon$. Entonces,*

$$g(\chi_1)g(\chi_2) \cdots g(\chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) g(\chi_1\chi_2 \cdots \chi_l) .$$

Demostración:
Tenemos,

$$\begin{aligned} g(\chi_1)g(\chi_2) \cdots g(\chi_l) &= \left(\sum_{t_1} \chi_1(t_1)\zeta^{t_1} \right) \left(\sum_{t_2} \chi_2(t_2)\zeta^{t_2} \right) \cdots \left(\sum_{t_l} \chi_l(t_l)\zeta^{t_l} \right) \\ &= \sum_s \zeta^s \left(\sum_{t_1+t_2+\cdots+t_l=s} \chi_1(t_1)\chi_2(t_2) \cdots \chi_l(t_l) \right) . \end{aligned}$$

Para $s = 0$, tenemos $\sum_{t_1+t_2+\cdots+t_l=0} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l) = 0$, por la Proposición 3.4.1.

Para $s \neq 0$, existe t_i' tal que $t_i = st_i'$ con $i = 1, 2, \ldots, l$. Entonces,

$$\sum_{t_1+t_2+\cdots+t_l=s} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l) = \chi_1\chi_2\cdots\chi_l(s) \sum_{t_1'+t_2'+\cdots+t_l'=1} \chi_1(t_1')\chi_2(t_2')\cdots\chi_l(t_l').$$

Luego,

$$\begin{aligned} g(\chi_1)g(\chi_2)\cdots g(\chi_l) &= \sum_s \zeta^s \left(\sum_{t_1+t_2+\cdots+t_l=s} \chi_1(t_1)\chi_2(t_2)\cdots\chi_l(t_l) \right) \\ &= \sum_{s\neq 0} \chi_1\chi_2\cdots\chi_l(s)\zeta^s \left(\sum_{t_1'+t_2'+\cdots+t_l'=1} \chi_1(t_1')\chi_2(t_2')\cdots\chi_l(t_l') \right) \\ &= g(\chi_1\chi_2\cdots\chi_l)J(\chi_1, \chi_2, \ldots, \chi_l). \end{aligned}$$

□

Corolario 3.4.1. *Sean $\chi_1, \chi_2, \ldots, \chi_l$ caracteres multiplicativos no triviales tales que $\chi_1\chi_2\cdots\chi_l = \epsilon$. Entonces,*

$$g(\chi_1)g(\chi_2)\cdots g(\chi_l) = \chi_l(-1)pJ(\chi_1, \chi_2, \ldots, \chi_{l-1}).$$

Demostración: Debido a que $\chi_1\chi_2\cdots\chi_{l-1} \neq \epsilon$, entonces aplicamos el Teorema 3.4.1 para obtener,

$$g(\chi_1)g(\chi_2)\cdots g(\chi_{l-1}) = J(\chi_1, \chi_2, \ldots, \chi_{l-1})g(\chi_1\chi_2\cdots\chi_{l-1});$$

multiplicando la ecuación anterior por $g(\chi_l)$, y debido a que $g(\chi_1\chi_2\cdots\chi_{l-1})g(\chi_l) = \chi_l(-1)p$, tenemos

$$\begin{aligned} g(\chi_1)g(\chi_2)\cdots g(\chi_{l-1})g(\chi_l) &= J(\chi_1, \chi_2, \ldots, \chi_{l-1})g(\chi_1\chi_2\cdots\chi_{l-1})g(\chi_l) \\ &= \chi_l(-1)pJ(\chi_1, \chi_2, \ldots, \chi_{l-1}). \end{aligned}$$

□

Corolario 3.4.2. *Tomando las mismas hipótesis del corolario anterior tenemos,*

$$J(\chi_1, \chi_2, \ldots, \chi_l) = -\chi_l(-1)J(\chi_1, \chi_2, \ldots, \chi_{l-1}).$$

(*Si* $l = 2$ *tomemos* $J(\chi_1) = 1$.)

Demostración: Desarrollando $g(\chi_1)g(\chi_2)\cdots g(\chi_l)$ de la misma forma que en el Teorema 3.4.1, obtenemos

$$g(\chi_1)g(\chi_2)\cdots g(\chi_l) = J_0(\chi_1, \chi_2, \ldots, \chi_l) + J(\chi_1, \chi_2, \ldots, \chi_l)\sum_{t\neq 0}\zeta^s.$$

Tomando en cuenta la última parte de la Proposición 3.4.1, el Corolario 3.4.1 y que $\sum_{t\neq 0}\zeta^s = -1$, se tiene que

$$\chi_l(-1)pJ(\chi_1, \chi_2, \ldots, \chi_{l-1}) = \chi_l(-1)(p-1)J(\chi_1, \chi_2, \ldots, \chi_{l-1}) + J(\chi_1, \chi_2, \ldots, \chi_l)(-1).$$

El resultado se tiene despejando el término $J(\chi_1, \chi_2, \ldots, \chi_l)$. □

Teorema 3.4.2. *Sean* $\chi_1, \chi_2, \ldots, \chi_l$ *caracteres multiplicativos no triviales. Entonces,*

(*a*) *Si* $\chi_1\chi_2\cdots\chi_l \neq \epsilon$, *entonces*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = 0 \quad y \quad |J(\chi_1, \chi_2, \ldots, \chi_l)| = p^{(l-1)2}.$$

(*b*) *Si* $\chi_1\chi_2\cdots\chi_l = \epsilon$, *entonces*

$$|J_0(\chi_1, \chi_2, \ldots, \chi_l)| = (p-1)p^{(l/2)-1} \quad y \quad |J(\chi_1, \chi_2, \ldots, \chi_l)| = p^{(l/2)-1}.$$

Demostración: El resultado se obtiene combinando la Proposición 3.4.1, el Teorema 3.4.1, el Corolario 3.4.2 y tomando en cuenta que $|g(\chi)| = \sqrt{p}$ con $\chi \neq \epsilon$.
□

Ahora, apliquemos los resultados establecidos para las sumas de Jacobi, calculando el número de soluciones de la ecuación $X_1^2 + X_2^2 + \cdots + X_l^2 = 1$ en $\mathbb{F}_p$.

Denotemos por N al número de soluciones de dicha ecuación y por χ al símbolo de Legendre. Entonces,

$$\begin{aligned} N &= \sum_{t_1+t_2+\cdots+t_l=1} N(X_1^2=t_1)N(X_2^2=t_2)\cdots N(X_l^2=t_l) \\ &= \sum_{t_1+t_2+\cdots+t_l=1} (1+\chi(t_1))(1+\chi(t_2))\cdots(1+\chi(t_l)) \\ &= p^{l-1} + \sum_{t_1+t_2+\cdots+t_l=1} \chi(t_1)\chi(t_2)\cdots\chi(t_l) \\ &= p^{l-1} + \underbrace{J(\chi,\chi,\ldots,\chi)}_{l \text{ veces}}. \end{aligned}$$

Por el Teorema 3.4.1, tenemos que si l es impar, entonces

$$\begin{aligned} \underbrace{J(\chi,\chi,\ldots,\chi)}_{l \text{ veces}} &= g(\chi)^{l-1} \\ &= \left(g(\chi)^2\right)^{(l-1)/2} \\ &= \left((-1)^{(p-1)/2}p\right)^{(l-1)/2} \\ &= (-1)^{((p-1)/2)((l-1)/2)}p^{(l-1)/2}. \end{aligned}$$

Si l es par, por el Corolario 3.4.2, tenemos que

$$\begin{aligned} \underbrace{J(\chi,\chi,\ldots,\chi)}_{l \text{ veces}} &= -\chi(-1)\,\underbrace{J(\chi,\chi,\ldots,\chi)}_{l-1 \text{ veces}} \\ &= -(-1)^{(p-1)/2}(-1)^{((p-1)/2)((l-2)/2)}p^{(l-2)/2} \\ &= -(-1)^{((p-1)/2)(l/2)}p^{(l-2)/2} \\ &= -(-1)^{((p-1)/2)(l/2)}p^{(l/2)-1}. \end{aligned}$$

Lo anterior se puede resumir en la siguiente proposición.

Proposición 3.4.2. *Si l es impar, entonces*

$$N = p^{l-1} + (-1)^{((p-1)/2)((l-1)/2)}p^{(l-1)/2}.$$

Si l es par, entonces

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

□

Capítulo 4

Reciprocidad cúbica y bicuadrática

4.1. El anillo $\mathbb{Z}[\omega]$

En este capítulo trabajaremos con el anillo $D = \mathbb{Z}[\omega]$, donde $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ es una raíz cúbica primitiva de la unidad. Este anillo claramente es un dominio entero; más aún, veremos en seguida que es un dominio de ideales principales y, por lo tanto, un dominio de factorización única, al probar que es un dominio euclideano con norma $N : D \to \mathbb{N} \cup \{0\}$ dada de la siguiente forma

$$N(a + b\omega) = (a + b\omega)(\overline{a + b\omega}) = a^2 - ab + b^2,$$

donde la barra indica conjugación compleja.

Es fácil probar que si $\alpha,\ \beta \in \mathbb{Z}[\omega]$, entonces $N(\alpha) = 0$ si, y sólo si $\alpha = 0$; y que $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proposición 4.1.1. $\mathbb{Z}[\omega]$ *es un dominio euclideano con la norma antes propuesta.*

Demostración: La función norma es tal que $N : D - \{0\} \to \mathbb{N}$, por lo tanto demostremos que

(a): $N(\alpha\beta) \geq N(\alpha)$ si $\alpha, \beta \neq 0$.
(b): Si $\alpha, \beta \in D$, $\beta \neq 0$, entonces existen $\rho, \gamma \in D$ tales que

$$\alpha = \rho\beta + \gamma \text{ , donde } \gamma = 0 \text{ ó } N(\beta) > N(\gamma)$$

El inciso (a) no es difícil de demostrar. Para el inciso (b), hagamos $\dfrac{\alpha}{\beta} = c + d\omega$, con c y d reales. Entonces, tomemos que $\rho = a + b\omega$, donde a y b son los enteros más próximos a c y d, respectivamente. De esta forma tenemos que $\gamma = \alpha - \rho\beta$. Si $\gamma \neq 0$, tenemos

$$\begin{aligned} N(\gamma) &= N(\alpha - \rho\beta) = N(\beta)N\left(\frac{\alpha}{\beta} - \rho\right) \\ &= N(\beta)N(c + d\omega - (a + b\omega)); \end{aligned}$$

puesto que $|c - a|$, $|d - b| \leq \dfrac{1}{2}$, obtenemos que

$$N(\beta)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) \geq N(\beta)N(c + d\omega - (a + b\omega)) = N(\gamma).$$

Por lo tanto $N(\beta) > N(\gamma)$. Con esto concluimos que D es un dominio euclideano. □

Proposición 4.1.2. *Sea $\alpha \in D$. Entonces, α es una unidad si, y sólo si $N(\alpha) = 1$. Además, las únicas unidades en D son $1, \omega, \omega^2, -1, -\omega$ y $-\omega^2$.*

Demostración: Hagamos $\alpha = a + b\omega$, con a y b enteros. Supongamos primero que $N(\alpha) = 1$, es decir, $\alpha\overline{\alpha} = 1$. Debido a que $\overline{\alpha} = (a - b) - b\omega \in D$, tenemos que α es una unidad en D.

Ahora, supongamos que α es una unidad, entonces $\alpha\alpha^{-1} = 1$, con $\alpha^{-1} \in D$, luego $N(\alpha\alpha^{-1}) = 1$, por lo tanto $N(\alpha) = 1$.

Finalmente, si $a + b\omega$ fuese una unidad, entonces $N(\alpha) = a^2 - ab + b^2 = 1$, luego $4 = (2a - b)^2 + 3b^2$, por lo tanto se tienen dos casos:

$$2a - b = \pm 1 \text{ y } b = \pm 1;$$

$$2a - b = \pm 2 \text{ y } b = 0.$$

Después de evaluar todas las posibilidades, concluimos que $a + b\omega = 1, -1, \omega, -\omega, 1 + \omega, -1 - \omega$ y, como $\omega^2 + \omega + 1 = 0$, entonces $1 + \omega = -\omega^2$ y $-1 - \omega = \omega^2$. □

Debido a que los elementos primos en D y en $\mathbb{Z}$ son distintos (por ejemplo, $13 = (4 + \omega)(3 - \omega)$), entonces nos referiremos a los primos en $\mathbb{Z}$ como primos racionales y a los primos en D simplemente como primos.

Proposición 4.1.3. *Si π es un primo en D, entonces $N(\pi) = p$ ó p^2, con p primo racional. Si $N(\pi) = p$ entonces π no está asociado con ningún primo racional. Si $N(\pi) = p^2$ entonces π y p son asociados.*

Demostración: Supongamos que $N(\pi) = \pi\overline{\pi} = n$, con $n \geq 2$, entonces existe p primo racional tal que $\pi \mid p$, luego existe γ tal que $p = \pi\gamma$; esto implica que $p^2 = N(\pi)N(\gamma)$. Por lo tanto, si γ fuera una unidad, entonces $N(\pi) = p^2$, con π y p asociados. Si γ no fuera una unidad, entonces $N(\gamma) = N(\pi) = p$; además, si π fuera asociado con q primo racional, entonces $p = N(\pi) = q^2$, lo cual es una contradicción. Por lo tanto, π no está asociado con ningún primo racional. □

Proposición 4.1.4. *Sea $\pi \in D$ tal que $N(\pi) = p$, con p primo racional. Entonces, π es primo.*

Demostración: Si π no fuera primo, entonces existirían γ y ρ tales que $\pi = \gamma\rho$, con $N(\gamma) > 1$ y $N(\rho) > 1$. Por lo tanto, $N(\pi) = N(\gamma)N(\rho) = p$, lo cual es una contradicción. □

Proposición 4.1.5. *Sean p y q primos racionales. Si $q \equiv 2 \pmod 3$, entonces q es primo en D. Si $p \equiv 1 \pmod 3$, entonces existe π primo en D tal que $N(\pi) = p$. Además, $3 = -\omega^2(1-\omega)^2$.*

Demostración: Supongamos que q no es primo, entonces existen γ y ρ tales que $q = \gamma\rho$, con $N(\gamma) > 1$ y $N(\rho) > 1$. Luego, $q^2 = N(\gamma)N(\rho)$ y, por lo tanto, $N(\gamma) = q$. Además, si escribimos $\gamma = a + b\omega$, entonces

$$a^2 - ab + b^2 = N(\gamma) = q,$$

lo cual implica que $4q = (2a-b)^2 + 3b^2$, o equivalentemente, $q \equiv (2a-b)^2 \pmod 3$. Luego, necesariamente $q \equiv 0,\ 1 \pmod 3$. Lo cual contradice que $q \equiv 2 \pmod 3$. Por lo tanto, q es primo en D.

