UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LEY DE RECIPROCIDAD CUBICA

TESIS PROFESIONAL
PARA OBTENER EL TITULO DE:
LICENCIADO EN MATEMATICAS
PRESENTA
JESUS GARCIA LOPEZ

CIUDAD UNIVERSITARIA MEXICO, D.F. 1991

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INTRODUCCION

La Ley de reciprocidad cuadrática nos da respuesta a la siguiente pregunta:

Para que primos p, $X^2 \equiv a \pmod{p}$ es soluble. Si la misma pregunta se plantea para $X^n \equiv a \pmod{p}$, entonces nos estamos dirigiendo a las leyes de reciprocidad superior. En este trabajo estudiaremos el caso $n=3$ y por tanto la ley de reciprocidad cúbica.

Vale la pena mencionar que Gauss fue el primero en hacer un estudio muy completo de los residuos cuadráticos. El pensaba que esta teoría se encontraba a tal grado de perfección que no había nada más que hacer por ella, asi, prosiguio su estudio hacia la reciprocidad cúbica y bicuadrática y aunque no tuvo mucho éxito podemos decir que él fue el primero en iniciar una teoría general, la teoría de los números algebraicas.

En el capítulo uno se dan resultados generales sobre el anillo de los enteros de Eisenstein los cuales son indespensables para estudiar la reciprocidad cúbica.

En el capítulo dos se definen caracteres sobre un campo con p elementos $\mathbb{F}_p$, y aunque se pueden definir sobre $\mathbb{F}_{p^n}$, para nosotros será suficiente trabajarlos en $\mathbb{F}_p$. Se estudian también las sumas de Gauss y de Jacobi asi como algunas relaciones entre ellas.

En el capítulo tres se plantea y se prueba la ley de reciprocidad cúbica.

CONTENIDO

CAPITULO UNO / ANILLO DE LOS ENTEROS DE EISENSTEIN

§1

Nuestro punto de partida sera la ecuación:

$$X^3 = 1.$$

Tenemos que:

$$X^3-1=(X-1)(X^2+X+1)=(X-1)\left(X-\frac{-1+i\sqrt{3}}{2}\right)\left(X-\frac{-1-i\sqrt{3}}{2}\right)$$

cuyas raices son 1, $\left(\frac{-1+i\sqrt{3}}{2}\right)$ y $\left(\frac{-1-i\sqrt{3}}{2}\right)$ donde $i=\sqrt{-1}$.

Sea $w=\frac{-1+i\sqrt{3}}{2}=e^{\frac{2\pi i}{3}} \in \mathbb{C}$ y denotamos por $\mathbb{Z}[w]$ el conjunto de números complejos de la forma $a+bw$ donde a y b son enteros, es decir:

$$\mathbb{Z}[w]=\{a+bw \mid a,b \in \mathbb{Z}\}.$$

Con las operaciones de adición y multiplicación de $\mathbb{C}$ inducida en $\mathbb{Z}[w]$ tenemos nuestro primer resultado.

PROPOSICION 1.1.1. $\mathbb{Z}[w]$ es un dominio entero con 1.

Definición. $\mathbb{Z}[w]$ es llamado el anillo de los enteros de Eisenstein.

Observación: $\overline{w}=w^2$, $w^2+w+1=0$, $a+bw=a-b-bw^2$,

y $a+b\bar{w} = a-b-bw$.

De lo anterior se ve que si $\alpha \in \mathbb{Z}[w]$, entonces $\bar{\alpha} \in \mathbb{Z}[w]$.

§2

DIVISIBILIDAD.

Definición. Sean $\alpha, \beta \in \mathbb{Z}[w]$, $\beta \neq 0$, decimos que β divide a α, denotado por $\beta \mid \alpha$, si existe un elemento $\gamma \in \mathbb{Z}[w]$ tal que $\alpha = \beta\gamma$.

Observación. La definición anterior es consistente con la definición de divisibilidad en $\mathbb{Z}$.

Si $a \neq 0$, $b \neq 0$ están en $\mathbb{Z}$ y $b \mid a$ en $\mathbb{Z}[w]$ entonces para alguna $\gamma = c + dw$ tenemos que $a = b\gamma$.

Pero la ecuación $a = b\gamma = bc + bdw$ conduce a:

$a = bc$ y $bd = 0$, y como $b \neq 0$ entonces $d = 0$, γ es un entero. Así $\gamma \in \mathbb{Z}$ y $b \mid a$ en $\mathbb{Z}[w]$ implica $b \mid a$ en $\mathbb{Z}$. ∎

Definición. Sea $\alpha = (a+bw) \in \mathbb{Z}[w]$ definimos la norma de α, $N\alpha$, por la fórmula $N\alpha = \alpha\bar{\alpha} = a^2 - ab + b^2$.

Observaciones:

1) $N\alpha = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4} b^2 =$

$N(\alpha) = (b - \frac{a}{2})^2 + 3(\frac{a}{2})^2$, por tanto, $N\alpha \geq 0$.

2) Es fácil comprobar que para cualquier α y β en $\mathbb{Z}[w]$, entonces $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. Es decir la norma es multiplicativa.

3) De (2) se deduce que:
Si $\alpha | \beta$, entonces $N(\alpha) | N(\beta)$.

Definición. Sea $\alpha = (a+bw) \in \mathbb{Z}[w]$, diremos que α es unidad si $\alpha | u$ donde $u \in \mathbb{Z}[w] - \{0\}$.

Ciertos Enteros Eisenianos dividen a todo entero Eiseniano, denominandose unidades de $\mathbb{Z}[w]$.

PROPOSICION 1.2.1

I) $\alpha \in \mathbb{Z}[w]$ es unidad sii $N(\alpha) = 1$.

II) Las unicas unidades son ± 1, $\pm w$ y $\pm w^2$.

Demostración.

I) $\Leftarrow$] Sea $\alpha \in \mathbb{Z}[w]$, entonces $\bar{\alpha} \in \mathbb{Z}[w]$. Por tanto $\alpha\bar{\alpha} \in \mathbb{Z}[w]$, como $N\alpha = 1$, $\alpha\bar{\alpha} = 1 \in \mathbb{Z}[w]$, lo cual significa que α es unidad.
$\Rightarrow$] Como $\alpha \in \mathbb{Z}[w]$ unidad, entonces existe $\beta \in \mathbb{Z}[w]$

tal que $\alpha\beta = 1 \Rightarrow N\alpha N\beta = 1$ y como $N\alpha$, $N\beta$ son enteros positivos tenemos que $N\alpha = 1$

II) Ahora veamos las unidades.

Si $\alpha \in \mathbb{Z}[w]$ es unidad, entonces α debe tener algunas de las formas ± 1 ó $\pm w$ ó $\pm w^2$.

Sea $\alpha = (a+bw)$ unidad en $\mathbb{Z}[w]$, entonces

$$1 = N\alpha = a^2 - ab + b^2 \Rightarrow 4 = 4a^2 - 4ab + 3b^2 + b^2$$
$$= (2a-b)^2 + 3b^2 \ldots\ldots (*)$$

de lo cual obtenemos:

(1) $2a - b = \pm 1$, $b = \pm 1$ ó

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

(1) supongamos que

(a) $2a - b = 1$ y $b = 1$, entonces $a = 1$ y $b = 1$, es decir, $\alpha = 1 + w = -w^2$

(b) $2a - b = 1$ y $b = -1 \Rightarrow a = 0$ y $b = -1$, por tanto $\underline{\alpha = -w}$

(c) Si $2a - b = -1$ y $b = 1$, entonces $a = 0$ y $b = 1$, por tanto $\underline{\alpha = w}$

(d) Si $2a - b = -1$ y $b = -1$, entonces $\underline{\alpha = w^2}$

(2) Supongamos que:

(a) Si $2a-b=2$ y $b=0$, entonces $\alpha=1$

(b) Si $2a-b=-2$ y $b=0$, entonces $\alpha=-1$

Así que, si α es unidad tenemos que α es de la forma: ± 1 ó $\pm w$ ó $\pm w^2$, es decir, las únicas unidades son ± 1, $\pm w$ y $\pm w^2$.

Ahora notemos un importante detalle:

$7=(3+w)(2-w)=N(3+w)=N(2-w)$.

Como 7 en $\mathbb{Z}$ es primo racional, y $(3+w)$, $(2-w)\in\mathbb{Z}[w]$ tenemos que el número 7 no es primo en los enteros eisenianos. Por 1.2.1. $(3+w)$ y $(2-w)$ no son unidades, entonces cabe preguntar: ¿son primos o no?, contestaremos luego.

Continuando damos la siguiente definición.

Definición.

Si α,β en $\mathbb{Z}[w]$ tales que $\alpha|\beta$ y $\beta|\alpha$, entonces se dice que α y β son asociados.

Definición. Un entero eiseniano que no sea unidad y tal que no tiene más divisores que sus asociados y las unidades, se llama primo en $\mathbb{Z}[w]$ o si, el contexto está bien entendido, simplemente se dice que es un primo.

A veces distinguiremos los dos conceptos de primos, refiriendose a primos eisenianos como primos y los primos de $\mathbb{Z}$ como primos racionales.

Observación.
No existe forma de introducir una relación "$<$" en $\mathbb{Z}[w]$ de tal manera que se cumplan las dos proposiciones siguientes:

(a) $\forall \alpha, \beta \in \mathbb{Z}[w]$, se cumple exactamente una y sólo una de las relaciones:

$$\alpha < \beta \quad o \quad \alpha = \beta \quad o \quad \beta < \alpha$$

(b) Si $\alpha < \beta$ y $o < \gamma$, entonces $\alpha\gamma < \beta\gamma$.

Prueba.
Veamos que bajo cualquier definición de "$\alpha < \beta$" que sea consistente con (a) y (b), necesariamente $o < 1$. Porque en caso contrario por (a) debería tenerse que $o < -1$. Pero entonces por (b) con $\alpha = o$ y $\beta = \gamma = -1$, tendríamos:

$$o < -1 \quad y \quad o < -1 \quad \text{por tanto} \quad o < (-1)^2 = 1 \text{ ¡}$$

Completando la prueba de la imposibilidad afirmada, demostraremos que ninguna de las relaciones:

$$i < 0 \quad o \quad 0 < i \quad ,$$ pueden cumplirse.

Ya que si $i<0$ entonces $0<-i$ de aqui $0<(-i)^2=-1$

$\therefore \; 0<-1$!?

Si $0<i$ entonces $0<(i)^2=-1$!?. ∎

Así hay una clase "débil" de comparación de los elementos de $\mathbb{Z}[w]$, comparando normas. De esta forma se desprende un teorema importante, $\mathbb{Z}[w]$ es anillo euclideano.

Observaciones.

1) $\forall \alpha \in \mathbb{Z}[w]$ no cero se tiene $N\alpha > 0$, es decir, $N\alpha$ es nuestra función-euclideano en la definición de anillo euclideano

2) $\forall \alpha, \beta \in \mathbb{Z}[w]$, entonces $N(\alpha\beta) = N\alpha \cdot N\beta$.

Si $\beta \neq 0$, entonces $N(\beta) \geq 1$, $N\alpha = N\alpha \cdot 1 \leq N\alpha \cdot N\beta$

$\therefore N\alpha \leq N\alpha \cdot N\beta = N\alpha\beta$, $N\alpha \leq N\beta\alpha$.

TEOREMA 1. $\mathbb{Z}[w]$ es anillo euclideano.

Demostración. Tomando en cuenta las observaciones (1) y (2), basta demostrar que: Si $\alpha, \beta \in \mathbb{Z}[w]$, $\beta \neq 0$, entonces existen $\gamma, \rho \in \mathbb{Z}[w]$ tales que

$\alpha = \beta\gamma + \rho$ donde $\rho = 0$ o $N\rho < N\beta$.

Demostración.

Como $\beta \neq 0$, podemos escribir

$$\frac{\alpha}{\beta} = \frac{a+bw}{c+dw} = \frac{(a+bw)(c+d\bar{w})}{(c+dw)(c+d\bar{w})} = \frac{(ac+bd-ad)+(bc-ad)w}{c^2-cd+d^2},$$

$(\bar{w} = w^2)$

entonces $\frac{\alpha}{\beta} = r + sw$ ——— (*)

donde $r = \frac{ac+bd-ad}{c^2-cd+d^2}$ y $s = \frac{bc-ad}{c^2-cd+d^2}$ son números racionales, no necesariamente enteros.

Como $r \in \mathbb{Q}$ entonces existen $(q-1)$ y q en $\mathbb{Z}$ tales que $q-1 < r < q$ $(|(q-1)-q| = 1)$, entonces

$$|r-(q-1)| \leq \frac{1}{2} \quad \text{o} \quad |r-q| \leq \frac{1}{2}.$$

Así tomamos m $(m = q-1$ o $m = q)$ el más cercano a r tal que $|r-m| \leq \frac{1}{2}$.

Haciendo lo mismo para s, tenemos que existe $n \in \mathbb{Z}$ tal que $|s-n| \leq \frac{1}{2}$.

Por tanto $(r-m)^2 \leq \frac{1}{4}$ y $(s-n)^2 \leq \frac{1}{4}$ ——— (1)

Entonces

$\frac{\alpha}{\beta} - (m+nw) = (r-m)+(s-n)w$ implica

$N\left[\frac{\alpha}{\beta} - (m+nw)\right] = N\left[(r-m)+(s-n)w\right] = (r-m)^2 - (r-m)(s-n) + (s-n)^2 \leq$

$\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} < 1 \quad \therefore N\left[\frac{\alpha}{\beta} - (m+nw)\right] < 1.$

Ahora si hacemos: $\gamma = m+nw$ y $\alpha - \beta(m+nw) = \rho$,

entonces $\alpha = \beta\gamma + \rho$ y $N\left(\frac{\alpha}{\beta} - \gamma\right) < 1$.

Ahora $N\rho = N(\alpha - \beta\gamma) = N\left[\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right] = N\beta \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) <$

$< N\beta \quad \therefore N\rho < N\beta$. Es decir, para $\alpha, \beta \in \mathbb{Z}[w]$, $\beta \neq 0$, Tenemos que existen γ, ρ en $\mathbb{Z}[w]$ tal que

$$\alpha = \beta\gamma + \rho \quad \text{donde } \rho = 0 \text{ o } N\rho < N\beta.$$

COROLARIO 1. $\mathbb{Z}[w]$ es un dominio de ideales principales.

COROLARIO 2. $\mathbb{Z}[w]$ es un dominio de factorización única.

TEOREMA 2. La expresión de un entero de $\mathbb{Z}[w]$ como producto de primos es única.

En base al teorema I, se puede generalizar el algoritmo euclideano de $\mathbb{Z}$ a los enteros eisenianos, en la siguiente forma:

$$\alpha = \beta\gamma_1 + \rho_1 \qquad \text{donde} \quad N\rho_1 < N\beta$$
$$\beta = \rho_1\gamma_2 + \rho_2 \qquad N\rho_2 < N\rho_1$$
$$\vdots$$
$$\rho_{n-2} = \rho_{n-1}\gamma_n + \rho_n \qquad N\rho_n < N\rho_{n-1}$$
$$\rho_{n-1} = \rho_n\gamma_{n+1}$$

La secuencia de ecuaciones termina porque $N\beta, N\rho_1, \ldots, N\rho_2, \ldots$ es una sucesión decreciente de enteros positivos.

Puede verse que ρ_n, último residuo que no se anula, es un divisor tanto de α como de β, considerando las ecuaciones de la última a la primera y así mismo puede probarse que todo divisor común de α y β es un divisor de ρ_n, considerando ahora las ecuaciones anteriores de la primera a la última; de la penúltima ecuación, puede escribirse ρ_n como combinación lineal de ρ_{n-1} y ρ_{n-2}; $\rho_{n-1}, \rho_{n-2}, \ldots, \rho_1$ pueden ser eliminadas con las ecuaciones anteriores, para dar a ρ_n una combinación lineal de α y β.

Asi ρ_n es un entero eiseniano con todas las propiedades del número δ en la siguiente proposición.

PROPOSICION 1.2.2.

Sean $\alpha, \beta \in \mathbb{Z}[w]$, al menos uno de ellos no cero, entonces existe un entero $\delta \in \mathbb{Z}[w]$ con las siguientes propiedades:

I) $\delta \mid \alpha$ y $\delta \mid \beta$.

II) Si $\delta' \in \mathbb{Z}[w]$ tal que $\delta' \mid \alpha$ y $\delta' \mid \beta$, entonces $\delta' \mid \delta$.

III) Existen ξ y η en $\mathbb{Z}[w]$ tales que $\delta = \alpha\xi + \beta\eta$.

Dos enteros δ_1 y δ_2 cualesquiera que tienen las propiedades (I) y (II) son asociados.

La prueba es esencialmente la misma en cualquier anillo euclideano.

Asi' cualquier $\delta \in \mathbb{Z}[w]$ con propiedades (I) y (II) se llama M.C.D de α y β y escribimos $(\alpha, \beta) = \delta$ (estrictamente seria $(\alpha, \beta) \in \{\pm\delta, \pm w\delta, \pm w^2\delta\}$).

Observación. Si $(\alpha, \beta) = 1$ decimos que α y β son primos relativos.

Ejemplo.

Encontrar el M.C.D de $(11+12w)$ y de $(3+2w)$

Como

$$7 = N(3+2w) < N(11+12w) = 133,$$ entonces

$$\frac{11+12w}{3+2w} = \frac{(11+12w)(3+2w^2)}{N(3+2w)} = \frac{(33+24-22)+(36-22)w}{7} =$$

$$= \frac{35}{7} + \frac{14}{7}w = 5+2w \Rightarrow 11+12w = (3+2w)(5+2w)+0$$

entonces $(11+12w, 3+2w) = 3+2w$

PROPOSICION 1.2.3

Si $(\alpha,\beta)=1$ y $\alpha \mid \beta\gamma$, entonces $\alpha \mid \gamma$.

Demostración.

Como $(\alpha,\beta)=1$ entonces existen ξ y η en $\mathbb{Z}[2w]$ tales que $1=\alpha\xi+\beta\eta$, por tanto

$$\alpha\gamma\xi + \beta\gamma\eta = \gamma \quad (*)$$

pero α divide a $\beta\gamma$ y a $\alpha\gamma$ entonces α divide a cualquier combinación de ellos así por (*) tenemos que α divide a esa combinación, é.e., $\alpha \mid \gamma$. ∎

PROPOSICION 1.2.4.

Si $\pi, \pi_1, \pi_2, \ldots, \pi_n$ son primos eisenianos y $\pi \mid \prod_{i=1}^{n} \pi_i$, entonces por lo menos para una m, π es un asociado de π_m.

Demostración.

Si π es diferente a cualquiera de los valores $\pi_1, \pi_2, \ldots \pi_{n-1}$. Entonces π es primo relativo con el producto, $\pi_1 \cdot \pi_2 \cdots \pi_{n-1}$ (esto se deduce del hecho de que si $(\alpha,\beta)=1$ y $(\alpha,\gamma)=1$ entonces $(\alpha,\beta\gamma)=1$) entonces

$$(\pi,\ \pi_1\cdot\pi_2\cdots\pi_{n-1})=1 \quad y \quad \pi \Big| (\pi_1\cdot\pi_2\cdots\pi_{n-1})\cdot\pi_n$$

se tiene que

$$\pi/\pi_n \quad \text{por 1.2.3.}$$

Como π y π_n son primos, y π/π_n entonces π y π_n son asociados, n es igual a m ■

§ 3

PRIMOS EN $\mathbb{Z}[w]$.

PROPOSICION 1.3.1

Si $\pi \in \mathbb{Z}[w]$ es primo, entonces existe un primo-racional p tal que $N(\pi)=p$ o $N(\pi)=p^2$.

En el primer caso π no es asociado con p y en el otro caso π es asociado con p.

Demostración:

Sea q entero racional (no-primo) entonces sea

$$q=\prod_{i=1}^{n} p_i \quad \text{donde } p_i \text{ es primo-racional para } 1\le i\le n$$

y sup $\underline{q = N\pi}$, por lo tanto

$p_1 \cdot p_2 \cdots p_n = \pi\overline{\pi}$, entonces $\pi \mid \prod_{k=1}^{n} p_k$ de e/lo

$\pi \mid p_i$ para alguna i , sea $p_i = p$, por tanto $\pi \mid p$,

implica que $p = \pi\gamma$, para alguna $\gamma \in \mathbb{Z}[\omega]$, aplicando norma tenemos $p^2 = (N\pi)(N\gamma)$, entonces

$$\left(N(\pi) = p^2 \text{ y } N\gamma = 1\right) \overset{(1)}{\longrightarrow} \left(N\pi = p\right) \overset{(2)}{\longrightarrow}$$

Si sucede (1), significa que γ es unidad, entonces π es asociado con p.

De (2) tenemos que π no es asociado con p.

Ya que si no, sea $\pi = u q^*$ donde u-unidad y q^* - primo racional, entonces

$$p = N\pi = (Nu)(Nq^*) = Nq^* = (q^*)^2 \Longrightarrow p = (q^*)^2$$

lo cual es absurdo ya que p y q^* son primos-racionales.

Por tanto π no es asociado con p, como se afirmaba ■

A continuación damos un resultado que es importante por su naturaleza misma.

PROPOSICION 1.3.2

Si $\pi \in \mathbb{Z}[w]$ tal que $N(\pi)=p$, p-primo racional, entonces π es primo.

Demostración.

Supongamos que π no es primo. Sea $\pi=\gamma\beta$ donde $N(\beta), N(\gamma) > 1$.

Ahora por hipótesis sabemos que $N(\pi)=p$, p-primo-racional, por lo tanto:

$p= N(\pi)= N(\gamma\beta)= N(\gamma)N(\beta)$, es decir, $p = N(\gamma)N(\beta)$ ∇ ya que p-es primo racional y $N\gamma>1, N\beta>1$. De esta manera tenemos que π es primo en $\mathbb{Z}[w]$. ∎

Ahora contestando una pregunta anterior, con respecto a los ejemplos anteriores, tenemos que:

1) $\frac{5}{2} + \frac{i\sqrt{3}}{2} = 3+w$ y $N(3+w)=7$ entonces $3+w$ es primo en $\mathbb{Z}[w]$.

2) $\frac{5}{2} - \frac{i\sqrt{3}}{2} = 2-w$ y $N(2-w)= 7$ entonces $2-w$ es primo en $\mathbb{Z}[w]$.

Observación. (1) ¿Que primos racionales son primos en $\mathbb{Z}[w]$?, por ejemplo ¿podemos decir que los primos racionales de la forma $3n+1$ no son primos en $\mathbb{Z}[w]$?.

Observación 2. Sea $p \in \mathbb{Z}$ entonces $p \in \mathbb{Z}[w]$.
Si p es primo racional y no es primo en $\mathbb{Z}[w]$ entonces sea $p = \pi\gamma$ donde $N(\pi), N(\gamma) > 1$, de lo cual tenemos: $p^2 = N(\pi)N(\gamma)$ entonces

$p = N(\pi)$.

Por otro lado sea $\pi = (a+bw)$ entonces

$4p = (2a-b)^2 + 3b^2$ implica que: $p \equiv (2a-b)^2 \pmod 3$.

Supongamos que $3 \nmid p$ entonces todo número al cuadrado módulo 3 es 0 ó 1, pero como $3 \nmid p$, tenemos que solamente es 1, es decir, $p \equiv 1 \pmod 3$.

Resumiendo.
Sea $p \in \mathbb{Z}$ primo racional, $(3,p)=1$ y p no es primo en $\mathbb{Z}[w]$ entonces $p \equiv 1 \pmod 3$.

PROPOSICION 1.3.3.
Sean p, q primos racionales, entonces:

I) Si $q \equiv 2 \pmod 3$, entonces q es primo en $\mathbb{Z}[w]$.
II) Si $p \equiv 1 \pmod 3$, entonces $p = \pi\bar{\pi}$, con π primo en $\mathbb{Z}[w]$.
III) Vea que $3 = -w^2(1-w)^2$, $1-w$ es primo en $\mathbb{Z}[w]$.