Por otro lado, calculemos $(-3/p)$. Tenemos que

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

Luego, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -3 \pmod p$, por lo tanto existe $b \in \mathbb{Z}$ tal que

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

Si p fuera primo que divide a $(a+1+2\omega)$ o a $(a-1-2\omega)$, entonces $2/p \in \mathbb{Z}$, lo cual es absurdo. Por lo tanto, existen π y γ tales que $p = \pi\gamma$, con $N(\pi) > 1$ $N(\gamma) > 1$; en consecuencia, $N(\pi) = p$. Además, por la Proposición 4.1.4, tenemos que π es primo.

Para la última parte, puesto que $X^2+X+1 = (X-\omega)(X-\omega^2)$, sustituyendo $x = 1$, obtenemos que

$$3 = (1 - \omega)(1 - \omega^2) = (1 + \omega)(1 - \omega)^2.$$

Tomando en cuenta que $\omega^2 + \omega + 1 = 0$, se tiene que $3 = -\omega^2(1 - \omega)^2$. Aplicando normas en la última igualdad, tenemos que $9 = N(1-\omega)^2$, por lo tanto $N(1-\omega) = 3$. □

4.2. Anillos de residuos

Sean $\alpha, \beta, \gamma \in D$, entonces tenemos que $\alpha \equiv \beta \pmod{\gamma}$ si existe $\delta \in D$ tal que $\alpha - \beta = \gamma\delta$.

Proposición 4.2.1. *Sea $\pi \in D$ primo. Entonces $D/\pi D$ es un campo con $N(\pi)$ elementos.*

Demostración: Sea $\alpha \in D$ tal que $\alpha \notin \pi D$, entonces demostremos que $\alpha + \pi D \in D/\pi D$ tiene inverso. Como $(\alpha, \pi) = 1$, entonces existen β, $\gamma \in D$ tales que $\alpha\beta + \pi\gamma = 1$, es decir, $\alpha\beta \equiv 1 \pmod{\pi}$, por lo tanto $(\alpha + \pi D)^{-1} = \beta + \pi D$.

Supongamos primero que $N(\pi) = q^2$, entonces π y q son asociados, por lo tanto $\pi D = qD$. Demostremos que $\{a + b\omega \mid 0 \leq a < q,\ 0 \leq b < q\}$ es un conjunto completo de representantes de las clases módulo q. Sea $\mu = m + n\omega$, entonces existen $r, s, x, y \in \mathbb{Z}$ tales que $m = rq + s$ y $n = xq + y$ con $0 \leq s, y < q$, luego $m + n\omega = rq + xq\omega + s + y\omega$, por lo tanto $m + n\omega \equiv s + y\omega \pmod{q}$. Además si $a + b\omega \equiv a' + b'\omega \pmod{q}$ con $0 \leq a, b, a', b' < q$, entonces $q|(a - a') + (b - b')\omega$ y debido a que $|a - a'|,\ |b - b'| < q$, entonces $a = a'$ y $b = b'$.

Ahora supongamos que $N(\pi) = p$. Probemos que $\{0, 1, \ldots, p - 1\}$ es un conjunto completo de representantes de las clases módulo π. Sea $\pi = a + b\omega$ y $\mu = m + n\omega$. Como $p = a^2-ab+b^2$, entonces $p \nmid b$, luego existen $r, s \in \mathbb{Z}$ tales que $rb+sp = 1$, luego $nrb + nsp = n$. Entonces $\mu - nr\pi = m - nra + nsp\omega$, luego $\mu \equiv m - nra \pmod{\pi}$.

Además existe $0 \leq t < p$ tal que $m-nra \equiv t \pmod{p}$, luego $m-nra \equiv t \pmod{\pi}$, por lo tanto $\mu \equiv t \pmod{\pi}$. Supongamos que $r \equiv r' \pmod{\pi}$ con $0 \leq r, r' < p$, entonces $r - r' = \pi\gamma$, luego $(r-r')^2 = pN(\gamma)$, por lo tanto $r = r'$. □

Proposición 4.2.2. *Sea π primo y α tal que $\pi \nmid \alpha$, entonces $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.*

Demostración: Basta notar que el grupo multiplicativo de $D/\pi D$ es de orden $N(\pi) - 1$. □

Si π es un primo tal que $N(\pi) \neq 3$, entonces $1, \omega, \omega^2$ pertenecen a clases distintas. Supongamos que $1 \equiv \omega \pmod{\pi}$, entonces existe γ tal que $1 - \omega = \pi\gamma$, lo cual implica que $1-\omega$ y π son asociados, es decir, $N(\pi) = 3$, lo cual es una contradicción. De modo similar se demuestra que $1 \not\equiv \omega^2 \pmod{\pi}$ y que $\omega \not\equiv \omega^2 \pmod{\pi}$.

Notemos además que $\{1 + \pi D, \omega + \pi D, \omega^2 + \pi D\}$ es subgrupo cíclico de $(D/\pi D)^*$, entonces $3|N(\pi) - 1$.

Proposición 4.2.3. *Si π es un primo tal que $N(\pi) \neq 3$ y α tal que $\pi \nmid \alpha$, entonces $\alpha^{(N(\pi)-1)/3} \equiv \omega^m \pmod{\pi}$ con $m = 0, 1$ ó 2.*

Demostración: Como $\pi|\alpha^{N(\pi)-1} - 1$ y tomando en cuenta que

$$\alpha^{N(\pi)-1} - 1 = (\alpha^{(N(\pi)-1)/3} - 1)(\alpha^{(N(\pi)-1)/3} - \omega)(\alpha^{(N(\pi)-1)/3} - \omega^2).$$

Entonces π divide sólo a uno de los tres factores. Esto prueba la proposición. □

Definición 4.2.1. *Si $N(\pi) \neq 3$, entonces el **caracter cúbico de** α **módulo** π está dado por:*

(a) $(\alpha/\pi)_3 = 0$ *si* $\pi|\alpha$.

(b) $(\alpha/\pi)_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}$ *con* $(\alpha/\pi)_3 = 1, \omega, \omega^2$.

Proposición 4.2.4.

(a) $(\alpha/\pi)_3 = 1$ *si, y sólo si* $x^3 \equiv \alpha \pmod{\pi}$ *es soluble, es decir, α es un residuo cúbico.*

(b) $\alpha^{(N(\pi)-1)/3} \equiv (\alpha/\pi)_3 \pmod{\pi}$.

(c) $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.

(d) Si $\alpha \equiv \beta \pmod{\pi}$, *entonces* $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Demostración: La parte (a) se deduce de la Proposición 1.1.1 y la parte (b) se obtiene de la definición anterior.

Para otro lado, para (c), si $\pi \nmid \alpha\beta$ (el caso $\pi|\alpha\beta$ es evidente), entonces

$$(\alpha\beta)^{(N(\pi)-1)/3} = \alpha^{(N(\pi)-1)/3}\beta^{(N(\pi)-1)/3} \equiv (\alpha/\pi)_3(\beta/\pi)_3 \pmod{\pi}$$

Entonces $(\alpha\beta/\pi)_3 \equiv (\alpha/\pi)_3(\beta/\pi)_3 \pmod{\pi}$. Por lo tanto $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.

Para la parte (d) tenemos que $\alpha^{(N(\pi)-1)/3} \equiv \beta^{(N(\pi)-1)/3} \pmod{\pi}$, luego $(\alpha/\pi)_3 \equiv (\beta/\pi)_3 \pmod{\pi}$, por lo tanto $(\alpha/\pi)_3 = (\beta/\pi)_3$. □

De aquí en adelante emplearemos la siguiente notación: $\chi_\pi(\alpha) = (\alpha/\pi)_3$.

Proposición 4.2.5.
(a) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
(b) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

Demostración: Notemos que $\overline{\omega^m} = \omega^{2m}$ com $m = 0, 1, 2$, entonces $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2$ y, por la parte (c) de la proposición anterior, tenemos que $\chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.

Por otro lado, como $\alpha^{(N(\pi)-1)/3} \equiv \chi_\pi(\alpha) \pmod{\pi}$, entonces $\overline{\alpha}^{(N(\pi)-1)/3} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$, por lo tanto $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$. □

Corolario 4.2.1. *Sea q primo racional tal que $q \equiv 2 \pmod 3$ y $n \in \mathbb{Z}$ tal que $q \nmid n$, entonces $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$ y $\chi_q(n) = 1$.*

Demostración: La primera parte resulta de combinar los dos resultados de la proposición anterior. De igual forma para la segunda parte, ya que $\chi_{\overline{q}}(\overline{n}) = \chi_q(n)^2$, y por lo tanto $\chi_q(n) = 1$. □

Definición 4.2.2. *Se dice que $\pi \in D$ es un **elemento primario** si es primo y además $\pi \equiv 2 \pmod 3$.*

De acuerdo con la definición anterior, tenemos equivalentemente que si $\pi = a + b\omega$, entonces π es primario si, y sólo si es un primo tal que $a \equiv 2 \pmod 3$ y $b \equiv 0 \pmod 3$.

Proposición 4.2.6. *Sea $\pi \in D$ primo. Si $N(\pi) \neq 3$, entonces π tiene un sólo asociado que es primario. Si $N(\pi) = 3$, entonces π no es primario.*

Demostración: Primero demostremos que por lo menos alguno de los asociados de π es primario. Hagamos $\pi = a + b\omega$, entonces sus asociados son:

(a) $\pi = a + b\omega$
(b) $-\pi = -a - b\omega$
(c) $\omega\pi = -b + (a - b)\omega$
(d) $-\omega\pi = b - (a - b)\omega$
(e) $\omega^2\pi = (b - a) - a\omega$
(f) $-\omega^2\pi = -(b - a) + a\omega$

Los posibles valores de a y b son $a \equiv 0, 1, 2 \pmod 3$ y $b \equiv 0, 1, 2 \pmod 3$. Se descarta el caso $a \equiv b \equiv 0 \pmod 3$, ya que $3 \nmid \pi$. También se descartan los casos $a \equiv -b \equiv \pm 1 \pmod 3$ ya que $N(\pi) = a^2 - ab + b^2 \not\equiv 0 \pmod 3$. Analizando los casos restantes podemos encontrar un asociado de π que es primario.

Para demostrar la unicidad tomemos $a + b\omega$ primario, es decir, $a \equiv 2 \pmod 3$ y $b \equiv 0 \pmod 3$, basta analizar los asociados restantes para notar que ninguno de ellos es primario.

Para la última parte. Si π fuera primario entonces $a \equiv 2 \pmod 3$ y $b \equiv 0 \pmod 3$, entonces $3 = a^2 - ab + b^2 \equiv 1 \pmod 3$, lo que es una contradicción. □

Proposición 4.2.7. *Sea $p \equiv 1 \pmod 3$ un primo racional, entonces existen enteros A y B tales que $4p = A^2 + 27B^2$. Además, las únicas soluciones para $4p = X^2 + 27Y^2$ son $X = \pm A$, $Y = \pm B$.*

Demostración: Sea $\pi = a + b\omega$ primario tal que $N(\pi) = a^2 - ab + b^2 = p$, entonces hagamos $A = (2a - b)$ y $B = b/3$ para obtener $4p = A^2 + 27B^2$, con $A \equiv 1 \pmod 3$.

Supongamos además que existen enteros C y D tales que $4p = C^2 + 27D^2$, entonces hagamos $d = 3D$ y $c = (C + d)/2$ para obtener $4p = (2c - d)^2 + 3d^2$, es decir, $p = c^2 - cd + d^2$, por lo tanto $\alpha = c + d\omega$ es primo en D con $N(\alpha) = p$.

Debido a que $d \equiv 0 \pmod 3$, entonces α ó $-\alpha$ es primario; denotemos este elemento primario como $\pm\alpha$. Por lo tanto, $\pm\alpha = \pi = a + b\omega$ ó $\pm\alpha = \overline{\pi} = a - b - b\omega$, luego $C = \pm A$ y $D = \pm B$. □

4.3. Prueba de la ley de la reciprocidad cúbica

Sea π primo tal que $N(\pi) = p \equiv 1 \pmod 3$, entonces existe un isomorfismo $\varphi : D/\pi D \to \mathbb{Z}/p\mathbb{Z}$ tal que $\varphi(r + \pi D) = r + p\mathbb{Z}$ para $r = 0, 1, \ldots, p-1$. Entonces podemos considerar a χ_π como un caracter cúbico de $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Recordemos además que si χ es un caracter cúbico de $\mathbb{F}_p$, entonces:

(a) $g(\chi)^3 = pJ(\chi, \chi)$.
(b) Si $J(\chi, \chi) = a + b\omega$ entonces $a \equiv -1 \pmod 3$ y $b \equiv 0 \pmod 3$.

Tomando en cuenta que $J(\chi, \chi)\overline{J(\chi, \chi)} = p$, por el inciso (b) tenemos que $J(\chi, \chi)$ es primario.

Proposición 4.3.1. *Sean $k \in \mathbb{N}$ y $p \in \mathbb{Z}$ primo tales que $p - 1 \nmid k$, entonces*

$$\sum_{t=0}^{p-1} t^k \equiv 0 \pmod p.$$

Demostración: Denotemos por $T = \sum_{t \in \mathbb{F}_p} t^k$. Sea g un generador de ${\mathbb{F}_p}^*$, entonces

$$g^k T = \sum_{t \in \mathbb{F}_p} (gt)^k = \sum_{s \in \mathbb{F}_p} s^k = T \ .$$

Por lo tanto $T = 0$, ya que $g^k \neq 1$. □

Proposición 4.3.2. *Sean $m \in \mathbb{N}$ y p primo tales que $2m < p - 1$, entonces*

$$\sum_{t=0}^{p-1} (t)^m (1-t)^m \equiv 0 \pmod p \ .$$

Demostración:
Tenemos,

$$\begin{aligned} \sum_{t=0}^{p-1} (t)^m (1-t)^m = \sum_{t=0}^{p-1} (t - t^2)^m &= \sum_{t=0}^{p-1} \sum_{l=0}^{m} \binom{m}{l} (t)^l (-t^2)^{m-l} \\ &= \sum_{l=0}^{m} \binom{m}{l} (-1)^{m-l} \sum_{t=0}^{p-1} t^{2m-l} \ . \end{aligned}$$

Además, por la proposición anterior, tenemos que $\sum_{t=0}^{p-1} t^{2m-l} \equiv 0 \pmod{p}$ para $l = 0, 1, \ldots, m$.

Por lo tanto, $\sum_{t=0}^{p-1}(t)^m(1-t)^m \equiv 0 \pmod{p}$. □

Proposición 4.3.3. *Sea π primario tal que $N(\pi) = p$, entonces $J(\chi_\pi, \chi_\pi) = \pi$.*

Demostración: Por la proposición anterior tenemos

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &\equiv \sum_{t=0}^{p-1}(t)^{(p-1)/3}(1-t)^{(p-1)/3} \pmod{\pi} \\ &\equiv 0 \pmod{\pi}. \end{aligned}$$

Entonces $\pi | J(\chi_\pi, \chi_\pi)$ y, por lo tanto, $J(\chi_\pi, \chi_\pi) = \pi$. □

Como consecuencia inmediata de la proposición anterior, tenemos el siguiente:

Corolario 4.3.1. $g(\chi_\pi)^3 = p\pi$. □

Teorema 4.3.1 (Ley de la Reciprocidad Cúbica). *Sean π_1 y π_2 primarios tales que $N(\pi_1),\ N(\pi_2) \neq 3$ y $N(\pi_1) \neq N(\pi_2)$, entonces*

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

Demostración: Dividamos esta demostración en tres casos.