Demostración.

I) Si $q \in \mathbb{Z}[w]$ no es primo. Sabemos que $(3,q)=1$ y por obs (2) tenemos que $q \equiv 1 \pmod 3$ ó y a que $q \equiv 2 \pmod 3$ por hipótesis. Por tanto q es primo en $\mathbb{Z}[w]$.

II) Como $p \equiv 1 \pmod 3$ entonces

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}=(-1)^{p-1}\left(\frac{1}{3}\right)=1,$$

Por tanto $\left(\frac{-3}{p}\right)=1$, la decir, -3 es residuo cuadrático módulo p, lo cual implica que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -3 \pmod p$ por tanto:

$$p \mid a^2+3=\left(a-\sqrt{-3}\right)\left(a+\sqrt{-3}\right)=\left(a+1+2\left[-\frac{1+i\sqrt{3}}{2}\right]\right)\left(a+1+2\left[\frac{-1+i\sqrt{3}}{2}\right]\right)=$$

$$=\left((a+1)+2\bar{w}\right)\left((a+1)+2w\right), \text{ i.e, } p \mid \left((a+1)+2\bar{w}\right)\left((a+1)+2w\right)$$

Si P fuera primo en $\mathbb{Z}[w]$ entonces por 1.2.4

$p \mid (a+1)+2\bar{w}$ ó $p \mid (a+1)+2w$ lo que implica que

$\frac{(a+1)}{p}+\frac{2}{p}\bar{w} \in \mathbb{Z}[w]$ ó $\frac{a+1}{p}+\frac{2}{p}w \in \mathbb{Z}[w]$, lo que implica que $\frac{a+1}{p}$ y $\frac{2}{p} \in \mathbb{Z}$! porque $p \neq 2$.

Por lo tanto p no es primo en $\mathbb{Z}[w]$. Así, sea

$p = \pi\gamma$ donde π y γ no son unidades con π primo, entonces $p^2 = N(\pi)N(\gamma)$ implica que:

(1) $N(\pi) = p$, $N(\gamma) = p$, o

(2) $N(\pi) = p^2$ y $N(\gamma) = 1$.

De lo cual obtenemos que $N(\pi) = p$ ∴ $\pi\bar{\pi} = p$

donde π es primo en $\mathbb{Z}[w]$.

Y como $p = \pi\gamma$ tenemos que $\gamma = \bar{\pi}$.

Nota: Si $N(\pi) = p$ entonces $p \equiv 1 \pmod 3$

III) Inmediato de $x^3 - 1 = 0$. ∎

Observación.

Por (III) tenemos que $3 = -w^2(1-w)^2$ ..... (*)

y $N(1-w) = 3$ entonces por 1.3.2 $1-w$ es primo en $\mathbb{Z}[w]$. Así de (*) 3 es producto de más de un primo en $\mathbb{Z}[w]$, por lo tanto 3 no es primo eiseniano.

COROLARIO.

Los primos en $\mathbb{Z}[w]$ son:

I) $1-w$ y sus asociados

II) Los primos racionales de la forma $3n+2$ y sus asociados.

III) Los factores $a+bw$ de los primos racionales de la forma $3n+1$.

Demostración. Basta demostrar que son todos los primos. Supongamos que π fuera otro primo diferente a los anteriores. Sea $\pi\bar{\pi} = N(\pi) \in \mathbb{N}$, $N(\pi)>1$ puesto que π no es una unidad, ya que es un primo. $\pi\bar{\pi} = p_1 p_2 \cdots p_s$, entonces $\pi \mid p_i =: p$, para algún $i \in \{1,2,\ldots,s\}$, así que:

Caso(1) Si p no es primo en $\mathbb{Z}[w]$ por lo tanto $p \equiv 1 \pmod 3$ $\not\Rightarrow_0$, ya que sería alguno de los anteriores.

Caso(2) Si π es asociado con p y $p \not\equiv 1 \pmod 3$, $p \not\equiv 2 \pmod 3$, entonces π es asociado de $p \equiv 0 \pmod 3$ por lo tanto π es asociado de 3 $\not\Rightarrow$, ya que 3 no es primo en $\mathbb{Z}[w]$. ∎

Veamos nuestra proxima sección, "Clases-Residuales."

§ EL ANILLO DE LAS CLASES RESIDUALES

La noción de congruencia es extremadamente útil en $\mathbb{Z}[w]$.

Como en $\mathbb{Z}$ tenemos que "$a \equiv b \pmod{n}$ si y sólo si $n \mid a-b$". En $\mathbb{Z}[w]$ tenemos algo análogo.

Definición.

Sean α, β y γ en $\mathbb{Z}[w]$ y $\gamma \neq 0$, no unidad,

decimos que:

$$\alpha \equiv \beta \pmod{\gamma} \text{ si: } \gamma \mid \alpha - \beta.$$

En $\mathbb{Z}$ las clases residuales juegan un papel primordial. Así, las clases residuales módulo γ pueden ser introducidas en $\frac{\mathbb{Z}[w]}{\gamma\mathbb{Z}[w]}$.

De esta manera hablaremos del cociente y diremos

que $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ es el anillo de las clases residuales.

PROPOSICION 1.4.1.
Sea π primo en $\mathbb{Z}[\omega]$, entonces $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ es campo finito y $\left|\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]\right| = N\pi$.

Demostración.
Basta ver que todos los elementos no cero en $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ forman un grupo abeliano bajo la multiplicación.
Sea $\alpha \in \mathbb{Z}[\omega]$ tal que $\alpha \not\equiv 0 \pmod{\pi}$ y π primo, entonces $(\pi, \alpha) = 1$ por tanto existen $\beta, \gamma \in \mathbb{Z}[\omega]$ tal que $\beta\alpha + \pi\gamma = 1$, ésto implica que $\beta\alpha \equiv 1 \pmod{\pi}$ y por tanto α es unidad en $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, i.e., es campo.

Ahora veamos el número de elementos que tiene.
caso (1)
Supongamos que $\pi = q \equiv 2 \pmod 3$, $\pi = a + b\omega$.
Afirmamos que el conjunto $\{a + b\omega \mid 0 \le a < q \text{ y } 0 \le b < q\}$ es un conjunto completo de representantes, cuyo número es q^2. Ésto probará que $\left|\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]\right| = N\pi = Nq = q^2$

elementos.

Sea $\mu = (m+nw) \in \mathbb{Z}[w]$ y supongamos que:

$m = qs + a$

$n = qt + b$ donde s, t, a, b en $\mathbb{Z}$, $0 \leq a < q$ y $0 \leq b < q$

Sustituyendo m, n en μ tenemos que:

$\mu = (qs+a) + (qt+b)w = q(s+tw) + (a+bw) \equiv (a+bw) \pmod{q}$,

$\mu \equiv (a+bw) \pmod{q}$, es decir, $\forall \mu \in \mathbb{Z}[w]$ es congruente a un representante del conjunto dado módulo q.

Ahora veamos que todos los elementos son distintos.

Supongamos que:

$(a+bw) \equiv (a'+b'w) \pmod{q}$, donde $0 \leq a < q$, $0 \leq a' < q$, $0 \leq b < q$ y $0 \leq b' < q$, entonces $(a-a') + (b-b')w \equiv 0 \pmod{q}$, es decir, $\left[\left(\frac{a-a'}{q}\right) + \left(\frac{b-b'}{q}\right)w\right] \in \mathbb{Z}[w]$ de lo cual obtenemos que $\left(\frac{a-a'}{q}\right), \left(\frac{b-b'}{q}\right) \in \mathbb{Z}$ (*). Sean $a \geq a' \geq 0$ y $b \geq b' \geq 0$ **ésto implica que:**

$0 \leq a-a' < q$ y $0 \leq b-b' < q$, $0 \leq \frac{a-a'}{q} < 1$ y $0 \leq \frac{b-b'}{q} < 1$, entonces $\frac{a-a'}{q} = 0$ y $\frac{b-b'}{q} = 0$ por *, por tanto $a = a'$ y $b = b'$.

Resumiendo, los representantes del conjunto son distintos y es un conjunto completo de representantes de $\mathbb{Z}[w]/q\mathbb{Z}[w]$

por lo tanto $N\pi = Nq = q^2$. Así $\left|\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right| = N\pi$.

Caso (2). Supongamos que $N\pi = p$, p-primo racional.

Afirmamos que: $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-2}, \overline{p-1}\}$ es un conjunto completo de representantes de $\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}$, esto probará que tiene $p = N\pi$ elementos.

Veámoslo:

Sea $\pi = a + bw$ y $N\pi = p$, por tanto $p = a^2 - ab + b^2$ ..... (*)

de lo cual tenemos que $p \nmid b$.

Porque si $p \mid b$, y $p = a^2 - ab + b^2$, entonces $a^2 \equiv 0 \pmod{p}$ lo cual es imposible. Por tanto $p \nmid b$, entonces $(p, b) = 1$.

Sea $u = (m + nw) \in \mathbb{Z}[w]$ y $(p, b) = 1$ entonces existe $c \in \mathbb{Z}$ tal que $bc \equiv n \pmod{p}$ ..... (**). Así,

$u - c\pi = (m + nw) - c(a + bw) = m + nw - ca - (cb)w$, es decir,

$u - c\pi \equiv (m + nw - ca - nw) \pmod{p}$, por (**) ∴

$u - c\pi \equiv (m - ca) \pmod{p}$, así tendremos que

$u - c\pi = (m - ca) + pt$ para algún $t \in \mathbb{Z}$, $p = \pi\bar{\pi}$,

$= (m - ca) + \pi(\bar{\pi}t)$, es decir,

$u - c\pi \equiv (m - ca) \pmod{\pi}$ ..... (***).

Ahora, sea $l \in \mathbb{Z}$ y $l = sp + r$, donde $0 \leq r < p$, entonces $l \equiv r \pmod{p}$ implica que $l \equiv r \pmod{\pi}$, con r entero. Como l es arbitrario y por (***) tenemos que $u \equiv r \pmod{\pi}$, donde $r \in \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$.

Así todo elemento de $\mathbb{Z}[\omega]$ es congruente a un elemento de $\{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ módolo π, π primo.

Afirmamos que: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}$ son distintos módulo π.

Supongamos que no, es decir que:

$r \equiv r' \pmod{\pi}$ entonces $r - r' = \gamma\pi$, $\gamma \in \mathbb{Z}[\omega]$ y $0 \leq r < p$, $0 \leq r' < p$, enteros, ésto implica que:

$N(r-r') = N(\gamma\pi)$ $\therefore$ $(r-r')^2 = p\,N\gamma$, ya que $N\pi = p$,

por tanto $p \mid (r-r')^2 \Rightarrow p \mid r-r' \rightarrow r \equiv r' \pmod{p}$, es decir,

$r = r'$ por ser clases residuales.

Así el número de elementos de $\dfrac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}$ es $N\pi = p$, p primo racional.

Caso (3) Sea $\pi = 1 - \omega$, hay que ver que:

$N\pi = N(1-\omega)$ es el número de elementos de $\dfrac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}$.

Por lo anterior, propongo que $\{\bar{0}, \bar{1}, \bar{2}\} \simeq \left(\dfrac{\mathbb{Z}[\omega]}{(1-\omega)\mathbb{Z}[\omega]}\right)$

Basta ver que: $\frac{\mathbb{Z}[w]}{(1-w)\mathbb{Z}[w]} \subset \{\bar{0}, \bar{1}, \bar{2}\}$.

Vemos que: $1-w = 1+(-1)w$, $3 = N(1-w) = 1^2 - 1(-1) + (-1)^2$ y $3 \nmid (-1)$, es decir, $(3,-1)=1$, por tanto existe $c \in \mathbb{Z}$ tal que $c(-1) \equiv n \pmod 3$.

Sea $u = m+nw$. Así $u - c(1-w) = m+nw-c-cw$ ∴

$u - c(1-w) \equiv (m-cw-c+cw) \pmod 3$ entonces

$u \equiv m-c \pmod{1-w}$, $m, c \in \mathbb{Z}$ ..... (1),

es decir, cualquier elemento de $\mathbb{Z}[w]$ es congruente a un entero, $m-c$, racional módulo $(1-w)$.

Ahora sea $l \in \mathbb{Z}$ tal que: $l = 3s+r$, $0 \leq r < 3$, entonces $l \equiv r \pmod 3$ implica que $l \equiv r \pmod{1-w}$ ... (2).

Como l fue arbitrario y es congruente a r módulo $(1-w)$.

De (1) y (2) obtenemos que:

$u \equiv r \pmod{1-w}$, donde $r \in \{\bar{0}, \bar{1}, \bar{2}\}$, por consiguiente $\{\bar{0}, \bar{1}, \bar{2}\} \simeq \frac{\mathbb{Z}[w]}{(1-w)\mathbb{Z}[w]}$ y

$\left| \frac{\mathbb{Z}[w]}{(1-w)\mathbb{Z}[w]} \right| = N\pi = N(1-w) = 3$, número de elementos. ■

Veamos nuestro último resultado en este capítulo.

COROLARIO

I) Sea $\pi=(a+bw)$ primo. Si $p=a^2-ab+b^2=N(\pi)$, p primo racional. Entonces

$\left(\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right)\approx \mathbb{F}_p$, donde $\mathbb{F}_p$ es el campo finito con p elementos.

II) Si $N\pi=p^2$, Entonces $\left(\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right)\approx \mathbb{F}_{p^2}$, donde $\mathbb{F}_{p^2}$ es el campo finito con p^2 elementos.

III) Si $\pi=(1-w)$. Entonces $\left(\frac{\mathbb{Z}[w]}{(1-w)\mathbb{Z}[w]}\right)\approx \mathbb{F}_3$.

CAPITULO DOS/ SUMAS DE GAUSS Y JACOBI

§ 1. CARACTERES MULTIPLICATIVOS.

Definición. Un carácter multiplicativo sobre $\mathbb{F}_p$ (campo) es un homomorfismo.

$$\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*.$$

El conjunto de caracteres de $\mathbb{F}_p$ no es vacío pues por lo menos $\chi(a) = \left(\frac{a}{p}\right)$ símbolo de Legendre $\forall a \in \mathbb{F}_p^*$ y $\varepsilon(a) = 1 \quad \forall a \in \mathbb{F}_p^*$, son ejemplos de caracteres sobre $\mathbb{F}_p$. Ahora extendemos la definición a todo $\mathbb{F}_p$. $\varepsilon(0) = 1$ y si $\chi \neq \varepsilon$ entonces $\chi(0) = 0$. Veamos nuestro primer resultado.

PROPOSICION 2.1.1
Sea χ carácter multiplicativo y $a \in \mathbb{F}_p^*$, entonces

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

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

III) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

Demostración.

I) $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$ entonces $\chi(1) = 1$.

II) Sea $a \in \mathbb{F}^*$ entonces $a^{p-1} \equiv 1 \pmod{p}$ y por tanto

$$1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}.$$

III) Se afirma que: $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Como $1 = \chi(1) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$ entonces $\chi(a^{-1}) = \chi(a)^{-1}$.

Ahora por (II) $\chi(a)^{p-1} = 1$ y asi $|\chi(a)| = 1$, además $|\chi(a)|^2 = \chi(a)\overline{\chi(a)}$, entonces $1 = \chi(a)\overline{\chi(a)}$.

Por tanto $\chi(a)^{-1} = \overline{\chi(a)}$, y de aquí:

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

PROPOSICION 2.1.2.

Sea χ carácter multiplicativo.

I) Si $\chi \neq \varepsilon$ entonces $\sum_{t \in \mathbb{F}_p} \chi(t) = 0$

II. Si $\chi = \varepsilon$ entonces $\sum_{t} \chi(t) = p$.

Demostración.

I. si $\chi \neq \varepsilon$ existe $a \in \mathbb{F}_p^*$ talque $\chi(a) \neq \varepsilon(a) = 1$.

Sea $T := \sum_{t \in \mathbb{F}_p} \chi(t)$, entonces

$\chi(a)T = \chi(a)\sum_{t \in \mathbb{F}_p} \chi(t) = \sum_{t \in \mathbb{F}_p} \chi(at) = T$, por lo tanto

$T(\chi(a)-1) = 0$ y $\chi(a) \neq 1$, así que $T = 0$.

II) Si $\chi = \varepsilon$, tenemos $\sum_t \chi(t) = \sum_t \varepsilon(t) = \sum_t (1) = p$.

Definición. Sean χ y λ caracteres sobre $\mathbb{F}_p$. Entonces

$\chi\lambda : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ definida por $\chi\lambda(a) = \chi(a)\lambda(a)$.

y

$\chi^{-1} : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ definida por $\chi^{-1}(a) = \chi(a^{-1})$.

Son caracteres multiplicativos sobre $\mathbb{F}_p$ ——(*).

Sea $\mathcal{F}$ el conjunto formado por todos los **caracteres sobre** $\mathbb{F}_p$, entonces por lo anterior $\mathcal{F}$ tiene estructura de grupo, y el siguiente resultado nos da una descripción más precisa de $\mathcal{F}$.

PROPOSICION 2.1.3.

$\mathcal{F}$ es un grupo cíclico de orden $p-1$.
Si $a \in \mathbb{F}_p^*$ y $a \neq 1$ entonces existe un carácter χ tal que $\chi(a) \neq 1$.

Demostración.
Sabemos que $\mathbb{F}_p^*$ es cíclico. Entonces sea $g \in \mathbb{F}_p^*$ generador y $a \in \mathbb{F}_p^*$ cualquiera, así que $a = g^l$ para alguna $l \in \mathbb{Z}$.
Por otro lado sea $\chi \in \mathcal{F}$ entonces $\chi(a) = \chi(g)^l$, lo

lo cual significa que $\chi(a)$ depende solo del valor de $\chi(g)$, como $\chi(g)$ es una $(p-1)$ raíz de la unidad, por 2.1.1, y $\mathbb{F}_p^*$ tiene $\varphi(p-1)$ generadores, entonces hay a lo más $\varphi(p-1)$ caracteres, por tanto $|\overline{G}| \leq p-1$.

Definimos ahora $\lambda(g^k) := e^{\frac{2\pi i k}{p-1}}$, λ es un carácter y está bien definido. Sea $n = o(\lambda)$ entonces

$n = o(\lambda) \leq o(\overline{G}) \leq p-1$, i.e., $n \leq p-1$ ..... (1).

Por otro lado tenemos que $\lambda^n(g) = e^{2\pi i\left(\frac{n}{p-1}\right)} = 1$, i.e.,

$e^{2\pi i\left(\frac{n}{p-1}\right)} = 1$ sii $p-1 \mid n$, lo cual significa que $p-1 \leq n$ ....(2).

De (1) y (2) $n = p-1$, por tanto $|\overline{G}| = p-1$ y $\overline{G} = \langle \lambda \rangle$.

Para la segunda parte de la proposición consideremos a $\chi := \lambda$, entonces si $a \in \mathbb{F}_p^*$, $a = g^l$ y $p-1 \nmid l$, por tanto $\lambda(a) = \lambda(g^l) = e^{2\pi i\left(\frac{l}{p-1}\right)} \neq 1$. ∎

COROLARIO.
Si $a \in \mathbb{F}_p^*$ y $a \neq 1$, entonces $\sum_{\chi \in \overline{G}} \chi(a) = 0$.

Demostración.
Por 2.1.3 existe λ carácter tal que $\chi(a) \neq 1$, i.e.,

$\lambda(a)-1\neq 0$. Sea $T:=\sum_{\chi}\chi(a)$, entonces:

$\lambda(a)T=\lambda(a)\sum_{\chi\in E}\chi(a)=\sum_{\lambda\chi\in E}\lambda\chi(a)=T$ por lo tanto

$\lambda(a)T=T$ implica que $T(\lambda(a)-1)=0$ y $T=0$. ∎

Ahora veremos que los caracteres tienen relación con el estudio de ciertas ecuaciones diofantinas.
Sea $x^n=a$ para $a\in\mathbb{F}_p^*$. Se sabe que esta ecuación tiene soluciones sii $a^{\frac{p-1}{d}}\equiv 1 \pmod p$, donde $d=(n,p-1)$, y si tiene una solución entonces existen d-soluciones exactamente.
Utilizaremos lo anterior en el siguiente resultado.

PROPOSICION 2.1.4.
Si $a\in\mathbb{F}_p^*$, $n\mid p-1$ y $x^n=a$ no es soluble, entonces existe un carácter χ tal que:
I) $\chi^n=\varepsilon$
II) $\chi(a)\neq 1$.

Demostración.
Sea λ un generador de E y g un generador de $\mathbb{F}_p^*$, definimos $\chi:=\lambda^{\frac{p-1}{n}}$, entonces $\chi\in E$. Veamos que

se cumplen (I) y (II).

Por 2.1.2 $\chi(g) = \lambda^{\frac{p-1}{n}}(g) = e^{2\pi i \frac{1}{n}}$. Sea $a = g^l$

ahora por hipótesis $x^n \equiv a \pmod p$ no es soluble, es decir;

$x^n \equiv g^l \pmod p$ no es soluble, así $\left(g^l\right)^{\frac{p-1}{n}} \neq 1$ sii $n \nmid l$,

por tanto $\chi(a) = \chi(g)^l = e^{2\pi i \frac{l}{n}} \neq 1$, i.e., $\chi(a) \neq 1$.

Es claro que $\chi^n = \varepsilon$.

PROPOSICION 2.1.5.

Para $a \in \mathbb{F}_p$, sea $N(x^n = a)$ el número de soluciones de la ecuación $x^n \equiv a \pmod p$. Si $n \mid p-1$, entonces $N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$.

Analizaremos por separado los siguientes casos:

(a) Si $a = 0$ y $x^n \equiv 0 \pmod p$ entonces $\sum_{\chi^n = \varepsilon} \chi(0) = 1$.

(b) Si $a \neq 0$ y $x^n \equiv a \pmod p$ es soluble entonces $\sum_{\chi^n = \varepsilon} \chi(a) = n$.

(c) Si $a \neq 0$ y $x^n \equiv a \pmod p$ no es soluble entonces $\sum_{\chi^n = \varepsilon} \chi(a) = 0$

Demostración.

(a) Claramente $N(x^n \equiv 0 \pmod p) = 1$, por lo tanto

$\sum_{\chi^n = \varepsilon} \chi(0) = \varepsilon(0) + \chi'(0) + \chi^2(0) + \cdots + \chi^{n-1}(0) = 1 + \chi(0) + \cdots + \chi(0) = 1$ y

$N(x^n = 0) = \sum_{\chi^n = \varepsilon} \chi(0) = 1$.

(b) Puesto que $x^n \equiv a \pmod p$ tiene $(n, p-1) = n$ soluciones y $n \mid p-1$ entonces $N(x^n = a) = n$.

Por otro lado, como $x^n = a$ es soluble, entonces existe $b \in \mathbb{F}_p^*$ tal que $b^n \equiv a \pmod p$. Sea $\chi \in \mathcal{X}$ tal que $\chi^n = \varepsilon$ entonces $\chi(a) = \chi^n(b) = \varepsilon(b) = 1$, luego

$$\sum_{\chi^n = \varepsilon} \chi(a) = \sum_{\chi^n = \varepsilon} 1 = n.$$

c) Si $a \neq 0$ y $x^n \equiv a \pmod p$ no soluble entonces $a \neq 1$ y por 2.1.3 existe $\rho \in \mathcal{X}$ tal que $\rho(a) \neq 1$ y $\rho^n = \varepsilon$.

Considero $T := \{\varphi \in \mathcal{X} \mid \varphi^n = \varepsilon\}$.

Si $\langle g \rangle = \mathbb{F}_p^*$, existe $\chi \in \mathcal{X}$ tal que $\chi(g) = e^{\frac{2\pi i}{n}}$, entonces $o(\chi) = n$, es decir, $\chi^n = \varepsilon$ y por tanto $T \supset \{\chi^0, \chi^1, \chi^2, \ldots, \chi^{n-1}\}$.