(a) $\pi_1 = q_1$ y $\pi_2 = q_2$, donde $q_1 \equiv q_2 \equiv 2 \pmod{3}$.
(b) $N(\pi_1) = p \equiv 1 \pmod{3}$ y $\pi_2 = q \equiv 2 \pmod{3}$.
(c) $N(\pi_1) = p_1$ y $N(\pi_2) = p_2$, donde $p_1 \equiv p_2 \equiv 1 \pmod{3}$.

El primer caso se obtiene por el Corolario 4.2.1.

Para el segundo caso denotemos $\pi = \pi_1$, entonces:

$$\begin{aligned} g(\chi_\pi)^{q^2} &= g(\chi_\pi)^{3(q^2-1)/3} g(\chi_\pi) \\ &= (p\pi)^{(q^2-1)/3} g(\chi_\pi) \\ &\equiv \chi_q(p\pi) g(\chi_\pi) \pmod{q} \\ &\equiv \chi_q(\pi) g(\chi_\pi) \pmod{q} \text{ , ya que } \chi_q(p) = 1. \end{aligned}$$

Además

$$g(\chi_\pi)^{q^2} \equiv \sum_t \chi_\pi(t)^{q^2} \zeta^{q^2 t} \pmod{q}.$$

Dado que $q^2 \equiv 1 \pmod 3$, por la Proposición 3.2.1, tenemos en el anillo de enteros algebraicos que

$$\begin{aligned} g(\chi_\pi)^{q^2} &\equiv \sum \chi_\pi(t) \zeta^{q^2 t} \pmod{q} \\ &\equiv \chi_\pi(q^{-2}) g(\chi_\pi) \pmod{q} \\ &\equiv \chi_\pi(q) g(\chi_\pi) \pmod{q}. \end{aligned}$$

Igualando ambas expresiones para $g(\chi_\pi)^{q^2}$ obtenemos

$$\chi_q(\pi) g(\chi_\pi) \equiv \chi_\pi(q) g(\chi_\pi) \pmod{q},$$

lo cual implica que

$$\chi_q(\pi) g(\chi_\pi) \overline{g(\chi_\pi)} \equiv \chi_\pi(q) g(\chi_\pi) \overline{g(\chi_\pi)} \pmod{q},$$

y de quí que

$$\chi_q(\pi) p \equiv \chi_\pi(q) p \pmod{q}.$$

Así que, existe $c+di$ entero algebraico tal que $(\chi_q(\pi) - \chi_\pi(q))p = (c+di)q$. Además $c - di$ también es un entero algebraico, por lo tanto $(c+di)(c-di) = c^2 + d^2$ es un entero algebraico.

Luego,

$$\begin{aligned} N(\chi_q(\pi) - \chi_\pi(q))p^2 &= N((\chi_q(\pi) - \chi_\pi(q))p) = N((c+di)q) \\ &= (c^2 + d^2)q^2 \ . \end{aligned}$$

Debido a que $N(\chi_q(\pi) - \chi_\pi(q)) = 0$ ó 3, entonces $c^2 + d^2 \in \mathbb{Q}$, por lo tanto $c^2 + d^2 \in \mathbb{Z}$.

Con esto obtenemos que $q \mid N(\chi_q(\pi) - \chi_\pi(q))$, luego $\chi_q(\pi) = \chi_\pi(q)$.

Para el tercer caso, hagamos $\gamma_1 = \overline{\pi_1}$ y $\gamma_2 = \overline{\pi_2}$, donde γ_1 y γ_2 también son primarios. De forma similar al caso anterior, tenemos que

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}$$

y

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \pmod{p_2}$$

luego $\chi_{\pi_2}(p_1\gamma_1) = \chi_{\gamma_1}(p_2^2)$.

De igual forma, se tiene que $\chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1^2)$.

Además, por la Proposición 4.2.5, tenemos que $\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2)$.

En consecuencia,

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2)\\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)\\ &= \chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(\pi_1 p_1\gamma_1)\\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).\end{aligned}$$

Eliminando $\chi_{\pi_2}(p_1\gamma_1)$ obtenemos el resultado. □

Teorema 4.3.2 (Suplemento de la Ley de la Reciprocidad Cúbica). *Sea π primario tal que $N(\pi) \neq 3$. Si $\pi = a + b\omega$, con $a = 3m - 1$, entonces $\chi_\pi(1-\omega) = \omega^{2m}$.*

Para obtener la demostración de este teorema, se desarrollarán los resultados pertinentes para su obtención.

Definición 4.3.1. *Sea $\alpha \in D$ no cero y no unidad tal que $3 \nmid N(\alpha)$, con $\alpha = \pi_1\pi_2\cdots\pi_n$ su descomposición en elementos primos, y sea $\beta \in D$ tal que $(\alpha, \beta) = 1$. Entonces, definimos*

$$\chi_\alpha(\beta) = \chi_{\pi_1}(\beta)\chi_{\pi_2}(\beta)\cdots\chi_{\pi_n}(\beta).$$

Si α es una unidad, entonces escribimos $\chi_\alpha(\beta) = 1$ para toda $\beta \in D$.

En base a esta definición, enunciamos la proposición siguiente que determinan algunas propiedades, las cuales son fáciles de obtener.

Proposición 4.3.4.

(*a*) $\chi_\alpha(\beta) = \chi_\alpha(\beta')$, *si* $\beta \equiv \beta' \pmod{\alpha}$.

(*b*) $\chi_\alpha(\beta) = \chi_{\alpha'}(\beta)$, *si* α *y* α' *son asociados.*

(*c*) $\chi_\alpha(\beta\gamma) = \chi_\alpha(\beta)\chi_\alpha(\gamma)$.

(*d*) $\chi_{\alpha\gamma}(\beta) = \chi_\alpha(\beta)\chi_\gamma(\beta)$. □

Proposición 4.3.5. *Sea* $a \in \mathbb{Z}$ *tal que* $a \neq 0, 1, -1$ *y* $3 \nmid a$, *entonces* a *se puede descomponer en elementos primarios salvo signo.*

Demostración: Sea $a = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$, con p_i y q_j primos positivos en $\mathbb{Z}$, tales que $p_i \equiv 1 \pmod{3}$ y $q_j \equiv 2 \pmod{3}$. Entonces,

$$a = \pm \pi_1 \overline{\pi_1} \pi_2 \overline{\pi_2} \cdots \pi_s \overline{\pi_s} q_1 q_2 \cdots q_t \ ,$$

donde π_i es primario tal que $N(\pi_i) = p_i$. □

Para la siguiente proposición notemos que si $a, b \in \mathbb{Z}$, entonces $(a, b) = 1$ en $\mathbb{Z}$ si, y sólo si $(a, b) = 1$ en D.

Proposición 4.3.6. *Sean* $a, b \in \mathbb{Z}$ *tales que* $3 \nmid a$ *y* $(a, b) = 1$. *Entonces* $\chi_a(b) = 1$.

Demostración: El resultado se tiene para $a = 1, -1$. Entonces, supóngase que $a = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$, con p_i, q_j primos positivos en $\mathbb{Z}$ tales que $p_i \equiv 1 \pmod{3}$ y $q_j \equiv 2 \pmod{3}$. Entonces,

$$\chi_a(b) = \chi_{p_1}(b) \cdots \chi_{p_s}(b) \chi_{q_1}(b) \cdots \chi_{q_t}(b)$$

Por el Corolario 4.2.1, tenemos que $\chi_{q_j}(b) = 1$. Ahora demostremos que $\chi_{p_i}(b) = 1$. Dado que $p_i = \pi_i \overline{\pi_i}$, con π_i primo, se tiene por la parte (b) de la Proposición 4.2.5 que

$$\chi_{p_i}(b) = \chi_{\pi_i}(b)\chi_{\overline{\pi_i}}(b) = \chi_{\pi_i}(b)\overline{\chi_{\pi_i}(b)} = 1.$$

Por lo tanto $\chi_a(b) = 1$. □

Lema 4.3.1. *Sean* $r_1, r_2, \ldots, r_t \in \mathbb{Z}$ *tales que* $r_1 \equiv r_2 \equiv \cdots \equiv r_t \equiv 1 \pmod 3$. *Entonces*

$$\frac{r_1 r_2 \cdots r_t - 1}{3} \equiv \frac{r_1 - 1}{3} + \frac{r_2 - 1}{3} + \cdots + \frac{r_t - 1}{3} \pmod 3.$$

Demostración: Ver el Lema 1.2.2 y Corolario 1.2.1 para demostraciones similares. □

Proposición 4.3.7. *Sea* $\pi \in D$ *primario y* $a \in \mathbb{Z}$ *tales que* $N(\pi) = p \equiv 1 \pmod 3$, $a \equiv 2 \pmod 3$ *y* $p \nmid a$. *Hagamos* $a = 3m - 1$, *entonces*

(*a*) $\chi_a(\pi) = \chi_\pi(a)$.
(*b*) $\chi_a(\omega) = \omega^m$.

Demostración: El caso $a = -1$ se obtiene del hecho de que $\chi_\pi(-1) = 1$.

De acuerdo con la Proposición 4.3.5, $a = \pm\pi_1\pi_2\cdots\pi_r$, donde los $\pi_i\,'s$ son primarios. Además, la condición $p \nmid a$ nos garantiza que $N(\pi_i) \neq p$. Aplicando la ley de la reciprocidad cúbica, obtenemos

$$\begin{aligned}\chi_a(\pi) &= \chi_{\pi_1}(\pi)\chi_{\pi_2}(\pi)\cdots\chi_{\pi_r}(\pi)\\ &= \chi_\pi(\pi_1)\chi_\pi(\pi_2)\cdots\chi_\pi(\pi_r)\\ &= \chi_\pi(\pm 1)\chi_\pi(\pi_1\pi_2\ldots\pi_r)\\ &= \chi_\pi(a).\end{aligned}$$

Ahora demostraremos la parte (*b*). El caso $a = -1$ es evidente, entonces expresemos $a = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$, con lo cual

$$\chi_a(\omega) = \chi_{p_1}(\omega)\cdots\chi_{p_s}(\omega)\chi_{q_1}(\omega)\cdots\chi_{q_t}(\omega).$$

Además $p_i = \pi_i\overline{\pi_i}$, con π_i primo. Luego

$$\chi_{p_i}(\omega) = \chi_{\pi_i}(\omega)\chi_{\overline{\pi_i}}(\omega) = \omega^{(p_i-1)/3}\omega^{(p_i-1)/3} = \omega^{(p_i^2-1)/3}\ .$$

Por lo tanto

$$\begin{aligned}\chi_a(\omega) &= \omega^{(p_1^2-1)/3}\cdots\omega^{(p_s^2-1)/3}\omega^{(q_1^2-1)/3}\cdots\omega^{(q_t^2-1)/3}\\ &= \omega^{(p_1^2\cdots p_s^2 q_1^2\cdots q_t^2-1)/3}\\ &= \omega^{(a^2-1)/3}\ .\end{aligned}$$

Para terminar con la demostración falta ver que $\frac{a^2-1}{3} \equiv m \pmod 3$.

Entonces, tenemos que $a = 3m - 1$, con lo cual $a^2 - 1 = 9m^2 - 6m$; luego,

$$\begin{aligned}\frac{a^2-1}{3} = 3m^2 - 2m &\equiv -2m \pmod 3 \\ &\equiv m \pmod 3\end{aligned}$$

□

Finalizamos la demostración del suplemento de la ley de la reciprocidad cúbica con la siguiente proposición.

Proposición 4.3.8. *Sea $\pi \in D$ primario tal que $N(\pi) = p \equiv 1 \pmod 3$, $\pi = a + b\omega$, con $a = 3m - 1$ y $b = 3n$. Entonces:*

(a) $(p-1)/3 \equiv -2m + n \pmod 3$.
(b) $\chi_\pi(a) = \omega^m$.
(c) $\chi_\pi(a+b) = \omega^{2n}\chi_\pi(1-\omega)$.
(d) $\chi_{a+b}(\pi) = \omega^{2(m+n)}$.
(e) $\chi_\pi(1-\omega) = \omega^{2m}$.

Demostración: Para la parte (a) tenemos,

$$\begin{aligned}p = a^2 - ab + b^2 &= (3m-1)^2 - (3m-1)(3b) + (3b)^2 \\ &\equiv -6m + 3n + 1 \pmod 9.\end{aligned}$$

Por lo tanto $(p-1)/3 \equiv -2m + n \pmod 3$.

Para la parte (b), aplicando la Proposición 4.3.6 y Proposición 4.3.7 obtenemos

$$\begin{aligned}\chi_\pi(a) &= \chi_a(\pi) \\ &= \chi_a(b\omega), \text{ ya que } \pi \equiv b\omega \pmod a \\ &= \chi_a(b)\chi_a(\omega) \\ &= \omega^m\end{aligned}$$

Para la parte (c), notemos que $\omega(a+b) \equiv -a(1-\omega) \pmod \pi$, entonces tenemos que

$$\chi_\pi(\omega)\chi_\pi(a+b) = \chi_\pi(-a)\chi_\pi(1-\omega),$$

que de acuerdo con el inciso (b)

$$\omega^{(p-1)/3}\chi_\pi(a+b) = \omega^m\chi_\pi(1-\omega)$$

pero por el inciso (a)

$$\omega^{-2m+n}\chi_\pi(a+b) = \omega^m\chi_\pi(1-\omega).$$

Por lo tanto,

$$\chi_\pi(a+b) = \omega^{2n}\chi_\pi(1-\omega).$$

Para la parte (d), notemos que $\pi \equiv a(1-\omega) \pmod{a+b}$, entonces

$$\chi_{a+b}(\pi) = \chi_{a+b}(a)\chi_{a+b}(1-\omega),$$

aplicando la Proposición 4.3.6 obtenemos

$$\chi_{a+b}(\pi) = \chi_{a+b}(1-\omega),$$

así que,

$$\begin{aligned}
\overline{\chi_{a+b}(\pi)} &= \chi_{a+b}((1-\omega)^2) \text{ , por la Proposición 4.2.5} \\
&= \chi_{a+b}(-3\omega) \\
&= \chi_{a+b}(\omega) \\
&= \omega^{m+n} \text{ , por la Proposición 4.3.7.}
\end{aligned}$$

Por lo tanto,

$$\chi_{a+b}(\pi) = \omega^{2(m+n)}.$$

Para la parte (e), ayundándonos de la Proposición 4.3.7, tenemos

$$\chi_\pi(a+b) = \chi_{a+b}(\pi) = \omega^{2n}\chi_\pi(1-\omega) = \omega^{2(m+n)}$$

Por lo tanto $\chi_\pi(1-\omega) = \omega^{2m}$. □

Para completar la demostración del suplemento de la ley de la reciprocidad cúbica, suponemos ahora que $\pi = q \in \mathbb{Z}$, con $q = 3m-1$. Entonces

$$\begin{aligned}\overline{\chi_q(1-\omega)} &= \chi_q((1-\omega)^2)\\ &= \chi_q(-3\omega) = \chi_q(\omega) = \omega^m.\end{aligned}$$

Por lo tanto $\chi_q(1-\omega) = \omega^{2m}$.

4.4. Otra prueba para la ley de la reciprocidad cúbica

Emplearemos la teoría sobre sumas de Jacobi para dar una demostración alterna de la ley de la reciprocidad cúbica.

Si π es primario, tal que $N(\pi) = p \equiv 1 \pmod 3$ y $q \equiv 2 \pmod 3$ es un primo racional, entonces por el Corolario 3.4.1 tenemos

$$g(\chi_\pi)^{q+1} = pJ(\underbrace{\chi_\pi, \ldots, \chi_\pi}_{q \text{ veces}}).$$

Empleando el hecho que $g(\chi_\pi)^3 = \pi p$, tenemos

$$(\pi p)^{(q+1)/3} = pJ(\chi_\pi, \ldots, \chi_\pi)$$

con lo cual

$$\pi^{(q+1)/3} p^{(q-2)/3} = J(\chi_\pi, \ldots, \chi_\pi).$$

Por otro lado, $J(\underbrace{\chi_\pi, \ldots, \chi_\pi}_{q \text{ veces}}) = \sum_{t_1+t_2+\cdots+t_q=1} \chi_\pi(t_1)\cdots\chi_\pi(t_q)$. Supongamos que $t_1 = t_2 = \cdots = t_q = 1/q$, entonces

$$\chi_\pi(t_1)\cdots\chi_\pi(t_q) = \chi_\pi(q^{-1})^q = \chi_\pi(q^{-1})^2 = \chi_\pi(q).$$

Supongamos ahora que $t_1 = t_2 = \cdots = t_s$ con $1 < s < q$, y los restantes sean distintos a pares, entonces la cantidad de q-tuplas que se pueden generar con estos elementos es $\binom{q}{s}(q-s)!$, el cual es múltiplo de q.

Si los elementos $t_1, \ldots, t_q$ fueran todos distintos a pares, entonces la cantidad de q-tuplas sería $q!$.

Por lo tanto $J(\chi_\pi, \ldots, \chi_\pi) \equiv \chi_\pi(q) \pmod q$, luego

$$\pi^{(q+1)/3}p^{(q-2)/3} \equiv \chi_\pi(q) \pmod{q},$$

elevando a la $q-1$ tenemos que

$$\pi^{(q^2-1)/3}p^{(q-1)(q-2)/3} \equiv \chi_\pi(q)^{q-1} \pmod{q}$$

con lo cual

$$\pi^{(q^2-1)/3} \equiv \chi_\pi(q) \pmod{q},$$

ya que $p^{q-1} \equiv 1 \pmod{q}$. En consecuencia,

$$\chi_q(\pi) \equiv \chi_\pi(q) \pmod{q},$$

es decir, $\chi_q(\pi) = \chi_\pi(q)$.

Si π_1, π_2 son primarios tales que $N(\pi_1) = p_1$ y $N(\pi_2) = p_2$, con $p_1 \equiv p_2 \equiv 1 \pmod 3$ y, además, $\overline{\pi_1} = \gamma_1$ y $\overline{\pi_2} = \gamma_2$ entonces, por el Teorema 3.4.1, tenemos que

$$g(\chi_{\gamma_1})^{p_2} = g(\chi_{\gamma_1})J(\underbrace{\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}}_{p_2 \ veces}),$$

o equivalentemente

$$g(\chi_{\gamma_1})^{p_2-1} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}).$$

Un análisis similar al anterior nos muestra que

$$J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}) \equiv \chi_{\gamma_1}(p_2^{-1}) \pmod{p_2}.$$

Además $g(\chi_{\gamma_1})^{p_2-1} = g(\chi_{\gamma_1})^{3(p_2-1)/3} = (\gamma_1 p_1)^{(p_2-1)/3}$, por lo tanto

$$(\gamma_1 p_1)^{(p_2-1)/3} \equiv \chi_{\gamma_1}(p_2^{-1}) \pmod{p_2},$$

y

$$\chi_{\pi_2}(\gamma_1 p_1) \equiv \chi_{\gamma_1}(p_2^2) \pmod{\pi_2}.$$

Por lo tanto,

$$\chi_{\pi_2}(\gamma_1 p_1) = \chi_{\gamma_1}(p_2^2).$$

Similarmente se demuestra que $\chi_{\pi_1}(\pi_2 p_2) = \chi_{\pi_2}(p_1^2)$.

De esta forma obtenemos las mismas dos igualdades que hallamos al final de la demostración del teorema de la reciprocidad cúbica, obteniéndose así que $\chi_\pi(\pi_2) = \chi_{\pi_2}(\pi_1)$.

4.5. El caracter cúbico de 2

Enseguida veremos para qué elementos primarios π, se tiene que $\chi_\pi(2) = 1$. Si $q \equiv 2 \pmod 3$ es un primo racional, con $q \neq 2$, entonces $\chi_q(2) = 1$.

Proposición 4.5.1. *Sea $\pi = a + b\omega$ primario, con $N(\pi) = p \equiv 1 \pmod 3$. Entonces, $\chi_\pi(2) = 1$ si, y sólo si a es impar y b es par.*

Demostración: Por la ley de la reciprocidad cúbica tenemos

$$\chi_\pi(2) = \chi_2(\pi) \equiv \pi^{(N(2)-1)/3} \equiv \pi \pmod 2.$$

Por lo tanto $\chi_\pi(2) = 1$ si, y sólo si $\pi \equiv 1 \pmod 2$. □

Proposición 4.5.2. *Sea $p \equiv 1 \pmod 3$ un primo racional tal que $p = \pi\overline{\pi}$, con $\pi = a+b\omega$ primario. Entonces, $X^3 \equiv 2 \pmod p$ es soluble en $\mathbb{Z}$ si, y sólo si existen C y $D \in \mathbb{Z}$ tales que $p = C^2 + 27D^2$.*

Demostración: Supongamos primero que $x^3 \equiv 2 \pmod p$ es soluble, entonces $\chi_\pi(2) = 1$, luego a es impar y b es par. Además $4p = (2a - b)^2 + 3b^2$, entonces definimos $C = (2a - b)/2$ y $D = b/6$ para obtener $p = C^2 + 27D^2$.

Por otro lado, si existieran C y $D \in \mathbb{Z}$ tales que $p = C^2+27D^2$, entonces $4p = (2C)^2+27(2D)^2$, luego por la unicidad de la última expresión tenemos que $b/3 = \pm 2D$, es decir, b es par y por lo tanto a es impar, luego $X^3 \equiv 2 \ (\pi)$ es soluble. Debido a que $\{0, 1, \ldots, p-1\}$ es un sistema completo de representantes de $D/\pi D$, entonces existe $h \in \mathbb{Z}$ tal que $h^3 \equiv 2 \pmod \pi$, luego $(h^3 - 2) = \pi\lambda$ para algún $\lambda \in D$; tomando normas obtenemos que $p|(h^3 - 2)$, es decir, $X^3 \equiv 2 \pmod p$ es soluble. □

Por ejemplo, para $p = 7, p = 13$ y $p = 19$ no exite solución para $X^3 \equiv 2 \pmod p$. Para $p = 43$ tenemos $43 = 4^2 + 27$, luego $20^3 \equiv 2 \pmod{43}$.

4.6. Reciprocidad bicuadrática

En esta parte trabajaremos en el dominio $D = \mathbb{Z}[i]$ el cual tiene una norma dada por $N(\alpha) = \alpha\overline{\alpha}$. Esta norma hace de D un dominio euclideano y, por lo tanto, un dominio de factorización única.

Proposición 4.6.1. *$D = \mathbb{Z}[i]$ es un dominio euclideano con la norma antes propuesta.*

Demostración: La función norma es tal que $N : D - \{0\} \to \mathbb{N}$, entonces demostremos que

(a): $N(\alpha\beta) \geq N(\alpha)$ si $\alpha, \beta \neq 0$.
(b): Si $\alpha, \beta \in D$, $\beta \neq 0$, entonces existen $\rho, \gamma \in D$ tales que

$$\alpha = \rho\beta + \gamma, \text{ donde } \gamma = 0 \text{ ó } N(\beta) > N(\gamma)$$

El inciso (a) no es difícil de demostrar. Para el inciso (b), hagamos $\frac{\alpha}{\beta} = c + di \in \mathbb{C}$, entonces tomemos $\rho = a + bi$, donde a y b son los enteros más próximos a c y d respectivamente. De esta forma tenemos que $\gamma = \alpha - \rho\beta$. Si $\gamma \neq 0$, tenemos

$$\begin{aligned} N(\gamma) &= N(\alpha - \rho\beta) = N(\beta)N\left(\frac{\alpha}{\beta} - \rho\right) \\ &= N(\beta)N(c + d\omega - (a + b\omega)); \end{aligned}$$

puesto que $|c - a|$, $|d - b| \leq \frac{1}{2}$, obtenemos que

$$N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) \geq N(\beta)N(c + d\omega - (a + b\omega)) = N(\gamma).$$

Por lo tanto $N(\beta) > N(\gamma)$. Con esto concluimos que D es un dominio euclideano. □

Proposición 4.6.2. *Sea $\alpha \in D$. Entonces, α es una unidad si, y sólo si $N(\alpha) = 1$. Además, las únicas unidades en D son $1, -1, i$ y $-i$.*

Demostración: Hagamos $\alpha = a + bi$, con a y b enteros. Supongamos primero que $N(\alpha) = 1$, es decir, $\alpha\overline{\alpha} = 1$. Como $\overline{\alpha} = a - bi \in D$, entonces α es una unidad en D.

Ahora supongamos que α es una unidad, entonces $\alpha\alpha^{-1} = 1$, con $\alpha^{-1} \in D$, luego $N(\alpha\alpha^{-1}) = 1$, por lo tanto $N(\alpha) = 1$.

Finalmente, si $a + bi$ fuese una unidad, entonces $N(\alpha) = a^2 + b^2 = 1$, por lo tanto $\alpha = 1, -1, i, -i$. □

Debido a que los primos en D y en $\mathbb{Z}$ son distintos (por ejemplo $13 = (3+2i)(3-2i)$), entonces nos referiremos a los primos en $\mathbb{Z}$ como primos racionales y a los primos en D simplemente como irreducibles.

Proposición 4.6.3. *Sea $\pi \in D$ irreducible, entonces $N(\pi) = p$ ó p^2, con p primo racional. Si $N(\pi) = p$ entonces π no está asociado a ningún primo racional. Si $N(\pi) = p^2$ entonces π y p son asociados.*

Demostración: La demostración es similar a la dada en la Proposición 4.1.3. □

Proposición 4.6.4. *Si $\pi \in D$ tal que $N(\pi) = p$, con p primo racional. Entonces π es irreducble.*

Demostración: La demostración es similar a la dada en la proposición 4.1.4. □

Proposición 4.6.5. *Sean p y q primos racionales. Si $q \equiv 3 \pmod 4$, entonces q es primo en D. Si $p \equiv 1 \pmod 4$, entonces existe $\pi \in D$ irreducible tal que $N(\pi) = p$. Además, $2 = -i(1+i)^2$.*

Demostración: Supongamos que q no es primo, entonces existen γ y ρ tales que $q = \gamma\rho$, con $N(\gamma)$, $N(\rho) > 1$. Luego, $q^2 = N(\gamma)N(\rho)$ y, por lo tanto, $N(\gamma) = q$. Además si escribimos $\gamma = a + bi$, entonces

$$N(\gamma) = a^2 + b^2 \equiv 0, 1 \text{ ó } 2 \pmod 4$$

Lo que lleva a una contradicción, ya que $N(\gamma) = q \equiv 3 \pmod 4$.

Como $p \equiv 1 \pmod 4$ entonces $(-1/p) = 1$, es decir, existe $c \in \mathbb{Z}$ tal que $c^2 \equiv -1 \pmod p$, entonces $p|(c^2+1) = (c+i)(c-i)$, pero $p \nmid (c+i)$ y $p \nmid (c-i)$, por lo tanto p no es primo, luego existen π y γ tales que $N(\pi), N(\gamma) > 1$ y $p = \pi\gamma$; así, $N(\pi) = p$.

No es difícil demostrar que $2 = -i(1+i)^2$, notemos además que $N(1+i) = 2$, es decir, $1+i$ es irreducible. □

Definición 4.6.1. *Se dice que $\alpha \in D$ es primario si $\alpha \equiv 1 \pmod{(1+i)^3}$.*

Lema 4.6.1. *Sea $\alpha \in D$ tal que $\alpha = a + bi$. Entonces α es primario si, y sólo si $a \equiv 1 \pmod 4$ y $b \equiv 0 \pmod 4$ ó $a \equiv 3 \pmod 4$ y $b \equiv 2 \pmod 4$.*

Demostración: Tomando en cuenta que $(1+i)^3 = 2i(1+i)$, entonces

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

Por lo tanto, $\dfrac{a+bi-1}{(1+i)^3} \in D$ si, y sólo si

$$-a+b+1 \equiv 0 \pmod 4 \text{ y } -a-b+1 \equiv 0 \pmod 4.$$

Estas dos equivalencias se cumplen si, y sólo si $a \equiv 1 \pmod 4$ y $b \equiv 0 \pmod 4$ ó $a \equiv 3 \pmod 4$ y $b \equiv 2 \pmod 4$. □

Lema 4.6.2. *Si $\alpha \in D$ es tal que $1+i \nmid \alpha$, entonces sólo uno de los asociados de α es primario.*

Demostración: Tomemos $\alpha = a+bi$, entonces $a, b \equiv 0, 1, 2$ ó $3 \pmod 4$. Descartamos los casos $a, b \equiv 0$ ó $2 \pmod 4$ y $a, b \equiv 1$ ó $3 \pmod 4$ ya que $1+i \nmid \alpha$. Entonces, analizando los casos restantes, podemos encontrar un elemento primario entre los asociados de α. Dichos asociados son:

(a) $a+bi$
(b) $-a-bi$
(c) $-b+ai$
(d) $b-ai$

Para demostrar la unicidad, al tomemos $a+bi$ primario, basta analizar los asociados restantes para notar que ninguno de ellos es primario. □

Lema 4.6.3. *Si $\alpha \neq 1$ es primario, entonces α se puede expresar como producto de elementos irreducibles primarios.*

Demostración: Sea $\alpha = \mu\pi_1\pi_2\cdots\pi_r$, la descomposición de α en factores irreducibles, donde podemos suponer que los $\pi_i\,'s$ son primarios y μ es una unidad. Tomando congruencias módulo $(1+i)^3$, obtenemos

$$1 \equiv \mu \pmod{(1+i)^3}$$

Por lo tanto $\mu = 1$. □

Proposición 4.6.6. *Sea $\pi \in D$ irreducible. Entonces $D/\pi D$ es un campo con $N(\pi)$ elementos.*

Demostración: La demostración es similar a la dada en la Proposición 4.2.1. □

Proposición 4.6.7. *Sea $\pi \in D$ irreducible y $\alpha \in D$ tal que $\pi \nmid \alpha$, entonces $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$.*

Demostración: Basta notar que el grupo mutiplicativo $(D/\pi D)^*$ es de orden $N(\pi) - 1$. □

Si π es un elemento irreducible tal que $N(\pi) \neq 2$ (esta condición es equivalente a que π y $1+i$ no son asociados), entonces $1,\ -1,\ i$ y $-i$ pertenecen a clases distintas. Supongamos que $1 \equiv -1 \pmod{\pi}$, entonces existe γ tal que $2 = \pi\gamma$, lo cual implica que π y $1 + i$ son asociados, es decir, $N(\pi) = 2$, lo cual es una contradicción. De modo similar se demuestra para los casos restantes.