Ahora supongamos que $\varphi^n = \varepsilon$ $(\varphi \in T)$, donde $o(\varphi) = d$, $d \mid n$ y como $d \mid p-1$ tenemos que $\langle \varphi \rangle$ es subgrupo de $\langle \chi \rangle$, así que $\varphi \in \langle \chi \rangle$, por lo tanto $T = \langle \chi \rangle$. Ahora sea $H := \{\rho \chi^i \mid i = 0, 1, 2, \ldots, n-1\}$ entonces $H < \mathcal{X}$ (H es subgrupo de $\mathcal{X}$), $o(H) = n$ y por tanto $H = T$.

Por lo anterior $\rho(a) \sum_{\varphi^* \in T} \varphi^*(a) = \sum_{\varphi^* \in T} \rho\varphi^*(a) = \sum_{\varphi^* \in T} \varphi^*(a)$, entonces

$$\sum \varphi^*(a)[\rho(a) - 1] = 0 \quad \text{y} \quad \sum_{\varphi^* \in T} \varphi^*(a) = 0. \blacksquare$$

COROLARIO. Si $n=2$ y p-primo impar, entonces

$$N(x^2 \equiv a \pmod p) = 1 + \left(\frac{a}{p}\right).$$

Donde $\left(\frac{a}{p}\right)$ es el simbolo de Legendre y con el sobre-entendido de que $\left(\frac{0}{p}\right)=0$.

§2 SUMAS DE GAUSS

Sea $\zeta = e^{\frac{2\pi i}{p}}$, $a \in \mathbb{F}_p$. Si $b \in \bar{a}$ entonces $b = a+pq$ para alguna $q \in \mathbb{Z}$, por lo tanto $\underline{\zeta^b = \zeta^{a+pq}} = \zeta^a \zeta^{pq} = \underline{\zeta^a}$. Y la siguiente definición tiene sentido.

Definición. Sea χ carácter sobre $\mathbb{F}_p$ y $a \in \mathbb{F}_p^*$:

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at} \in \mathbb{C} \quad \text{es la suma de Gauss sobre } a \text{ donde } \zeta = e^{\frac{2\pi i}{p}}$$

Lema.

$$p^{-1}\sum_{a=0}^{p-1} \zeta^{a(x-y)} = \delta(x,y) := \begin{cases} 1 \text{ si } x \equiv y \pmod p \dots (1) \\ 0 \text{ si } x \not\equiv y \pmod p \dots (2) \end{cases}$$

Demostración

Caso (1). Si $x \equiv y \pmod{p}$ entonces $p \mid a(x-y)$, por tanto $a(x-y) = pk$ para algún $k \in \mathbb{Z}$. Entonces tenemos que $\zeta_p^{a(x-y)} = \zeta_p^{pk} = e^{2\pi i \frac{pk}{p}} = 1$, por consiguiente:

$$p^{-1} \sum_{a=0}^{p-1} \zeta_p^{a(x-y)} = p^{-1} \sum_{a=0}^{p-1} 1 = p^{-1} p = 1.$$

Caso (2).

Si $x \not\equiv y \pmod{p}$ entonces $p \nmid x-y$ implica que:

$$\zeta_p^{x-y} = e^{2\pi i \frac{(x-y)}{p}} \neq 1 \quad \text{y} \quad \zeta_p^{p(x-y)} = e^{2\pi i \frac{p(x-y)}{p}} = 1, \text{ por tanto}$$

$$p^{-1}\left(\sum_{a=0}^{p-1} \zeta_p^{a(x-y)}\right) = p^{-1}\left[\zeta_p^0 + \zeta_p^1 + \zeta_p^2 + \cdots + \zeta_p^{p-1}\right] = p^{-1} \cdot 0 = 0$$

Ya que $0 = \zeta_p^p - 1 = (\zeta_p - 1)(\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p^1 + \zeta_p^0)$ entonces $\zeta_p - 1 = 0$ o $\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p^0 = 0$, pero como $\zeta_p - 1 \neq 0$ tenemos que $\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p^1 + \zeta_p^0 = 0$. ∎

PROPOSICION 2.2.1.

I) Si $a \neq 0$ y $\chi \neq \varepsilon$ entonces $g_a(\chi) = \chi(a^{-1}) g_1(\chi)$.

II) Si $a \neq 0$ y $\chi = \varepsilon$ entonces $g_a(\varepsilon) = 0$.

III) Si $a = 0$ y $\chi \neq \varepsilon$ entonces $g_0(\chi) = 0$.

IV) Si $a=0$ y $\chi=\varepsilon$ entonces $g_0(\varepsilon)=p$.

Demostración.

I) Si $a\neq 0$ y $\chi\neq\varepsilon$ entonces $\chi(a)\neq 0$, fijándonos en: $\chi(a)g_a(\chi)=\chi(a)\sum_t \chi(t)f^{ta}=\sum_{at}\chi(at)f^{at}=g_1(\chi)$

tenemos que: $g_a(\chi)=\chi(a^{-1})g_1(\chi)$.

II) $g_a(\varepsilon)=\sum_t \varepsilon(t)f^{at}=\sum_t f^{at}=f^0+f^1+\cdots+f^{p-1}=0$.

III) Por 2.1.2 $g_0(\chi)=0$.

IV) $g_0(\varepsilon)=\sum_t \varepsilon(t)f^{0t}=\sum_{t\in\mathbb{F}_p}1=p$. ∎

Denotaremos $g_1(\chi)$ por $g(\chi)$.

Observación. $\overline{g_a(\chi)}=\sum_t \overline{\chi(t)}\,f^{\overline{at}}=\sum_t \overline{\chi(t)}\,f^{-at}$.

PROPOSICION 2.2.2. Si $\chi\neq\varepsilon$, entonces $|g(\chi)|=\sqrt{p}$.

Demostración.

Si $a=0$ y $\chi\neq\varepsilon$ entonces por 2.2.1.(III). $g_0(\chi)=0$, en este caso no hay igualdad.

Por tanto supongamos que $a\neq 0$ y $\chi\neq\varepsilon$, por 2.2.1.(II) tenemos que:

$g_a(x) = \chi(a^{-1})g(x)$ entonces $\overline{g_a(x)} = \overline{\chi(a^{-1})g(x)} = \overline{\chi(a^{-1})}\ \overline{g(x)}$

$= \overline{\chi(a)^{-1}}\ \overline{g(x)}$

$= \overline{\overline{\chi(a)}}\ \overline{g(x)}$, por 2.1.1,

$= \chi(a)\ \overline{g(x)}$, es decir,

$\overline{g_a(x)} = \chi(a)\overline{g(x)}$. Por consiguiente $g_a(x)\overline{g_a(x)} =$

$= \chi(a^{-1})g(x)\chi(a)\overline{g(x)} = \chi(a^{-1})\chi(a)\overline{g(x)}g(x) = g(x)\overline{g(x)} = |g(x)|^2$,

entonces $\sum_a g_a(x)\overline{g_a(x)} = \sum_a |g(x)|^2 = (p-1)|g(x)|^2$ .....(1).

Y por otro lado tenemos que:

$g_a(x)\overline{g_a(x)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$ (por obs. anterior)

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

$\sum_a g_a(x)\overline{g_a(x)} = \sum_a \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{a(x-y)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\, p\, \delta(x,y)$,

por Lema 2.1. Como $x \equiv y \pmod p$ entonces $\chi(x) = \chi(y)$, por tanto $\chi(x)\chi(y)^{-1} = 1$, es decir, $\chi(x)\overline{\chi(y)} = 1$ lo cual implica que: $\sum_a g_a(x)\overline{g_a(x)} = p\sum_x \sum_y \chi(x)\overline{\chi(y)} = p\sum_x \sum_y 1 = p(p-1)$ .....(2)

igualando (1) y (2), tenemos que: $|g(x)| = \sqrt{p}$. ∎

Observación (1). $\overline{g(\chi)} = \pm g(\overline{\chi})$, donde

$$\overline{\chi} : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$$
$$a \longmapsto \overline{\chi(a)}$$

Demostración.

$$\overline{g(\chi)} = \sum \overline{\chi(t)}\, \zeta^{-t} = \sum \overline{\chi(-1)}\,\overline{\chi(-t)}\,\zeta^{-t} = \overline{\chi(-1)} \sum \overline{\chi(-t)}\,\zeta^{-t} =$$
$$= \overline{\chi(-1)} \sum_t \overline{\chi}(-t)\,\zeta^{-t} = \overline{\chi(-1)} \sum_{-t=t^*} \overline{\chi}(t^*)\,\zeta^{t^*} = \overline{\chi(-1)}\, g(\overline{\chi}),$$

donde $-t = t^*$, por lo tanto $\overline{g(\chi)} = \overline{\chi(-1)}\, g(\overline{\chi}) =$
$$= \chi(-1)\, g(\overline{\chi}) \quad \ldots (1).$$

Por otro lado, $\overline{\chi(-1)} = \chi(-1)$ y $1 = \chi(1) = \chi[(-1)(-1)] = \chi(-1)^2$,

entonces $1 = \chi(-1)^2$, es decir, $\chi(-1) = \pm 1$, sustituyendo

en (1) obtenemos que $\boxed{\overline{g(\chi)} = \pm g(\overline{\chi})}$ ∎

Observacion (2). $g(\chi)\, g(\overline{\chi}) = \pm p = \chi(-1)\, p$.

Demostración.

$p = g(\chi)\,\overline{g(\chi)} = g(\chi)[\chi(-1)\, g(\overline{\chi})]$, entonces $p = \chi(-1)[g(\chi)\, g(\overline{\chi})]$.

Multiplicando por $\chi(-1)$ tenemos que $\boxed{g(\chi)\, g(\overline{\chi}) = \chi(-1)\, p}$ ∎

§3 SUMAS DE JACOBI

Consideremos la ecuación $X^2+Y^2=1$ sobre $\mathbb{F}_p$. Sea $N(x^2+y^2=1)$ el número de soluciones $(x,y)\in \mathbb{F}_p \times \mathbb{F}_p$ de $X^2+Y^2=1$. Más adelante probaremos que

$$N(x^2+y^2=1) = \begin{cases} p+1 & \text{si } p\equiv 3 \pmod 4 \\ p-1 & \text{si } p\equiv 1 \pmod 4 \end{cases} \quad \ldots\ldots\ldots (1)$$

Consideremos el resultado anterior como dado, notemos que en $\mathbb{F}_5$ las soluciones de la ecuación $X^2+Y^2=1$ son $(0,1),(1,0),(4,0)$ y $(0,4)$. Por otro lado aplicando la fórmula (1) obtenemos que para $p=5$, $N(x^2+y^2=1)=5-1=4$.

Ahora veamos que el número de soluciones de la ecuación $X^3+Y^3=1$ sobre $\mathbb{F}_p$ se puede apoximar.

Como $N(X^3+Y^3=1)=\sum_{a+b=1} N(X^3=a)\,N(Y^3=b)$. Analicemos 2 casos:

Caso (1)

Si $p\equiv 2 \pmod 3$ entonces $X^3\equiv a \pmod p$ es soluble $\forall a\in \mathbb{F}_p^*$, ya que $X^3\equiv a \pmod p$ tiene solución única para cada $a\in \mathbb{F}_p^*$, porque $a^{\frac{p-1}{d}}\equiv 1 \pmod p$ y $1=d=(p-1,3)$, y $X^3\equiv 0 \pmod p$ soluble,

Por tanto $N(x^3=a)=1 \quad \forall a \in \mathbb{F}_p$, entonces

$$N(x^3+y^3=1) = \sum_{a+b=1} N(x^3=a)\,N(y^3=b) = \sum_{a+b=1} 1 = p.$$

O bien como $\mathbb{F}_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ tenemos que

$(p-k)+(k+1) \equiv 1 \pmod{p}$, donde $1 \le k \le p-2$ por tanto

$\sum_{\substack{a+b=1 \\ a\neq 0,\, b\neq 0}} N(x^3=a)\,N(y^3=b) = p-2$, entonces tenemos que

$$\sum_{a+b=1} N(x^3=a)\,N(y^3=b) = p = N(x^3+y^3=1),$$ ya que

$0+1=a+b=1$ y $1+0=a+b=1$ son las otras dos soluciones que faltaban.