Notemos, además, que $\{1, -1, i, -i\}$ es subgrupo cíclico de $(D/\pi D)^*$, con lo cual $4 \mid N(\pi) - 1$.

Proposición 4.6.8. *Si π es irreducible tal que $N(\pi) \neq 2$ y α tal que $\pi \nmid \alpha$, entonces $\alpha^{(N(\pi)-1)/4} \equiv i^m \pmod{\pi}$ con $m = 0, 1, 2$ ó 3.*

Demostración: Basta notar que $\pi | \alpha^{N(\pi)-1} - 1$ y que

$$\alpha^{N(\pi)-1} - 1 = (\alpha^{(N(\pi)-1)/4} - 1)(\alpha^{(N(\pi)-1)/4} + 1)(\alpha^{(N(\pi)-1)/4} - i)(\alpha^{(N(\pi)-1)/4} + i)$$

con lo cual π divide sólo a uno de los cuatro factores. □

Definición 4.6.2. *Sea $\pi \in D$ irreducible tal que $N(\pi) \neq 2$, entonces el **caracter bicuadrático de** α **módulo** π está dado por:*

(a) $\chi_\pi(\alpha) = 0$ *si* $\pi \mid \alpha$.
(b) $\chi_\pi(\alpha) \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}$, *con* $\chi_\pi(\alpha) = 1, -1, i$ *ó* $-i$.

Proposición 4.6.9.

(a) $\chi_\pi(\alpha) = 1$ *si, y sólo si* $X^4 \equiv \alpha \pmod{\pi}$ *es soluble en* D.
(b) $\alpha^{(N(\pi)-1)/4} \equiv \chi_\pi(\alpha) \pmod{\pi}$.
(c) $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$.
(d) Si $\alpha \equiv \beta \pmod{\pi}$, *entonces* $\chi_\pi(\alpha) = \chi_\pi(\beta)$.

Demostración: La parte (a) se deduce de la Proposición 1.1.1, y la parte (b) se obtiene de la definición anterior.

Ver la Proposición 4.2.4 para la parte (c) y (d). □

Proposición 4.6.10. *Sea q primo racional tal que $q \equiv 3 \pmod 4$ y $a \in \mathbb{Z}$ tal que $p \nmid a$, entonces $\chi_q(a) = 1$.*

Demostración: Tomando en cuenta que $a^{q-1} \equiv 1 \pmod q$, entonces

$$\chi_q(a) = a^{(q^2-1)/4} = a^{(q-1)(q+1)/4} \equiv 1 \pmod q.$$

□

Definición 4.6.3. *Sea $\alpha \in D$ no cero ni unidad y $2 \nmid N(\alpha)$, sea $\alpha = \pi_1\pi_2\cdots\pi_n$ su descomposición en elementos irreducibles y $\beta \in D$ tal que $(\alpha, \beta) = 1$. Entonces, definimos*

$$\chi_\alpha(\beta) = \chi_{\pi_1}(\beta)\chi_{\pi_2}(\beta)\cdots\chi_{\pi_n}(\beta).$$

Si α es una unidad, entonces $\chi_\alpha(\beta) = 1$ para toda $\beta \in D$.

En base a esta definición podemos enunciar las siguientes propiedades.

Proposición 4.6.11.

(a) $\chi_\alpha(\beta) = \chi_\alpha(\beta')$, *si* $\beta \equiv \beta' \pmod \alpha$.

(b) $\chi_\alpha(\beta) = \chi_{\alpha'}(\beta)$, *si α y α' son asociados.*

(c) $\chi_\alpha(\beta\gamma) = \chi_\alpha(\beta)\chi_\alpha(\gamma)$.

(d) $\chi_{\alpha\gamma}(\beta) = \chi_\alpha(\beta)\chi_\gamma(\beta)$.

Para la siguiente proposición requeriremos del hecho que $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$, con π irreducible.

Proposición 4.6.12. *Sea $a \in \mathbb{Z}$ impar y $b \in \mathbb{Z}$ tal que $(a, b) = 1$. Entonces $\chi_a(b) = 1$.*

Demostración: El resultado se tiene para $a = 1$ y $a = -1$. Si a no es una unidad, entonces $a = \pm p_1p_2\cdots p_sq_1q_2\cdots q_t$, con p_i, q_j primos positivos en $\mathbb{Z}$ tales que $p_i \equiv 1 \pmod 4$ y $q_j \equiv 3 \pmod 4$. Entonces,

$$\chi_a(b) = \chi_{p_1}(b)\cdots\chi_{p_s}(b)\chi_{q_1}(b)\cdots\chi_{q_t}(b)$$

Por la Proposición 4.6.10, tenemos que $\chi_{q_j}(b) = 1$. Ahora demostremos que $\chi_{p_i}(b) = 1$. Dado que $p_i = \pi_i\overline{\pi_i}$, con π_i irreducible, entonces

$$\chi_{p_i}(b) = \chi_{\pi_i}(b)\chi_{\overline{\pi_i}}(b) = \chi_{\pi_i}(b)\overline{\chi_{\pi_i}(b)} = 1.$$

Por lo tanto $\chi_a(b) = 1$. □

Proposición 4.6.13. *Sean $r_1, r_2, \ldots, r_t \in \mathbb{Z}$ tales que $r_1 \equiv r_2 \equiv \cdots \equiv r_t \equiv 1$ (mód 4). Entonces*

$$\frac{r_1 r_2 \cdots r_t - 1}{4} \equiv \frac{r_1 - 1}{4} + \frac{r_2 - 1}{4} + \cdots + \frac{r_t - 1}{4} \pmod 4.$$

Demostración: Ver Lema 1.2.2 y Corolario 1.2.1 para demostraciones similares. □

Proposición 4.6.14. *Sea $n \in \mathbb{Z}$ tal que $n \equiv 1 \pmod 4$. Entonces, se tiene que $\chi_n(i) = (-1)^{(n-1)/4}$.*

Demostración: El caso $n = 1$ es fácil de demostrar. Supongamos que $n \neq 1$, entonces expresemos $n = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$, con p_i, q_j primos positivos en $\mathbb{Z}$ tales que $p_i \equiv 1 \pmod 4$ y $q_j \equiv 3 \pmod 4$. Entonces,

$$\chi_n(i) = \chi_{p_1}(i) \cdots \chi_{p_s}(i) \chi_{q_1}(i) \cdots \chi_{q_t}(i)$$

Además $p_i = \pi_i \overline{\pi_i}$ con π_i irreducible. Por la proposición anterior obtenemos,

$$\chi_{p_i}(i) = \chi_{\pi_i}(i) \chi_{\overline{\pi_i}}(i) = i^{(p_i - 1)/4} i^{(p_i - 1)/4} = i^{(p_i^2 - 1)/4} .$$

Por lo tanto

$$\begin{aligned} \chi_n(i) &= i^{(p_1^2 - 1)/4} \ldots i^{(p_s^2 - 1)/4} i^{(q_1^2 - 1)/4} \ldots i^{(q_t^2 - 1)/4} \\ &= i^{(p_1^2 \cdots p_s^2 q_1^2 \cdots q_t^2 - 1)/4} \\ &= i^{(n^2 - 1)/4} \\ &= i^{(n+1)(n-1)/4} = (-1)^{(n-1)/4} \text{ , ya que } n + 1 \equiv 2 \pmod 4. \end{aligned}$$

□

Proposición 4.6.15. *Sea $\pi = a + bi$ primario. Entonces, se cumple la congruencia* $\dfrac{N(\pi) - 1}{4} \equiv \dfrac{a - 1}{2} \pmod 2$.

Demostración: Basta ver que si $a \equiv 1 \pmod 4$ y $b \equiv 0 \pmod 4$, entonces

$$\frac{N(\pi) - 1}{4} \equiv \frac{a - 1}{2} \equiv 0 \pmod 2.$$

Si $a \equiv 3 \pmod 4$ y $b \equiv 2 \pmod 4$, entonces

$$\frac{N(\pi) - 1}{4} \equiv \frac{a - 1}{2} \equiv 1 \pmod 2.$$

□

Proposición 4.6.16. *Si $\lambda = c + di$ es primario, entonces $\chi_\lambda(-1) = (-1)^{(c-1)/2}$.*

Demostración: El caso $\lambda = 1$ es evidente. Si $\lambda \neq 1$, entonces sea $\lambda = \pi_1\pi_2\cdots\pi_r$ su descomposición en irreducibles primarios, entonces

$$\begin{aligned}\chi_\lambda(-1) &= \chi_{\pi_1}(-1)\cdots\chi_{\pi_r}(-1)\\ &= (-1)^{(N(\pi_1)-1)/4}\cdots(-1)^{(N(\pi_r)-1)/4}\\ &= (-1)^{(N(\pi_1)\cdots N(\pi_r)-1)/4}\text{ , por la Proposición 4.6.13.}\\ &= (-1)^{(N(\lambda)-1)/4} = (-1)^{(c-1)/2}\text{ , por la proposición anterior.}\end{aligned}$$

□

4.7. Ley de la reciprocidad bicuadrática

Teorema 4.7.1. *Sean $\alpha, \gamma \in D$ primarios, tales que $(\alpha, \gamma) = 1$. Entonces,*

$$\chi_\alpha(\gamma) = \chi_\gamma(\alpha)(-1)^{((N(\alpha)-1)/4)((N(\gamma)-1)/4)}.$$

Hagamos $\alpha = a+bi$ y $\gamma = c+di$. Debido a que se tienen las congruencias $\frac{N(\alpha)-1}{4} \equiv \frac{a-1}{2}$ (mód 2) y $\frac{N(\gamma)-1}{4} \equiv \frac{c-1}{2}$ (mód 2), tenemos que si a o $c \equiv 1$ (mód 4), entonces

$$\chi_\alpha(\gamma) = \chi_\gamma(\alpha).$$

En caso contrario, es decir, $a \equiv c \equiv 3$ (mód 4), tenemos

$$\chi_\alpha(\gamma) = -\chi_\gamma(\alpha).$$

Sea π irreducible tal que $N(\pi) = p \equiv 1$ (mód 4), entonces χ_π puede ser visto como un caracter multiplicativo en $D/\pi D = \mathbb{F}_p$. Debido a que χ_π es un caracter de orden cuatro, entonces χ_π^2 es el símbolo de Legendre, entonces denotaremos $\psi = \chi_\pi^2$.

Proposición 4.7.1. $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

Demostración: Por la Proposición 3.3.2, tenemos

$$g(\chi_\pi)^2 = J(\chi_\pi, \chi_\pi)g(\psi).$$

Elevando al cuadrado la igualdad anterior, y aplicando la Proposición 2.3.2, obtenemos

$$g(\chi_\pi)^4 = J(\chi_\pi, \chi_\pi)^2 g(\psi)^2 = pJ(\chi_\pi, \chi_\pi)^2.$$

□

Proposición 4.7.2. $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ *es primario.*

Demostración: Notemos que

$$J(\chi_\pi, \chi_\pi) = \sum_{t=0}^{p-1} \chi_\pi(t)\chi_\pi(1-t) = \chi_\pi\left(\frac{p+1}{2}\right)^2 + \sum_{t=2}^{(p-1)/2} 2\chi_\pi(t)\chi_\pi(1-t),$$

donde $\chi_\pi\left(\dfrac{p+1}{2}\right)^2 = \chi_\pi(2^{-1})^2 = \chi_\pi(2)^{-2} = \chi_\pi(2)^2 = \chi_\pi(-i(1+i)^2)^2 = \chi_\pi(-1)$.

Debido a que $\mu \equiv 1 \pmod{1+i}$ para μ unidad, y tomando en cuenta que $2 = -i(1+i)^2$, tenemos que $2\chi_\pi(t)\chi_\pi(1-t) \equiv 2 \pmod{(1+i)^3}$, luego

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &\equiv 2\left(\frac{p-3}{2}\right) + \chi_\pi(-1) \pmod{(1+i)^3} \\ &\equiv -2 + \chi_\pi(-1) \text{ , ya que } p-3 \equiv -2 \pmod 4. \end{aligned}$$

Por lo tanto,

$$-\chi_\pi(-1)J(\chi_{\pi,\chi_\pi}) \equiv 2\chi_\pi(-1) - 1 \pmod{(1+i)^3}.$$

Si $\chi_\pi(-1) = 1$ el resultado es claro. Si $\chi_\pi(-1) = -1$, entonces notemos que $-3 \equiv 1 \pmod 4$, por lo tanto $-3 \equiv 1 \pmod{(1+i)^3}$. □

De aquí en adelante, supondremos que π es un elemento irreducible primario tal que $N(\pi) = p \equiv 1 \pmod 4$.

Proposición 4.7.3. $-\chi_\pi(-1)J(\pi, \pi) = \pi$.

Demostración: Por el Corolario 3.3.1, tenemos que $N(J(\chi_\pi, \chi_\pi)) = p$, es decir, $J(\chi_\pi, \chi_\pi)$ es irreducible.

Además, empleando la Proposición 4.3.2, tenemos

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &\equiv \sum_{t=0}^{p-1} (t)^{(p-1)/4}(1-t)^{(p-1)/4} \pmod \pi \\ &\equiv 0 \pmod \pi. \end{aligned}$$

Luego $\pi \mid J(\chi_\pi, \chi_\pi)$. Por lo tanto $\pi = -\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$, dado que ambas partes son elementos primarios. □

Proposición 4.7.4. *$g(\chi_\pi)^4 = \pi^3\overline{\pi}$.*

Demostración: Se deduce de la Proposición 4.7.1, Proposición 4.7.3 y del hecho que $p = \pi\overline{\pi}$. □

Lema 4.7.1. *Sean $\alpha = a + bi \in D$ y $q \equiv 3 \pmod 4$ primo racional, entonces $\overline{\alpha} \equiv \alpha^q \pmod q$.*

Demostración:

$$(a + bi)^q \equiv a^q + (bi)^q \equiv a^q - b^q i \pmod q.$$

Además, por el Teorema Pequeño de Fermat, tenemos $a^q \equiv a \pmod q$ y $b^q \equiv b \pmod q$, por lo tanto

$$(a + bi)^q \equiv a^q - b^q i \equiv a - bi \pmod q.$$

□

Lema 4.7.2. *Sean $\alpha \in D$, β entero algebraico y $p > 2$ primo racional, tales que $\alpha = p\beta$. Entonces, $\beta \in D$.*

Demostración: Hagamos $\alpha = a + bi$, con $a, b \in \mathbb{Z}$ y $\beta = c + di$. Como β es un entero algebraico, tenemos que $\overline{\beta}$ también lo es, luego $\beta + \overline{\beta} = 2c$ y $2d$ son enteros algebraicos.

Debido a que $\alpha = p\beta$, se tiene que $a = pc$, luego $2a = p(2c)$, entonces $2c$ es un entero algebraico racional; por lo tanto, $2c$ es entero y $p \mid a$, en consecuencia $c \in \mathbb{Z}$, de igual forma obtenemos que $d \in \mathbb{Z}$. □

Proposición 4.7.5. *Sea $q \equiv 3 \pmod 4$ primo racional. Entonces $\chi_\pi(-q) = \chi_q(\pi)$.*

Demostración:

$$\begin{aligned} g(\chi_\pi)^q &\equiv \sum_t \chi_\pi(t)^q \zeta^{tq} \pmod q \\ &\equiv \sum_t \overline{\chi_\pi(t)}\zeta^{tq} \equiv \overline{\chi_\pi}(q^{-1})g(\overline{\chi}_\pi) \pmod q \\ &\equiv \chi_\pi(q)g(\overline{\chi}_\pi) \pmod q. \end{aligned}$$

Además,

$$\begin{aligned} g(\chi_\pi)^{q+1} &= g(\chi_\pi)^{4(q+1)/4} = \pi^{3(q+1)/4}\overline{\pi}^{(q+1)/4} \\ &\equiv \pi^{(q+3)(q+1)/4} \pmod{q} \text{ , por el Lema 4.7.1.} \end{aligned}$$

Por lo tanto,

$$\begin{aligned} g(\chi_\pi)^{q+1} \equiv \pi^{(q+3)(q+1)/4} &\equiv \chi_\pi(q)g(\overline{\chi}_\pi)g(\chi_\pi) \pmod{q} \\ \Longrightarrow \pi^{(q+3)(q+1)/4} &\equiv \chi_\pi(q)\chi_\pi(-1)\pi\overline{\pi} \pmod{q} \\ \Longrightarrow \pi^{(q+3)(q+1)/4} &\equiv \chi_\pi(-q)\pi^{q+1} \pmod{q} \\ \Longrightarrow \pi^{q+1}\pi^{(q^2-1)/4} &\equiv \pi^{q+1}\chi_\pi(-q) \pmod{q} \\ \Longrightarrow \pi^{q+1}\chi_q(\pi) &\equiv \pi^{q+1}\chi_\pi(-q) \pmod{q} \end{aligned}$$

Por el Lema 4.7.2, $\pi^{q+1}\chi_q(\pi) \equiv \pi^{q+1}\chi_\pi(-q) \pmod{q}$ es una congruencia en D, por lo tanto $\chi_q(\pi) = \chi_\pi(-q)$. □

Proposición 4.7.6. *Sea q primo racional, tal que $q \equiv 1 \pmod{4}$, entonces $\chi_\pi(q) = \chi_q(\pi)$.*

Demostración: Sea λ irreducible tal que $q = \lambda\overline{\lambda}$. Entonces,

$$\begin{aligned} g(\chi_\pi)^q &\equiv \sum_t \chi_\pi(t)\zeta^{qt} \pmod{q} \\ &\equiv \chi_\pi(q^{-1})g(\chi_\pi) \pmod{q}. \end{aligned}$$

Además

$$g(\chi_\pi)^{q+3} = g(\chi_\pi)^{4(q+3)/4} = (\pi^3\overline{\pi})^{(q+3)/4} .$$

Luego, se tiene que

$$(\pi^3\overline{\pi})^{(q+3)/4} \equiv \chi_\pi(q^{-1})g(\chi_\pi)^4 \pmod{q}$$

lo cual implica que

$$\pi^3\overline{\pi}\ (\pi^3\overline{\pi})^{(q-1)/4} \equiv \pi^3\overline{\pi}\ \overline{\chi_\pi(q)} \pmod{\lambda};$$

en consecuencia

$$\pi^3\overline{\pi}\ \chi_\lambda(\pi)^3\chi_\lambda(\overline{\pi}) \equiv \pi^3\overline{\pi}\ \overline{\chi_\pi(q)} \pmod{\lambda}.$$

Por el Lema 4.7.2, tenemos

$$\overline{\chi_\lambda(\pi)}\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi(q)}.$$

Tomando conjugados en la expresión anterior, obtenemos

$$\chi_\lambda(\pi)\chi_{\overline{\lambda}}(\pi) = \chi_\pi(q),$$

es decir

$$\chi_q(\pi) = \chi_\pi(q).$$

□

Proposición 4.7.7. *Sean $a \in \mathbb{Z}$ y λ primario, tales que $a \equiv 1 \pmod 4$ y $(a, \lambda) = 1$. Entonces $\chi_a(\lambda) = \chi_\lambda(a)$.*

Demostración: Para los casos $a = 1$ o $\lambda = 1$, el resultado es evidente. Entonces supongamos que $a \neq 1$ y $\lambda \neq 1$.

Sea $a = \pm p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$ su descomposición en primos racionales, donde $p_i \equiv 1 \pmod 4$ y $q_j \equiv 3 \pmod 4$. Además, sea $\lambda = \pi_1 \cdots \pi_r(-q_1') \cdots (-q_u')$ su descomposición en primarios irreducibles, donde $N(\pi_i) = p_i' \equiv 1 \pmod 4$ y $q_j' \equiv 3 \pmod 4$. Entonces, para $i = 1, \ldots, r$ tenemos los siguientes dos casos:

(a) Si $a < 0$, entonces t es impar. Empleando la Proposición 4.7.5 y Proposición 4.7.6 tenemos,

$$\begin{aligned}
\chi_a(\pi_i) &= \chi_{p_1}(\pi_i) \cdots \chi_{p_s}(\pi_i)\chi_{q_1}(\pi_i) \cdots \chi_{q_t}(\pi_i) \\
&= \chi_{\pi_i}(p_1) \cdots \chi_{\pi_i}(p_s)\chi_{\pi_i}(-q_1) \cdots \chi_{\pi_i}(-q_t) \\
&= \chi_{\pi_i}(-p_1 \cdots p_s q_1 \cdots q_t) \\
&= \chi_{\pi_i}(a).
\end{aligned}$$

(b) Para $a > 0$, basta notar que t es par y se procede de forma similar que el caso anterior.

Además, $\chi_a(-q_j') = \chi_{-q_j'}(a) = 1$ para $j = 1, \ldots, u$. Por lo tanto $\chi_a(\lambda) = \chi_\lambda(a)$. □

Proposición 4.7.8. *Sean π y λ elementos primarios tales que $\pi = a + bi$ y $\lambda = c + di$, con $(a, b) = (c, d) = (\pi, \lambda) = 1$. Entonces*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{(N(\pi)-1)}{4}\frac{(N(\lambda)-1)}{4}}.$$

Demostración: Tenemos que

$$c\pi = ca + cbi = ca + (\lambda - di)bi = (ac + bd) + b\lambda i$$

y

$$a\lambda = ac + adi = ac + (\pi - bi)di = (ac + bd) + d\pi i.$$

Entonces,

$$\chi_\lambda(c\pi) = \chi_\lambda(ac + bd). \tag{1}$$

y

$$\chi_\pi(a\lambda) = \chi_\pi(ac + bd). \tag{2}$$

Tomando el conjugado de la primera igualdad y después multiplicando ambas igualdades obtenemos,

$$\overline{\chi_\lambda(c\pi)}\chi_\pi(a\lambda) = \chi_{\overline{\lambda}}(ac + bd)\chi_\pi(ac + bd)$$

con lo cual se tiene que

$$\overline{\chi_\lambda(\pi)}\chi_\pi(\lambda) = \chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_{\overline{\lambda}\pi}(ac + bd).$$

Además, notemos que $c(-1)^{\frac{c-1}{2}} \equiv 1 \pmod 4$, de igual forma para a y $ac + bd$, entonces

$$\overline{\chi_\lambda(\pi)}\chi_\pi(\lambda) = \chi_c(\lambda)\chi_a(\overline{\pi})\chi_{ac+bd}(\overline{\lambda}\pi)\chi_\lambda(-1)^{\frac{c-1}{2}}\chi_{\overline{\pi}}(-1)^{\frac{a-1}{2}}\chi_{\overline{\lambda}\pi}(-1)^{\frac{ac+bd-1}{2}}\ .$$

Pero tomando en cuenta la Proposición 4.6.16, tenemos

(a) $\chi_\lambda(-1)^{\frac{c-1}{2}} = (-1)^{\frac{(c-1)}{2}\frac{(c-1)}{2}} = (-1)^{\frac{c-1}{2}}$
(b) $\chi_{\overline{\pi}}(-1)^{\frac{a-1}{2}} = (-1)^{\frac{a-1}{2}}$
(c) $\chi_{\overline{\lambda}\pi}(-1)^{\frac{ac+bd-1}{2}} = (-1)^{\frac{ac-1}{2}}$, ya que $bd \equiv 0 \pmod 4$.

Por lo tanto,

$$\begin{aligned}\chi_\lambda(-1)^{\frac{c-1}{2}}\chi_{\overline{\pi}}(-1)^{\frac{a-1}{2}}\chi_{\overline{\lambda}\pi}(-1)^{\frac{ac+bd-1}{2}} &= (-1)^{\frac{c-1}{2}}(-1)^{\frac{a-1}{2}}(-1)^{\frac{ac-1}{2}} \\ &= (-1)^{\frac{ac-1}{2}}(-1)^{\frac{ac-1}{2}}\ \text{, por el Corolario 1.2.1} \\ &= 1\end{aligned}$$

Notemos que

(a) $\chi_c(\lambda) = \chi_c(c + di) = \chi_c(d)\chi_c(i) = \chi_c(i)$
(b) $\chi_a(\overline{\pi}) = \chi_a(i)$

(c) $\chi_{ac+bd}(\overline{\lambda}\pi) = \chi_{ac+bd}(ac+bd+(-ad+bc)i) = \chi_{ac+bd}(i)$.

Luego

$$\begin{aligned}\overline{\chi_\lambda(\pi)}\chi_\pi(\lambda) &= \chi_a(i)\chi_c(i)\chi_{ac+bd}(i)\\ &= \chi_{ac(ac+bd)}(i) = (-1)^{\frac{ac(ac+bd)-1}{4}}\\ &= (-1)^{\frac{(a-1)}{2}\frac{(c-1)}{2}}\\ &= (-1)^{\frac{(N(\pi)-1)}{4}\frac{(N(\lambda)-1)}{4}}\ .\end{aligned}$$

□

Ahora, demostremos la ley de reciprocidad bicuadrática para π y λ primarios tales que $(\pi,\lambda) = 1$. Entonces, existen m y n tales que $m \equiv n \equiv 1 \pmod 4$, $\pi = m(a+bi)$, $\lambda = n(c+di)$ y $(a,b) = (c,d) = 1$. Luego

$$\begin{aligned}\chi_\pi(\lambda) &= \chi_{m(a+bi)}(n)\chi_m(c+di)\chi_{a+bi}(c+di)\\ &= \chi_n(m(a+bi))\chi_{c+di}(m)\chi_{c+di}(a+bi)(-1)^{\frac{(a-1)}{2}\frac{(c-1)}{2}}\\ &= \chi_\lambda(\pi)(-1)^{\frac{(a-1)}{2}\frac{(c-1)}{2}}\ .\end{aligned}$$

y debido a que $a \equiv ma \pmod 4$ y $c \equiv nc \pmod 4$, se tiene

$$\begin{aligned}\chi_\pi(\lambda) &= \chi_\lambda(\pi)(-1)^{\frac{(ma-1)}{2}\frac{(nc-1)}{2}}\\ &= \chi_\lambda(\pi)(-1)^{\frac{(N(\pi)-1)}{4}\frac{(N(\lambda)-1)}{4}}\ .\end{aligned}$$

Sean p, $q \equiv 1 \pmod 4$ primos distintos, π y λ primarios irreducibles tales que $\pi\overline{\pi} = p$ y $\lambda\overline{\lambda} = q$; además, hagamos $\pi = a+bi$ y $\lambda = c+di$. Sea $a \in \mathbb{Z}$, entonces denotemos $\psi_p(a) = (a/p)$, donde (a/p) es el símbolo de Legendre.

Proposición 4.7.9. *$\chi_\pi(q) = 1$ si, y sólo si $X^4 \equiv q \pmod p$ es soluble.*

Demostración: Supongamos primero que $\chi_\pi(q) = 1$, entonces existe $h \in \mathbb{Z}$ tal que $h^4 \equiv q \pmod \pi$. Luego existe $\beta \in D$ tal que $h^4 - q = \beta\pi$, tomando normas obtenemos que $p \mid h^4 - q$, por lo tanto $h^4 \equiv q \pmod p$.

Supongamos ahora que $X^4 \equiv q \pmod p$ es soluble, es decir, $X^4 \equiv q \pmod \pi$ es soluble, por lo tanto $\chi_\pi(q) = 1$. □

Proposición 4.7.10. *Si $\psi_p(q) = 1$, entonces $\chi_\pi(q) = \pm 1$ y $\chi_\lambda(p) = \pm 1$.*

Demostración: Debido a que $\chi_\pi^2(q) = \psi_p(q) = 1$, entonces $\chi_\pi(q) = \pm 1$. Además, por la ley de la reciprocidad cuadrática, tenemos que $\psi_p(q) = \psi_q(p) = 1$, entonces $\chi_\lambda(p) = \pm 1$. □

Proposición 4.7.11. $g(\chi_\pi)^2 = -(-1)^{(p-1)/4}\pi\sqrt{p}$.

Demostración: Por la parte (d) del Teorema 3.3.1 tenemos que

$$J(\chi_\pi, \chi_\pi)g(\psi_p) = g(\chi_\pi)^2.$$

Por la Proposición 2.4.4, se obtiene que $g(\psi_p) = \sqrt{p}$ y, en combinación con la Proposición 4.7.3, se deduce que

$$-\chi_\pi(-1)\pi\sqrt{p} = g(\chi_\pi)^2,$$

con lo cual

$$-(-1)^{(p-1)/4}\pi\sqrt{p} = g(\chi_\pi)^2.$$

□

De aquí en adelante, supondremos que $\psi_p(q) = 1$.