<u>Caso (2).</u> Si $p \equiv 1 \pmod 3$, por 2.1.3 tenemos que:

$\langle g \rangle = \mathbb{F}_p^*$, $\lambda(g^k) = e^{\frac{2\pi i k}{p-1}}$, donde $k=0,1,2,\ldots,p-2$,

con $\lambda^{p-1} = \varepsilon$, es decir, $\langle \lambda \rangle = S$.

Y por hipótesis $3 \mid p-1$, entonces $p-1 = 3m$ para algún $k \in \mathbb{Z}$.

Así $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ definida por

$$\chi(g^k) = e^{\frac{2\pi i k}{3}}, \quad k=0,1,2,\ldots,p-2,$$

Como ejemplo al caso ②, veamos las soluciones de la ecuación $X^3+Y^3=1$ sobre $\mathbb{F}_7$. Notemos primero que estas son, $\{(0,1),(1,0),(2,0),(0,2),(0,4),(4,0)\}$, es decir son 6 (ver tabla 2.2.1). Puesto que $\langle 3\rangle=\mathbb{F}_7^*$ y $\chi:\mathbb{F}_7^*\longrightarrow \mathbb{C}^*$ definido como $\chi(3^k)=e^{\frac{2\pi ik}{3}}$, $k=0,1,2,3,4,5$, es un generador del único subgrupo H de $\mathbb{C}$ de orden 3, entonces considerando que $\{(a,b)\in\mathbb{F}_7\times\mathbb{F}_7 \mid a+b=1\}=\{(0,1),(1,0),(2,6),(6,2),(3,5),(5,3),(4,4)\}$ (ver tabla 2.2.1.1) y además:

$e^{\frac{2\pi i}{3}}=-\frac{1}{2}+\frac{i\sqrt{3}}{2}$;

$-e^{\frac{\pi i}{3}}=-\frac{1}{2}-\frac{i\sqrt{3}}{2}$;

$\chi(2)=\chi(3^2)=e^{\frac{4\pi i}{3}}=-e^{\frac{\pi i}{3}}$;

$\chi^2(2)=e^{\frac{2\pi i}{3}}$;

$\chi(6)=\chi(3^3)=1$;

$\chi^2(6)=1$;

$\chi(5)=\chi(3^5)=e^{\frac{10\pi i}{3}}=-e^{\frac{\pi i}{3}}$

$\chi^2(5)=e^{\frac{2\pi i}{3}}$;

$\chi(3)=e^{\frac{2\pi i}{3}}$;

$\chi^2(3) = -e^{\frac{\pi i}{3}}$;

$\chi(4) = \chi(3^2) = e^{\frac{2\pi i}{3}} = e^{\frac{-2\pi i}{3}}$;

$\chi^2(4) = -e^{\frac{-\pi i}{3}}$.

Y suponiendo que $N(x^3+y^3=1) = \sum_{j=0}^{2}\sum_{i=0}^{2}\left(\sum_{a+b=1}\chi^i(a)\chi^j(b)\right)$ y

$N(x^3+y^3=1) = 6$, entonces $\sum_{j=0}^{2}\sum_{i=0}^{2}\sum_{a+b=1}\chi^i(a)\chi^j(b) =$

$= \sum_{a+b=1}[\varepsilon(a)\varepsilon(b) + \varepsilon(a)\chi(b) + \varepsilon(a)\chi^2(b) + \chi(a)\varepsilon(b) + \chi(a)\chi(b) + \chi(a)\chi^2(b) +$

$+ \chi^2(a)\varepsilon(b) + \chi^2(a)\chi(b) + \chi^2(a)\chi^2(b)] =$

$= (\varepsilon(0)\varepsilon(1) + \varepsilon(0)\chi(1) + \varepsilon(0)\chi^2(1) + \chi(0)\varepsilon(1) + \chi(0)\chi(1) + \chi(0)\chi^2(1) + \chi^2(0)\varepsilon(1) +$

$+ \chi^2(0)\chi(1) + \chi^2(0)\chi^2(1)) +$

$+ (\varepsilon(1)\varepsilon(0) + \varepsilon(1)\chi(0) + \varepsilon(1)\chi^2(0) + \chi(1)\varepsilon(0) + \chi(1)\chi(0) + \chi(1)\chi^2(0) + \chi^2(1)\varepsilon(0) + \chi^2(1)\chi(0) + \chi^2(1)\chi^2(0))$

$+ (\varepsilon(2)\varepsilon(6) + \varepsilon(2)\chi(6) + \varepsilon(2)\chi^2(6) + \chi(2)\varepsilon(6) + \chi(2)\chi(6) + \chi(2)\chi^2(6) + \chi^2(2)\varepsilon(6) + \chi^2(2)\chi(6) + \chi^2(2)\chi^2(6))$

$+ (\varepsilon(6)\varepsilon(2) + \varepsilon(6)\chi(2) + \varepsilon(6)\chi^2(2) + \chi(6)\varepsilon(2) + \chi(6)\chi(2) + \chi(6)\chi^2(2) + \chi^2(6)\varepsilon(2) + \chi^2(6)\chi(2) + \chi^2(6)\chi^2(2))$

$+ (\varepsilon(3)\varepsilon(5) + \varepsilon(3)\chi(5) + \varepsilon(3)\chi^2(5) + \chi(3)\varepsilon(5) + \chi(3)\chi(5) + \chi(3)\chi^2(5) + \chi^2(3)\varepsilon(5) + \chi^2(3)\chi(5) + \chi^2(3)\chi^2(5))$

$+ (\varepsilon(5)\varepsilon(3) + \varepsilon(5)\chi(3) + \varepsilon(5)\chi^2(3) + \chi(5)\varepsilon(3) + \chi(5)\chi(3) + \chi(5)\chi^2(3) + \chi^2(5)\varepsilon(3) + \chi^2(5)\chi(3) + \chi^2(5)\chi^2(3))$

$+ (\varepsilon(4)\varepsilon(4) + \varepsilon(4)\chi(4) + \varepsilon(4)\chi^2(4) + \chi(4)\varepsilon(4) + \chi(4)\chi(4) + \chi(4)\chi^2(4) + \chi^2(4)\varepsilon(4) + \chi^2(4)\chi(4) + \chi^2(4)\chi^2(4))$

$= (3) + (3) + 3(1 - e^{\frac{\pi i}{3}} + e^{\frac{2\pi i}{3}}) + 3(1 - e^{\frac{\pi i}{3}} + e^{\frac{2\pi i}{3}}) +$

$$+3\left(1+e^{\frac{2\pi i}{3}}-e^{\frac{\pi i}{3}}\right)+3\left(1+e^{\frac{2\pi i}{3}}-e^{\frac{\pi i}{3}}\right)+3\left(1+e^{\frac{2\pi i}{3}}-e^{\frac{\pi i}{3}}\right)=$$

$$=6+3\left(1-\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}-\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}\right)+3\left(1-\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}-\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}\right)+$$

$$+3\left(1-\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}-\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}\right)+3\left(1-\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}-\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}\right)+$$

$$+3\left(1-\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}-\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}\right)=6,$$ como queriamos.

Por tanto en $\mathbb{F}_7$ tenemos que se cumple que

$$N(x+y=1)=\sum_{j=0}^{2}\sum_{i=0}^{2}\left(\sum_{a+b=1}\chi^i(a)\chi^j(b)\right)=6.\blacksquare$$

Tabla 2.2.1.1.

$$\mathbb{F}_7\times\mathbb{F}_7=\begin{bmatrix}(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6)\\(1,0),(1,1),(1,2),(1,3),(1,4),(1,5),(1,6)\\(2,0),(2,1),(2,2),(2,3),(2,4),(2,5),(2,6)\\(3,0),(3,1),(3,2),(3,3),(3,4),(3,5),(3,6)\\(4,0),(4,1),(4,2),(4,3),(4,4),(4,5),(4,6)\\(5,0),(6,1),(5,2),(5,3),(5,4),(5,5),(5,6)\\(6,0),(6,1),(6,2),(6,3),(6,4),(6,5),(6,6)\end{bmatrix}$$

Definición. Sean χ y λ caracteres sobre $\mathbb{F}_p$ entonces
$J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b)$. Se le conoce como suma de Jacobi.

Teorema 1. Sean χ y λ caracteres no triviales. Entonces

I) $J(\varepsilon,\varepsilon)=p$.

II) $J(\varepsilon,\lambda)=0$.

III) $J(\chi,\chi^{-1})=-\chi(-1)$.

IV) Si $\chi\lambda\neq\varepsilon$, entonces $J(\chi,\lambda)=\dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Demostración.

I) $J(\varepsilon,\varepsilon)=\sum_{\substack{a+b=1\\ a,b\in\mathbb{F}_p}}1=p$ o por 2.1.2.II

II) $J(\varepsilon,\lambda)=\sum_{b\in\mathbb{F}_p}\lambda(b)=0$ por 2.1.2.I

III) Como $\chi(0)+\chi(1)+\chi(2)+\cdots+\chi(p-2)+\chi(p-1)=0$, es decir,
$\chi(0)+\chi(1)+\chi(2)+\cdots+\chi(p-2)+\chi(-1)=0$, entonces
$\chi(0)+\chi(1)+\chi(2)+\cdots+\chi(p-2)=-\chi(-1)$. Por tanto

$\sum_{\substack{c\neq-1\\ c\in\mathbb{F}_p}}\chi(c)=-\chi(-1)\ldots(1)$. Sea $c=\dfrac{a}{1-a}$ implica $a=\dfrac{c}{1+c}$.

Ahora $J(\chi,\chi^{-1})=\sum_{a+b=1}\chi(a)\chi^{-1}(b)=\sum_{\substack{a+b=1\\ b\neq0}}\chi(a)\chi(b^{-1})=\sum_{\substack{a+b=1\\ b\neq0}}\chi(ab^{-1})=$

$=\sum_{\substack{a+b=1\\ b\neq0}}\chi\left(\frac{a}{b}\right)=\sum_{\substack{a+b=1\\ a\neq1}}\chi\left(\frac{a}{1-a}\right)=\sum_{c\neq-1}\chi(c)=-\chi(-1)$, por (1).

Por tanto $J(\chi, \chi^{-1}) = -\chi(-1)$.

IV) $g(\chi)g(\lambda) = \left(\sum_x \chi(x)\zeta_p^x\right)\left(\sum_y \lambda(y)\zeta_p^y\right) =$

$= \sum_x \sum_y \chi(x)\lambda(y)\zeta_p^{x+y} = \sum_t \left[\sum_{x+y=t} \chi(x)\lambda(y)\right]\zeta_p^t$ .....(1)

Analizaremos

Caso (1)

Si $t=0$ tenemos que $\sum_{x+y=0} \chi(x)\lambda(y) = \sum_{y=-x} \chi(x)\lambda(-x) =$

$= \sum_x \chi(x)\lambda(-1)\lambda(x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$, por 2.1.2, asi que

$\sum_{x+y=0} \chi(x)\lambda(y) = 0$, sustituyendo en (1) tenemos que: $g(\chi)g(\lambda) = 0$.

Caso (2). Si $t \neq 0$, definimos $tx' = x$ y $ty' = y$ por lo que $x' + y' = 1$, ya que $x+y=t$. Por lo tanto:

$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \sum_{x'+y'=1} \chi\lambda(t)\chi(x')\lambda(y') =$

$= \chi\lambda(t)\sum_{x'+y'=1} \chi(x')\lambda(y') = \chi\lambda(t)\, J(\chi,\lambda)$, por definición.

Luego $\sum_{x+y=t} \chi(x)\lambda(y) = \chi\lambda(t)\, J(\chi,\lambda)$ ..... (2).