Proposición 4.7.12. $\pi^{(q-1)/2} \equiv \chi_\pi(q)\chi_\lambda(p) \pmod{q}$.

Demostración: Tenemos,

$$\begin{aligned} g(\chi_\pi)^q &\equiv \sum_t \chi_\pi(t)\zeta^{qt} \pmod{q} \\ &\equiv \chi_\pi(q^{-1})g(\chi_\pi) \pmod{q} \\ &\equiv \chi_\pi(q)g(\chi_\pi) \pmod{q}, \text{ ya que } \chi_\pi(q) = \pm 1. \end{aligned}$$

Además, la relación

$$g(\chi_\pi)^{q+3} \equiv \chi_\pi(q)g(\chi_\pi)^4 \pmod{q}$$

implica que

$$\begin{aligned} \chi_\pi(q)\pi^2 p &\equiv (\pi^2 p)^{(q+3)/4} \pmod{q} \\ &\equiv (\pi^2 p)^{(q-1)/4}\pi^2 p \pmod{q} \\ &\equiv \pi^{(q-1)/2}\chi_\lambda(p)\pi^2 p \pmod{q} \end{aligned}$$

con lo cual

$$\pi^{(q-1)/2}\pi^2 p \equiv \chi_\lambda(p)\chi_\pi(q)\pi^2 p \pmod{q}.$$

Por el Lema 4.7.2, tenemos que $\pi^{(q-1)/2} \equiv \chi_\lambda(p)\chi_\pi(q) \pmod{q}$ es una congruencia en D □

Lema 4.7.3. $\psi_q(ad-bc) = \psi_q(ad+bc)$.

Demostración: Debido a que $c^2 \equiv -d^2 \pmod{q}$ y $a^2+b^2 = p$, tenemos

$$\begin{aligned}\psi_q(ad-bc)\psi_q(ab+bc) &= \psi_q(a^2d^2-b^2c^2) = \psi_q(a^2d^2+b^2d^2)\\ &= \psi_q(d^2p) = \psi_q(p) = 1\end{aligned}$$

Por lo tanto $\psi_q(ad-bc) = \psi_q(ad+bc)$. □

Proposición 4.7.13. $\pi^{(q-1)/2} \equiv \psi_q(d)\psi_q(ad-bc) \pmod{q}$

Demostración: Tenemos que $d\pi = ad+bdi = ad+b(\lambda-c) = ad-bc+b\lambda$, luego

$$d\pi \equiv ad-bc \pmod{\lambda}$$

y

$$(d\pi)^{(q-1)/2} \equiv (ad-bc)^{(q-1)/2} \pmod{\lambda}.$$

Por lo tanto

$$\psi_q(d)\pi^{(q-1)/2} \equiv \psi_q(ad-bc) \pmod{\lambda}. \tag{1}$$

De igual forma para $\overline{\lambda} = c-di$ obtenemos que $d\pi = ad+b(c-\overline{\lambda})$, es decir, $d\pi \equiv ad+bc \pmod{\overline{\lambda}}$. Entonces

$$\psi_q(d)\pi^{(q-1)/2} \equiv \psi_q(ad+bc) \equiv \psi_q(ad-bc) \pmod{\overline{\lambda}}. \tag{2}$$

Debido a que λ y $\overline{\lambda}$ son primos relativos, entonces de (1) y (2) tenemos

$$\psi_q(d)\pi^{(q-1)/2} \equiv \psi_q(ad-bc) \pmod{q}.$$

□

Lema 4.7.4. $\psi_q(d) = (-1)^{(q-1)/4}$.

Demostración: Debido a que $q = c^2 + d^2$, tenemos que c o d es impar. Supongamos que c es impar y tomemos $c_0 = |c|$. Por la Proposición 1.2.4, tenemos

$$\psi_q(c_0) = \psi_{c_0}(q) = \psi_{c_0}(d^2) = 1.$$

Además, como $c_0^2 \equiv -d^2 \pmod{q}$, obtenemos que $c_0^{(q-1)/2} \equiv (-1)^{(q-1)/4} d^{(q-1)/2} \pmod{q}$, luego $1 \equiv (-1)^{(q-1)/4} \psi_q(d) \pmod{q}$. Por lo tanto $\psi_q(d) = (-1)^{(q-1)/4}$. □

Teorema 4.7.2. *$\chi_\pi(q)\chi_\lambda(p) = (-1)^{(q-1)/4}\psi_q(ad - bc)$.*

Demostración: Se sigue de la Proposición 4.7.12, Proposición 4.7.13 y del Lema 4.7.4. □

Capítulo 5

Aplicaciones

Proposición 5.1. *Sea $m > 1$ un número entero y $f(x)$ un polinomio con coeficientes enteros. Sea $m = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$, donde los p_i's son primos distintos y $k_i \geq 1$. Entonces, $f(x) \equiv 0 \pmod{m}$ es soluble si, y sólo si $f(x) \equiv 0 \pmod{p_i^{k_i}}$es soluble para cada $i = 1, 2, \ldots, n$.*

Demostración: Supongamos que existe $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod{m}$, entonces $f(a) \equiv 0 \pmod{p_i^{k_i}}$ para cada $i = 1, 2, \ldots, n$.

Recíprocamente, supongamos que para cada $i = 1, 2, \ldots, n$ existe a_i tal que $f(a_i) \equiv 0 \pmod{p_i^{k_i}}$. Por el Teorema Chino del Residuo, existe $a \in \mathbb{Z}$ tal que $a \equiv a_i \pmod{p_i^{k_i}}$. Además, $f(a_i) \equiv f(a) \pmod{p_i^{k_i}}$, por lo tanto $f(a) \equiv 0 \pmod{p_i^{k_i}}$, entonces $f(a) \equiv 0 \pmod{m}$. □

Proposición 5.2. *Sea $f(x)$ un polinomio con coeficientes enteros, entonces $f(x + h) = f(x) + f'(x)h + r(x, h)h^2$, donde $r(x, h)$ es un polinomio en las variables x y h.*

Demostración: Sea $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$, entonces

$$\begin{aligned} f(x+h) &= \sum_{i=0}^{n} a_i (x+h)^i = \sum_{i=0}^{n} \sum_{j=0}^{i} a_i \binom{i}{j} x^{i-j} h^j \\ &= \sum_{j=0}^{n} \sum_{i=j}^{n} a_i \binom{i}{j} x^{i-j} h^j \\ &= \sum_{i=0}^{n} a_i x^i + \sum_{i=1} i a_i x^{i-1} h + \sum_{j=2}^{n} \sum_{i=j}^{n} a_i \binom{i}{j} x^{i-j} h^j \\ &= f(x) + f'(x)h + r(x, h)h^2, \end{aligned}$$

donde $r(x,h) = \sum_{j=2}^{n}\sum_{i=j}^{n} a_i \binom{i}{j} x^{i-j}h^{j-2}$. □

Lema 5.1 (Lema de Hensel). *Sea $f(x)$ un polinomio con coeficientes enteros y $p \in \mathbb{Z}$ primo. Si existe x_1 tal que*

$$f(x_1) \equiv 0 \pmod{p}$$

y

$$f'(x_1) \not\equiv 0 \pmod{p},$$

entonces para cada $k \geq 2$ existe x_k tal que

$$f(x_k) \equiv 0 \pmod{p^k}$$

y

$$x_k \equiv x_{k-1} \pmod{p^{k-1}}.$$

Demostración: Procedemos por inducción. Como $f(x_1) \equiv 0 \pmod{p}$, entonces hagamos $f(x_1) = u_1 p$ y $f'(x_1) = v_1$ tal que $p \nmid v_1$, y elegimos y_1 tal que $f(x_1 + y_1 p) \equiv 0 \pmod{p^2}$. Por la Proposición 5.2, tenemos $f(x_1 + y_1 p) = u_1 p + v_1 y_1 p + r_1(x_1, y_1 p) y_1^2 p^2$, luego

$$f(x_1 + y_1 p) \equiv u_1 p + v_1 y_1 p \equiv (u_1 + v_1 y_1)p \pmod{p^2},$$

es decir

$$f(x_1 + y_1 p) \equiv (u_1 + v_1 y_1)p \pmod{p^2}. \tag{1}$$

Debido a que $(v_1, p) = 1$, existen s y t tales que $v_1 s + pt = 1$, luego $v_1 s u_1 + pt u_1 = u_1$, entonces hagamos $y_1 = -s u_1$, para obtener $u_1 + v_1 y_1 \equiv 0 \pmod{p}$; por lo tanto de (1) obtenemos

$$f(x_1 + y_1 p) \equiv (u_1 + v_1 y_1)p \equiv 0 \pmod{p^2}.$$

Haciendo $x_2 = x_1 + y_1 p$ concluimos que $f(x_2) \equiv 0 \pmod{p^2}$ y $x_2 \equiv x_1 \pmod{p}$.

Supongamos construidos $x_2, \ldots, x_{k-1}$ tales que $f(x_i) \equiv 0 \pmod{p^i}$ y $x_i \equiv x_{i-1} \pmod{p^{i-1}}$ para $i = 2, 3, \ldots, k-1$.

Debido a que $x_{k-1} \equiv x_1 \pmod{p}$, entonces $f'(x_{k-1}) \equiv f'(x_1) \not\equiv 0 \pmod{p}$. Sean $u_{k-1} p^{k-1} = f(x_{k-1})$ y $v_{k-1} = f'(x_{k-1})$, luego debemos hallar y_{k-1} tal que $f(x_{k-1} + y_{k-1} p^{k-1}) \equiv 0 \pmod{p^k}$. Aplicando la Proposición 5.2, obtenemos

$$f(x_{k-1}+y_{k-1}p^{k-1}) \equiv u_{k-1}p^{k-1} + v_{k-1}y_{k-1}p^{k-1} \equiv (u_{k-1}+v_{k-1}y_{k-1})p^{k-1} \pmod{p^k},$$

es decir

$$f(x_{k-1}+y_{k-1}p^{k-1}) \equiv (u_{k-1}+v_{k-1}y_{k-1})p^{k-1} \pmod{p^k}. \tag{2}$$

Debido a que $(v_{k-1}, p) = 1$, entonces existe y_{k-1} tal que $u_{k-1} + v_{k-1}y_{k-1} \equiv p$; por lo tanto de (2), obtenemos

$$f(x_{k-1}+y_{k-1}p^{k-1}) \equiv (u_{k-1}+v_{k-1}y_{k-1})p^{k-1} \equiv 0 \pmod{p^k}.$$

Haciendo $x_k = x_{k-1} + y_{k-1}p^{k-1}$ concluimos que $f(x_k) \equiv 0 \pmod{p^k}$ y $x_k \equiv x_{k-1} \pmod{p^{k-1}}$. □

Teorema 5.1. *Sean a y $m > 1$ impar, tales que $(a, m) = 1$ y $m = p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$, donde los p_i's son primos distintos y $k_i \geq 1$. Entonces, a es un residuo cuadrático módulo m si, y sólo si a es un residuo cuadrático módulo p_i para cada $i = 1, 2, \ldots, n$.*

Demostración: Consideremos el polinomio $x^2 - a$, y consideremos la Proposición 5.1 y Proposición 5.1, entonces

$$\begin{aligned} x^2 - a \equiv 0 \pmod{p_i} \text{ es soluble } \forall i &\iff x^2 - a \equiv 0 \pmod{p_i^{k_i}} \text{ es soluble } \forall i \\ &\iff x^2 - a \equiv 0 \pmod{m} \text{ es soluble.} \end{aligned}$$

□

Proposición 5.3. *Sean $a, b, c \in \mathbb{Z}$ y $m > 1$ impar, tales que $(a, m) = 1$ y $m = p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$, como en la proposición anterior. Consideremos la siguiente ecuación,*

$$aX^2 + bX + c \equiv 0 \pmod{m}. \tag{1}$$

Supongamos además que $(b^2 - 4ac, m) = 1$, entonces la ecuación (1) tiene solución si, y sólo si $\left(\frac{b^2-4ac}{p_i}\right) = 1$ para cada $i = 1, 2, \ldots, n$, donde $\left(\text{-}\right)$ denota al símbolo de Legendre.

Demostración: Debido a que m es impar y $(a, m) = 1$, se tiene que las siguientes ecuaciones son equivalentes.

$$\begin{aligned} aX^2 + bX + c &\equiv 0 \pmod{m}, \\ 4a(aX^2 + bX + c) &\equiv 0 \pmod{m}, \\ 4a^2X^2 + 4abX + 4ac &\equiv 0 \pmod{m} \text{ y} \\ (2aX + b)^2 &\equiv b^2 - 4ac \pmod{m}. \end{aligned}$$

Debido a que $(2a, m) = 1$, entonces $2a$ es una unidad en $\mathbb{Z}/m\mathbb{Z}$, por lo tanto la ecuación (1) es soluble si, y sólo si $b^2 - 4ac$ es un residuo cuadrático módulo m. Aplicando el Teorema 5.1, obtenemos que (1) es soluble si, y sólo si $b^2 - 4ac$ es un residuo cuadrático módulo p_i, para cada $i = 1, 2, \ldots, n$. □

Para ilustrar la proposición anterior analicemos las siguientes dos ecuaciones,

$$5X^2 + 7X + 2 \equiv 0 \pmod{77}. \tag{1}$$

y

$$5X^2 + 7X + 1 \equiv 0 \pmod{77}. \tag{2}$$

Para la primera ecuación tenemos, $(7)^2 - 4(5)(2) = 3^2$, luego $\left(\frac{3^2}{11}\right) = \left(\frac{3^2}{7}\right) = 1$, por lo tanto (1) es soluble.

Para la segunda ecuación tenemos, $(7)^2 - 4(5)(1) = 29$, luego $\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1$, pero $\left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1$, por lo tanto (2) no es soluble.

Enseguida estudiaremos una aplicación de las sumas de Gauss y Jacobi para determinar ciertos elementos construibles.

Definición 5.1. *Se dice que $\alpha \in \mathbb{C}$ es **construible** si existen campos $\mathbb{Q} = K_0, K_1, \ldots, K_n$ y $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ tales que que $\alpha_i \in K_i$, $\alpha \in K_n$ y $K_{i+1} = K_i(\sqrt{\alpha_i})$ para cada $i = 0, 1, \ldots, n-1$.*

Sea $m \in \mathbb{N}$, entonces denotaremos $\zeta_m = e^{2\pi i/m}$.

Proposición 5.4. *Si $n \in \mathbb{Z}$, entonces ζ_{2^n} es construible.*

Demostración: Se procede por inducción. Para $n = 1$, $\zeta_2 = -1$ es construible. Entonces, supongamos que $\zeta_2, \zeta_{2^2}, \ldots, \zeta_{2^k}$ son construibles; puesto que $(\zeta_{2^{k+1}})^2 = \zeta_{2^k}$, tenemos que $\zeta_{2^{k+1}}$ es construible. □

Proposición 5.5.

$$\sum_{\chi} \chi(a) = \begin{cases} 1 & si\ a = 0 \\ p-1 & si\ a = 1 \\ 0 & si\ a \neq 0, 1 \end{cases}$$

donde la suma es sobre todos los caracteres en $\mathbb{F}_p$.