Sustituyendo (2) en (1), obtenemos: $t \neq 0$, $t \in \mathbb{F}_p^*$ y

$g(\chi)g(\lambda) = \sum_t \left(\chi\lambda(t)\, J(\chi,\lambda)\right)\zeta_p^t = J(\chi,\lambda)\sum_t \chi\lambda(t)\zeta_p^t =$

$= J(\chi,\lambda)\ g(\chi\lambda)$, por definición. Por tanto

$$g(\chi)\,g(\lambda) = J(\chi,\lambda)\,g(\chi\lambda).$$

Como $\chi\lambda \neq \varepsilon$; $a=1$ tenemos que $g(\chi\lambda)\neq 0$, por 2.2.1, entonces

$$\boxed{J(\chi,\lambda) = \frac{g(\chi)\,g(\lambda)}{g(\chi\lambda)}} \quad \ldots\ldots (3)$$ ∎

COROLARIO.
Si χ,λ y $\chi\lambda$ son no triviales, entonces $|J(\chi,\lambda)| = \sqrt{p}$.
Demostración. Tomando el valor absoluto de (3), el resultado se sigue de 2.2.2.

Regresemos al análisis de $N(x^2+y^2=1)$ y $N(y^3+x^3=1)$. Teníamos que: $N(x^2\equiv a \pmod p) = 1+\left(\frac{a}{p}\right)$, por corolario de 2.1.5 ∎

$$N(x^2+y^2=1) = \sum_{a+b=1} N(x^2=a)\,N(y^2=b) = \sum_{a+b=1}\left[1+\left(\frac{a}{p}\right)\right]\left[1+\left(\frac{b}{p}\right)\right] =$$

$$= p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = p + \sum_{\substack{a+b=1 \\ a,b\in \mathbb{F}_p}} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ , porque}$$

hay tantos residuos cuadráticos como no cuadráticos. Por tanto

$$N(x^2+y^2=1) = p + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Como el símbolo de Legendre es un carácter cuadrático módulo p,

Sea $\left(\frac{a}{p}\right)=\chi(a)$ un carácter cuadrático módulo p; $\chi^2=\varepsilon$ implica que $\chi=\chi^{-1}$ ..... (*). Por lo tanto

$$N(x^2+y^2)=p+\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=p+\sum_{a+b=1}\chi(a)\chi(b)\text{, por notación}$$

$$=p+J(\chi,\chi)\quad\text{(por definición)}$$
$$=p+J(\chi,\chi^{-1})\quad\text{(por (*))}$$
$$=p-\chi(-1)\quad\text{(por teorema 1)}$$
$$=p-\left(\frac{-1}{p}\right)\quad\text{(por notación)}$$
$$=p-(-1)^{\frac{p-1}{2}}\text{, por tanto}$$

$N(x^2+y^2=1)=p-(-1)^{\frac{p-1}{2}}$, como se quería. Luego

$$N(x^2+y^2=1)=\begin{cases}p+1 & \text{si } p\equiv 3 \pmod 4,\ y\\ p-1 & \text{si } p\equiv 1 \pmod 4.\end{cases}$$

En el caso $N(x^3+y^3=1)$ teníamos que χ era un carácter de orden 3, así que: $N(x^3+y^3=1)=\sum_{i=0}^{2}\sum_{j=0}^{2}\left[\sum_{a+b=1}\chi^i(a)\chi^j(b)\right]=$

$$=\sum_{a+b=1}\Big[\Big(\varepsilon(a)\varepsilon(b)+\chi(a)\varepsilon(b)+\chi^2(a)\varepsilon(b)\Big)+\Big(\varepsilon(a)\chi(b)+\chi(a)\chi(b)+\chi^2(a)\chi(b)\Big)+$$
$$+\Big(\varepsilon(a)\chi^2(b)+\chi(a)\chi^2(b)+\chi(a)\chi^2(b)\Big)\Big]=p+J(\chi,\varepsilon)+J(\chi^2,\varepsilon)+$$

$+J(\varepsilon,\chi)+J(\chi,\chi)+J(\chi^2,\chi)+J(\varepsilon,\chi^2)+J(\chi,\chi^2)+J(\chi^2,\chi^2)=$

$=p+J(\chi,\chi)+J(\chi^2,\chi)+J(\chi,\chi^2)+J(\chi^2,\chi^2)$, por teorema1,

asigue: $N(x^3+y^3=1)=p+J(\chi,\chi^2)+J(\chi^2,\chi)+J(\chi,\chi)+J(\chi^2,\chi^2)$.

Como $\chi^3=\varepsilon$, por ser carácter cúbico, entonces

$\chi^2=\chi^{-1}=\overline{\chi}$ y con $-1=(-1)^3$ obtenemos $1=\chi^2(-1)=$

$=\chi^{-1}(-1)=\chi(-1)\chi^{-2}(-1)$ así $\chi^{-2}(-1)\chi(-1)=1$ y

$\underline{\chi(-1)=\chi^2(-1)=1}$. Por tanto

$$N(x^3+y^3=1)=p+2J(\chi,\chi^{-1})+J(\chi,\chi)+J(\overline{\chi},\overline{\chi})=$$
$$=p-2\chi(-1)+2\,\mathrm{Re}\,J(\chi,\chi)\text{ , por teorema1,}$$
$$N(x^3+y^3=1)=p-2+2\,\mathrm{Re}\,J(\chi,\chi)$$

Observaciones.

(1) $|N(x^3+y^3=1)-p+2|=|2\,\mathrm{Re}\,J(\chi,\chi)|\le 2|J(\chi,\chi)|=2\sqrt{p}$.

(2) Si N_p es el número de soluciones de $x^3+y^3=1$ sobre $\mathbb{F}_p$, entonces N_p es aproximadamente a $(p-2)$ con "error" de $2\sqrt{p}$.

Continuando tenemos del corolario del teorema1 la siguiente consecuencia.

PROPOSICION 2.3.1. Si $p\equiv 1 \pmod 3$ entonces existen enteros a y b tales que $p=a^2-ab+b^2$.

Demostración.

Como $p \equiv 1 \pmod 3$ entonces sea χ carácter de orden 3. Tenemos que las raíces de la ecuación $X^3 = 1$ son $1, w$ y w^2 donde $w = e^{\frac{3\pi i}{3}} = \left(\frac{-1+i\sqrt{3}}{2}\right)$, $w^2 + w + 1 = 0$, $w^2 = \overline{w}$ y $w^3 = 1$.

Para $a \in \mathbb{F}_p^*$, $\chi(a)$ es una raíz cúbica de la unidad, así los valores de χ están en $\{1, w, w^2\}$, de lo cual obtenemos que:

$$J(\chi, \chi) = \sum_{s+t=1} \chi(s)\chi(t) \in \mathbb{Z}[w].$$

Por tanto $J(\chi, \chi) = a + bw$ y $p = |J(\chi, \chi)|^2 = (a+bw)\overline{(a+bw)} = (a+bw)(a+b\overline{w}) = a^2 - ab + b^2$, es decir,

$$p = a^2 - ab + b^2. \blacksquare$$

Observación 1.

Notemos que $p = a^2 - ab + b^2 = (b-a)^2 - (b-a)b + b^2 = (a-b)^2 - (a-b)a + a^2$, por lo tanto la representación de p no es única.

Observación 2.,

$p = a^2 - ab + b^2$ entonces $4p = (2a-b)^2 + 3b^2 = (2b-a)^2 + 3a^2 = (a+b)^2 + 3(a-b)^2$.

Observación 3.

Si $p \equiv 1 \pmod 3$, entonces $p = a^2 - ab + b^2$ y 3 divide solamente a uno de los siguientes números: a, b y $a-b$.

Es decir $3|a$ ó $3|b$ ó $3|a-b$.

Observación 4.

Supongamos que $3|a-b$, es decir $a-b=3K$ para algún $k\in\mathbb{Z}$, entonces $3(a-b)^2 = 27k^2$ .....(1).

Como $4p = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2$

$= (2b-a)^2 + 3a^2$

$= (a+b)^2 + 3(a-b)^2$

$= (a+b)^2 + 27k^2$, por (1).

Por tanto $A^2 := (a+b)^2$ y $B^2 = k^2$, y

$4p = A^2 + 27B^2$.

De estas observaciones tenemos.

PROPOSICION 2.3.2

Si $p\equiv 1 \pmod 3$ entonces existen enteros A y B tales que $4p = A^2 + 27B^2$.

En la representación de $4p$, A y B estan determinados en forma única **salvo** el signo.

El siguiente resultado relaciona las sumas de Gauss con las sumas de Jacobi.

PROPOSICION 2.3.3.

Supongamos que $p\equiv 1 \pmod n$ y χ es carácter de orden n.

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

Demostración. Sea $x =: z$, por IV del teorema 1 tenemos que:

$$g(x)^2 = J(x,x)\, g(x^2) \quad \ldots\ldots (1).$$

Otra vez sea $x^2 =: z$ y por IV del teorema 1 tenemos

$$g(x)\, g(x^2) = g(x^3)\, J(x, x^2) \quad \ldots\ldots (2)$$

multiplicando (1) por $g(x)$ llegamos a

$$\begin{aligned} g(x)^3 = g(x)\, g(x)^2 &= g(x)\, J(x,x)\, g(x^2) \\ &= J(x,x)\, g(x)\, g(x^2) \\ &= J(x,x)\, J(x,x^2)\, g(x^3), \end{aligned}$$

por (2), por tanto

$$g(x)^3 = J(x,x)\, J(x,x^2)\, g(x^3) \quad \ldots\ldots (3),$$

multiplicando (3) por $g(x)$ obtenemos

$$g(x)^4 = J(x,x)\, J(x,x^2)\, g(x^3)\, g(x),$$

como $g(x)\, g(x^3) = J(x,x^3)\, g(x^4)$, entonces

$$g(x)^4 = J(x,x)\, J(x,x^2)\, J(x,x^3)\, g(x^4) \quad \ldots\ldots (4),$$

continuando el proceso, tenemos

$$g(x)^{n-1} = J(x,x)\, J(x,x^2)\, J(x,x^3) \ldots J(x,x^{n-2})\, g(x^{n-1}) \ldots (5).$$

Ahora por hipótesis tenemos que $\mathcal{E} = \mathcal{X}^n$, entonces $x^{n-1} = x^{-1} = \overline{x}$.

Así que $g(\chi)g(\chi^{n-1}) = g(\chi)\,g(\overline{\chi}) = \chi(-1)p$, por observación 2 de 2.2.2. Multiplicando (5) por $g(\chi)$ tenemos que

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

COROLARIO.
Si χ es carácter cúbico, entonces $g(\chi)^3 = p\,J(\chi,\chi)$.

Usando el corolario anterior, analizaremos $J(\chi,\chi)$ para tener una mejor "visualización" de $N(x^3+y^3=1)$. Recordemos que $J(\chi,\chi) = (a+b\omega)\in\mathbb{Z}[\omega]$, a,b en $\mathbb{Z}$ y $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$.

PROPOSICION 2.3.4
Supongamos que $p\equiv 1 \pmod 3$ y χ carácter cúbico.
Entonces
I) $b\equiv 0 \pmod 3$
II) $a\equiv -1 \pmod 3$
Demostración.
Como $g(\chi) = \sum_t \chi(t)\zeta^t$ tenemos

$$g(\chi)^3 = \left(\sum_t \chi(t)\zeta^t\right)^3 = \sum \chi(t)^3\zeta^{3t} \pmod 3,$$ entonces:

Como $\chi(0)=0$ y $\chi(t)^3=1$ para $t\neq 0$ tenemos

$$\sum_t \chi(t)^3 \zeta^{3t} = \sum_{t\neq 0} \zeta^{3t} = \zeta^{3\cdot 1}+\zeta^{3\cdot 2}+\cdots+\zeta^{3(p-1)} \equiv$$

$$\equiv \zeta^1+\zeta^2+\zeta^3+\cdots+\zeta^{p-1} \equiv -1 \equiv 2 \pmod 3, \text{ por tanto}$$

$$g(\chi)^3 \equiv -1 \equiv 2 \pmod 3 \quad \ldots\ldots (1).$$

Por corolario tenemos $g(\chi)^3 = p\,J(\chi,\chi)$, y por hipótesis $p\equiv 1 \pmod 3$, entonces

$$g(\chi)^3 \equiv J(\chi,\chi) \pmod 3$$

y $J(\chi,\chi)=a+b\omega$, $\quad g(\chi)^3 \equiv (a+b\omega) \pmod 3 \ldots\ldots (2).$

de (1) y (2)

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

Ahora reemplazando $\overline{\chi}$ por χ. Y $\overline{g(\chi)} = \chi(-1)g(\overline{\chi}) = g(\overline{\chi})$, ya que χ es carácter cúbico, es decir, $\chi(-1)=1$.