Demostración: Si $a = 0$, entonces $\chi(0) = 0$ para todo $\chi \neq \epsilon$ y $\epsilon(0) = 1$, por lo tanto $\sum_{\chi} \chi(0) = 1$.

Si $a = 1$, entonces $\sum_{\chi} \chi(1) = p-1$, ya que sólo existen $p-1$ caracteres multiplicativos en $\mathbb{F}_p$.

El último caso corresponde a lo probado en el Corolario 3.1.1. □

Notemos que el producto de elementos construibles es construible, y de igual forma la suma de elementos construibles es construible.

Proposición 5.6. *Sea p un primo de Fermat, es decir, $p = 2^n + 1$. Entonces ζ_p es construible.*

Demostración: Por la Proposición 5.5 tenemos

$$\sum_{\chi} g(\chi) = \sum_{t} \sum_{\chi} \chi(t)\zeta_p^t = 1 + (p-1)\zeta_p \ .$$

Luego,

$$\zeta_p = \frac{1}{p-1}(\sum_{\chi} g(\chi) - 1). \tag{1}$$

Demostremos que $g(\chi)$ es construible. Debido a que $p - 1 = 2^n$, entonces el orden de χ es 2^m, con $0 \leq m \leq n$, de aquí surgen los siguientes casos. Si $\chi = \epsilon$, entonces $g(\epsilon) = 0$, entonces $g(\epsilon)$ es construible. Si χ es de orden 2, entonces χ es el símbolo de Legendre, luego $g(\chi)^2 = (-1)^{(p-1)/2}p$, por lo tanto $g(\chi)$ es construible. Por último, si χ es de orden mayor que 2 entonces, al aplicar la Proposición 3.3.2, obtenemos

$$g(\chi)^{2^m} = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{2^m-2}).$$

Además, cada $J(\chi,\chi^i)$ esta formado por sumas de potencias de ζ_{2^n}, luego $J(\chi,\chi^i)$ es construible, por lo tanto $g(\chi)^{2^m}$ es construible, de aquí es fácil ver que $g(\chi)$ también es construible, concluyendo de (1) que ζ_p es construible. □

Las siguientes dos proposiciones involucran el residuo cuadrático de 2.

Proposición 5.7. *Sea $n > 3$ un número natural tal que $n \equiv 3 \pmod 4$ y $q = 2n + 1$ es primo, entonces $2^n - 1$ no es primo.*

Demostración: Como $n \equiv 3 \pmod 4$, entonces $q = 2n+1 \equiv -1 \pmod 8$, luego por la Proposición 1.1.3, 2 es un residuo cuadrático módulo q, es decir, $2^{(q-1)/2} \equiv 1 \pmod q$, luego $2^n - 1 \equiv 0 \pmod q$ y $2^n - 1 \neq q$. Por lo tanto $2^n - 1$ no es primo. □

Por ejemplo, con la ayuda de la proposición anterior, sabemos que $2^{83} - 1$ no es primo ya que $2(83) + 1 = 167$ es primo.

Proposición 5.8. *Sea p primo impar positivo, entonces existen $x, y \in \mathbb{Z}$ tales que $x^2 - 2y^2 = p$ si, y sólo si $p \equiv \pm 1 \pmod 8$.*

Demostración: Tomemos en cuenta que el anillo $\mathbb{Z}[\sqrt{2}]$ es un dominio euclideano con respecto a la función $\delta(x + y\sqrt{2}) = |x^2 - 2y^2|$, la cual cumple que $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)\ \forall \alpha, \beta \in \mathbb{Z}[\sqrt{2}]$, y $\delta(\gamma) = 1$ si, y sólo si γ es unidad en $\mathbb{Z}[\sqrt{2}]$.

Si $p \equiv \pm 1 \pmod 8$ entonces, por la Proposición 1.1.3, existe a tal que $a^2 - 2 \equiv 0 \pmod p$, luego $(a - \sqrt{2})(a + \sqrt{2}) \equiv 0 \pmod p$, de aquí se obtiene que p no es primo en $\mathbb{Z}[\sqrt{2}]$. Luego existen $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ tales que $\delta(\alpha), \delta(\beta) \neq 1$ y $p = \alpha\beta$, por lo tanto $\delta(\alpha) = p$. Hagamos $\alpha = x + y\sqrt{2}$, entonces $|x^2 - 2y^2| = p$, obteniendo los iguientes dos casos:

$$x^2 - 2y^2 = p, \text{ y } x^2 - 2y^2 = -p.$$

Si $x^2 - 2y^2 = -p$, entonces hagamos $x_0 + y_0\sqrt{2} = (x + y\sqrt{2})(1 + \sqrt{2})$ para obtener que $x_0^2 - 2y_0^2 = p$.

Supongamos ahora que existen x, y tales que $x^2 - 2y^2 = p$. Como x es impar, entonces $x^2 \equiv 1 \pmod 8$; además, $2y^2 \equiv 0, 2 \pmod 8$. Por lo tanto, $p = x^2 - 2y^2 \equiv \pm 1 \pmod 8$. □

Enseguida estudiaremos un test de primalidad probabilístico desarrollado por Robert M. Solovay y Volker Strassen, mejor conocido como Test de Primalidad Solovay-Strassen el cual emplea como herramienta principal el símbolo de Jacobi.

Proposición 5.9. *Sea $n > 1$ un entero impar compuesto, entonces existe $1 < b < n$ tal que $(b, n) = 1$ y $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod n$, donde $\left(\text{-}\right)$ representa el símbolo de Jacobi.*

Demostración: Supongamos que existe p primo tal que $p^2|n$, entonces hagamos $b = 1 + n/p$. Notemos que $(b, n) = 1$, $b \equiv 1 \pmod{p}$ y $b \equiv 1 \pmod{n/p}$, por lo tanto

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{n/p}\right) = \left(\frac{1}{p}\right)\left(\frac{1}{n/p}\right) = 1.$$

Además, $b^k = (1 + n/p)^k = \sum_{i=0}^{k} \binom{k}{i} \left(\frac{n}{p}\right)^i$, debido a que $\left(\frac{n}{p}\right)^i \equiv 0 \pmod{n}$ con $i > 1$; luego, $b^k \equiv 1 + (n/p)k \pmod{n}$.

Por lo tanto, $b^{(n-1)/2} \equiv 1 + \left(\frac{n}{p}\right)\left(\frac{n-1}{2}\right) \not\equiv 1 \pmod{n}$ ya que $\left(\frac{n}{p}\right)\left(\frac{n-1}{2}\right) \not\equiv 0 \pmod{n}$. Finalmente hallamos b tal que $(b, n) = 1$ y $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$.

Supongamos ahora que n es libre de cuadrado, sea p primo tal que $p|n$. Sea a tal que $\left(\frac{a}{p}\right) = -1$. Debido a que $(n/p, p) = 1$, por el Teorema Chino del Residuo, existe b tal que

$$b \equiv a \pmod{p} \text{ y } b \equiv 1 \pmod{n/p}.$$

Además, podemos elegir b tal que $1 < b < n$, luego

$$\left(\frac{b}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{1}{n/p}\right) = -1.$$

Puesto que $b \equiv 1 \pmod{n/p}$, se tiene que $b^{(n-1)/2} = 1 + d(n/p)$ con $d \in \mathbb{Z}$. Supongamos que $b^{(n-1)/2} \equiv -1 \pmod{n}$, entonces

$$1 + d(n/p) \equiv -1 \pmod{n} \text{ , es decir, } d(n/p) \equiv 2 \pmod{n}$$

por lo tanto existe c tal que $d(n/p) = 2 + nc$, es decir, $n(d - cp) = 2p$, lo cual contradice el hecho de que n es un entero impar compuesto. En consecuencia, $b^{(p-1)/2} \equiv 1 \pmod{n}$, y por lo tanto $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$.

□

Proposición 5.10. *Sea $n > 1$ un entero impar compuesto, entonces al menos la mitad de los elementos tales que $1 \leq b < n$ y $(b, n) = 1$, cumplen $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$.*

Demostración: Si $(\mathbb{Z}/n\mathbb{Z})^*$ es el conjunto de unidades del anillo $\mathbb{Z}/n\mathbb{Z}$, entonces $(\mathbb{Z}/n\mathbb{Z})^* = \{(a) \mid 1 \leq a < n, (a, n) = 1\}$ es un grupo multiplicativo de orden $\phi(n)$, donde ϕ es la función de Euler.

Sea $A = \{(a) \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}\}$ y $B = \{(b) \in (\mathbb{Z}/n\mathbb{Z})^* \mid b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}\}$, con $A \cup B = (\mathbb{Z}/n\mathbb{Z})^*$. Entonces, por la Proposición 5.9, existe b tal que $(b) \in B$, y para cada $(a) \in A$ se tiene que $(ab) \in B$; por lo tanto $|B| \geq |A|$. Es decir, $|B| \geq \phi(n)/2$. □

Resta por presentar un algoritmo para calcular el símbolo de Jacobi.

Sea $n > 1$ un entero impar y b tal que $1 < b < n$ con $(b, n) = 1$. Sea $-\frac{n-1}{2} \leq b_1 \leq \frac{n-1}{2}$ tal que $b \equiv b_1 \pmod{n}$, entonces

$$\begin{aligned}\left(\frac{b}{n}\right) = \left(\frac{b_1}{n}\right) &= \left(\frac{\pm b_2}{n}\right) \text{ con } 1 < b_2 < \frac{n-1}{2} \\ &= \left(\frac{\pm 1}{n}\right)\left(\frac{b_2}{n}\right).\end{aligned}$$

Sea $b_2 = 2^k b_3$ tal que b_3 es impar, entonces

$$\left(\frac{b}{n}\right) = \left(\frac{\pm 1}{n}\right)\left(\frac{2^k}{n}\right)\left(\frac{b_3}{n}\right).$$

Por los incisos (a) y (b) de la Proposición 1.2.4, podemos calcular $\left(\frac{-1}{n}\right)$ y $\left(\frac{2}{n}\right)$.
Si $b_3 > 1$, entonces aplicamos el inciso (c) de la Proposición 1.2.4 para obtener que

$$\left(\frac{b}{n}\right) = \left(\frac{\pm 1}{n}\right)\left(\frac{2^k}{n}\right)(-1)^{((n-1)/2)((b_3-1)/2)}\left(\frac{n}{b_3}\right).$$

Finalmente, para calcular $\left(\frac{n}{b_3}\right)$ se aplica el mismo procedimiento hasta ahora descrito.

De aquí surge el algoritmo probabilístico de Solovay-Strassen. Sean $b_1, b_2, \ldots, b_k$, k elementos elegidos al azar tales que $1 < b_i < n$ y $(b_i, n) = 1$. Supongamos que $b_i^{(n-1)/2} \equiv \left(\frac{b_i}{n}\right) \pmod{n}$ $\forall i$, entonces la probabilidad de que n sea compuesto es a lo más $\frac{1}{2^k}$.

Conclusiones

En este trabajo se logró demostrar de forma analítica la ley de la reciprocidad cuadrática, para luego demostrar que existe una cantidad infinita de primos de la forma $4k+1$ y $8k+7$, además demostramos que si a no es un cuadrado, entonces existe una cantidad infinita de primos p tales que $\left(\frac{a}{p}\right) = -1$.

La teoría desarrollada sobre las sumas cuadráticas de Gauss nos permitió realizar otra demostración de la ley de la reciprocidad cuadrática de forma más sencilla que la prueba analítica. Y además, logramos determinar el número de soluciones en $\mathbb{F}_p$ de las ecuaciones $X^3 + Y^3 = 1$ y $X_1^2 + X_2^2 + \cdots + X_l^2 = 1$.

Además, mediante el uso de las sumas de Gauss y de las sumas de Jacobi logramos demostrar la ley de la reciprocidad cúbica y su complemento. Dimos una condición necesaria y suficiente sobre $p \equiv 1 \pmod 3$ para que $X^3 \equiv 2 \pmod p$ fuera soluble en $\mathbb{Z}$. De igual forma se logró demostrar la ley de la reciprocidad bicuadrática y un resultado debido a K. Burde, el cual establece la relación que existe entre $\chi_\pi(q)$ y $\chi_\lambda(p)$, con π y $\lambda \in \mathbb{Z}[i]$ primarios tales que, $\pi\overline{\pi} = p$ y $\lambda\overline{\lambda} = q$.

Se logró dar condiciones necesarias y suficientes para las cuales a es un residuo cuadrático módulo m, con $m > 1$ y $(a, m) = 1$, y con ello determinar condiciones suficientes sobre a, b, c y m para que la ecuación $aX^2 + bX + c \equiv 0 \pmod m$ tuviera solución. Demostramos además que todo primo de Fermat es construible, y se determinaron ciertos números de Mersennen $(2^p - 1)$ que son compuestos cuando p es primo, sin embargo no se garantiza que exista una cantidad infinita de números de Mersenne de esta forma.

Se logró además presentar un test probabilístico para determinar la primalidad de $n > 1$ impar, basado principalmente en el hecho que si n es compuesto, entonces al menos la mitad de los elementos $1 \leq b < n$ tales que $(a, b) = 1$, cumplen que $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod n$, y de la facilidad que la ley de la reciprocidad cuadrática brinda para el cálculo del símbolo de Jacobi.

Bibliografía

[1] Everest, Graham y Ward, Thomas, *An introduction to number theory*, Graduate Texts in Mathematics (232), Springer-Verlag, 2005.

[2] Hungerford, T. W., *Algebra*, Springer-Verlag New York Inc., 1974.

[3] Ireland, Kenneth y Rosen, Michael, *A classical introduction to modern number theory*, Graduate Texts in Mathematics (84), Springer-Verlag, 1982.

[4] Janusz, Gerald J., *Algebraic Number Fields*, Graduate Studies in Mathematics (7), American Mathematical Society, Second Edition 1996.

[5] Karpilovsky, Gregory, *Field Theory*, Monographs and Textbooks in Pure an Applied Mathematics (120), Marcel Dekker, 1988.

[6] Lang, Serge, *Algebraic Number Theory*, Graduate Texts in Mathematics (110), Springer-Verlag, 1982.

[7] Nathanson, Melvyn B., *Elementary methods in number theory*, Graduate Texts in Mathematics (195), Springer-Verlag, 2000.

[8] Rademacher, Hans, *Topics in analytic number theory*, Springer-Verlag, 1973.

[9] Ribenboim, Paulo, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[10] Ribenboim, Paulo, *The Book of Prime Number Records*, Springer-Verlag, 1980.

[11] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics (83), Springer-Verlag, 1982.

Índice alfabético