Encontramos que

$$g(\overline{\chi})^3 = p\,J(\overline{\chi},\overline{\chi}) \equiv (a+b\overline{\omega}) \pmod 3, \text{ ya que } p\equiv 1 \pmod 3$$

$$\equiv (-1) \pmod 3, \text{ por } (3), \ldots\ldots (4)$$

de (3) y (4) obtenemos

$b(\omega-\overline{\omega}) \equiv 0 \pmod 3$ o $b\sqrt{-3} \equiv 0 \pmod 3$ entonces

$3 \mid b\sqrt{-3} \Rightarrow \exists\, \gamma \in \mathbb{Z}[\omega]$ tal que $b\sqrt{-3} = 3\gamma$. Esto implica que

TEOREMA 2. Supongamos $p \equiv 1 \pmod 3$, entonces existen enteros A y B tales que $4p = A^2 + 27B^2$. Si $A \equiv 1 \pmod 3$, A está determinado en forma única y $N(x^3+y^3=1) = p - 2 + A$.

Demostración. Basta ver que $N(x^3+y^3=1) = p-2+A$, si $A \equiv 1(3)$. Sabemos que $N(x^3+y^3=1) = p-2+2\operatorname{Re} J(\chi,\chi)$, con χ carácter de orden 3 y $J(\chi,\chi) = (a+b\omega)$. Entonces $\operatorname{Re} J(\chi,\chi) =$
$= \operatorname{Re}\left[a+b\left(\frac{-1+i\sqrt{3}}{2}\right)\right] = \operatorname{Re}\left[\left(\frac{2a-b}{2}\right)+\left(\frac{b\,i\sqrt{3}}{2}\right)\right] = \frac{2a-b}{2}$, implica

$2\operatorname{Re} J(\chi,\chi) = 2a-b$, sea $2a-b := A$ y por corolario anterior tenemos $2\operatorname{Re} J(\chi,\chi) = A \equiv 1 \pmod 3$. Entonces

$N(x^3+y^3=1) = p-2+A$. ∎

Veamos por último dos ejemplos al teorema (2).

Ejemplo 1. Si $p = 61 \equiv 1 \pmod 3$, entonces $4p = (4)(61) = (\pm 1)^2 + 27(3)^2$ y $A = 1 \equiv 1 \pmod 3$ entonces el número de soluciones de la ecuación $x^3+y^3=1$ en $\mathbb{F}_{61}$ es:

$$61 - 2 + 1 = 60 = N(x^3+y^3=1).$$

Ejemplo 2. Sea $p = 67 \equiv 1 \pmod 3$, así $(4)(67) = (\pm 5)^2 + 27(3)^2$. Como $5 \not\equiv 1 \pmod 3$ entonces $A := -5 \equiv 1 \pmod 3$, por tanto el número de soluciones de $x^3+y^3=1$ en $\mathbb{F}_{67}$ es: $67 - 2 - 5 = 60 = N(x^3+y^3=1)$.

Por tanto tenemos que el $N(x^3+y^3=1)$ tanto en $\mathbb{F}_{61}$ como en $\mathbb{F}_{67}$

son 60.

Aunque $x^3+y^3=1$ tienen el mismo número de soluciones en $\mathbb{F}_{61}$ y $\mathbb{F}_{67}$, éstas no se pueden comparar, puesto que la aritmetica de $\mathbb{F}_{61}$ es completamente diferente a la aritmética de $\mathbb{F}_{67}$.■

CAPITULO TRES/RECIPROCIDAD CUBICA

§1

Empezamos con algunos resultados que involucren al anillo $\mathbb{Z}[w]$.

Sea π primo en $\mathbb{Z}[w]$, entonces el grupo multiplicativo $\left(\mathbb{Z}[w]/\pi\mathbb{Z}[w]\right)^*$ tiene orden $N\pi-1$, por 1.X.1.

Con ello podemos decir que tenemos un resultado análogo al pequeño teorema de Fermat, dado por:

PROPOSICION 3.1.1. Sea π primo en $\mathbb{Z}[w]$. Si $\pi \nmid \alpha$, entonces $\alpha^{N\pi-1} \equiv 1 \pmod{\pi}$.

Demostración.

Supongamos que $N\pi \neq 3$, entonces las clases residuales de $1, w$ y w^2 son diferentes en $\mathbb{Z}[w]/\pi\mathbb{Z}[w]$, ya que si:

1) $w \equiv 1 \pmod{\pi}$, entonces $\pi \mid 1-w$. Como $1-w$ es primo, π y $1-w$ son asociados, es decir, $1-w = \pi\gamma$, γ unidad, entonces $3 = N(1-w) = N(\gamma\pi) = N\pi$, por tanto $N\pi = 3$ ↯.

2) $w \equiv w^2 \pmod{\pi}$, $\pi \mid w(1-w)$ y π primo entonces $\pi \mid w$ o'

$\pi \mid (1-w)$ lo cual es imposible, ya que w es unidad y

$\pi \nmid 1-w$ por (1), por tanto $w \not\equiv w^2 \pmod{\pi}$.

3) Si $w^2 \equiv 1 \pmod{\pi}$, entonces $\pi \mid -w^2+1 = (1+w)(1-w)$, asi que $\pi \mid 1+w$ ó $\pi \mid 1-w$ implica $\pi \mid 1+w$ por (1).

Si $\pi \mid 1+w$, $\pi \mid -w^2$ pues $1+w+w^2=0$, por tanto π es unidad ∇.

Es decir $1, w, w^2$ son diferentes en $\left(\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right)^*$, entonces $\{1, w, w^2\}$ es un grupo cíclico de orden 3 y además

$$3 \Big| \left|\left(\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right)^*\right| = N\pi - 1 \quad \ldots\ldots\ldots\ldots (*).$$

Asi cualquier α en $\left(\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}\right)^*$ elevado a la $3k$, para alguna $k \in \mathbb{N}$, es congruente con 1 módulo π, es decir,

$\alpha^{N\pi-1} = \alpha^{3k} \equiv 1 \pmod{\pi}$, para algún $k \in \mathbb{N}$.

Por tanto $\alpha^{N\pi-1} \equiv 1 \pmod{\pi}$. ∎

Notemos que si π es primo en $\mathbb{Z}[w]$ (excepto $1-w$), entonces:

1) $\pi = q$ racional y $N\pi = q^2 \equiv 1 \pmod{\pi}$.

2) π complejo, $N\pi = p \equiv 1 \pmod 3$.

Una prueba más elegante de la proposición anterior es la siguiente:

Sea $\alpha \in \left(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]\right)^*$, entonces $(\alpha)^{N\pi-1} = 1 + \pi\mathbb{Z}[\omega]$

Así que $\alpha^{N\pi-1} - 1 \in \pi\mathbb{Z}[\omega]$, por lo tanto

$$\alpha^{N\pi-1} \equiv 1 \pmod{\pi}$$

Observaciones.

1) Sea $A^* = \alpha^{\frac{N\pi-1}{3}}$, entonces

$\alpha^{N\pi-1} - 1 = (A^*-1)(A^*-\omega)(A^*-\omega^2)$. En efecto pues

$(A^*-1)(A^*-\omega)(A^*-\omega^2) = [A^*(A^*-\omega)-(A^*-\omega)](A^*-\omega^2) = [A^*(A^*-\omega)-(A^*-\omega)]A^* -$

$[A^*(A^*-\omega)-(A^*-\omega)]\omega^2 = A^{3*} - \omega A^{2*} - A^{2*} + A^{*}\omega - A^{*2}\omega^2 + A^*\omega^3 +$

$+ A^*\omega^2 - \omega^3 = A^{*3} - A^{2*}[1+\omega+\omega^2] + A^*[\omega^2+\omega+1] - 1 = A^{3*} - 1$, ya que $\omega^2+\omega+1 = 0$.

2) Si π primo y $N\pi \neq 3$, entonces π divide solamente <u>a uno</u> de los factores anteriores, es decir a: $(\alpha^{\frac{N\pi-1}{3}} - 1)$, $(\alpha^{\frac{N\pi-1}{3}} - \omega)$, $(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$.

Prueba: Por 3.1.1 $\pi \mid \alpha^{N\pi-1} - 1$ y por observación(1)

$\pi \mid (\alpha^{\frac{N\pi-1}{3}} - 1)(\alpha^{\frac{N\pi-1}{3}} - \omega)(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$. Como π es primo,

$\pi \mid \alpha^{\frac{N\pi-1}{3}}$ ó $\pi \mid \alpha^{\frac{N\pi-1}{3}} - \omega$ ó $\pi \mid \alpha^{\frac{N\pi-1}{3}} - \omega^2$.

Así π divide al menos a uno de ellos, veamos que solamente divide a uno de ellos.

Veámoslo. Supongamos que π divide a cualesquiera 2 de los factores, es decir, a:

a) $(\alpha^{\frac{N\pi-1}{3}} - 1)$ & $(\alpha^{\frac{N\pi-1}{3}} - \omega)$ ó

b) $(\alpha^{\frac{N\pi-1}{3}} - 1)$ & $(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$ ó

c) $(\alpha^{\frac{N\pi-1}{3}} - \omega)$ & $(\alpha^{\frac{N\pi-1}{3}} - \omega^2)$.

Demostración.

a) Si $\pi \mid \alpha^{\frac{N\pi-1}{3}} - 1$ & $\pi \mid \alpha^{\frac{N\pi-1}{3}} - \omega$ implica que

$\pi \mid (\alpha^{\frac{N\pi-1}{3}} - 1) - (\alpha^{\frac{N\pi-1}{3}} - \omega) = -1 + \omega = -(1-\omega)$, $\pi \mid -(1-\omega)$ ↯, porque no son asociados.

b) Si $\pi \mid \alpha^{\frac{N\pi-1}{3}} - 1$ & $\pi \mid \alpha^{\frac{N\pi-1}{3}} - \omega^2$ implica que

$\pi \mid (\alpha^{\frac{N\pi-1}{3}} - 1) - (\alpha^{\frac{N\pi-1}{3}} - \omega^2) = -1 + \omega^2$ entonces $\omega^2 \equiv 1 \pmod{\pi}$ ↯ ya que $\omega^2 \not\equiv 1 \pmod{\pi}$.

c) Si $\pi \mid \alpha^{\frac{N\pi-1}{3}} - w$ y $\pi \mid \alpha^{\frac{N\pi-1}{3}} - w^2$, π divide a su diferencia,

por tanto $\pi \mid -w + w^2$ implica $w^2 \equiv w \pmod{\pi}$ ↯ ya que

son diferentes w y w^2 en $\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]}$.

Por lo anterior π primo en $\mathbb{Z}[w]$ y $N\pi \neq 3$, entonces π

divide a uno y sólo a uno de los siguientes factores:

$$\left(\alpha^{\frac{N\pi-1}{3}} - 1\right), \left(\alpha^{\frac{N\pi-1}{3}} - w\right) \text{ y } \left(\alpha^{\frac{N\pi-1}{3}} - w^2\right).$$

PROPOSICION 3.1.2. Supongamos que π primo tal que $N\pi \neq 3$ y $\pi \nmid \alpha$. Entonces existe un único entero $m \in \{0,1,2\}$ tal que $\alpha^{\frac{N\pi-1}{3}} \equiv w^m \pmod{\pi}$.

Demostración:

Como π primo y $\pi \nmid \alpha$ entonces $\alpha^{N\pi-1} \equiv 1 \pmod{\pi}$ por 3.1.1,

implica que $\pi \mid \alpha^{N\pi-1} - 1 \Rightarrow \pi \mid \alpha^{\frac{N\pi-1}{3}} - 1$ ó

$\pi \mid \alpha^{\frac{N\pi-1}{3}} - w$ ó $\pi \mid \alpha^{\frac{N\pi-1}{3}} - w^2$ por obs. (1) y obs. (2).

Entonces $\alpha^{\frac{N\pi-1}{3}} \equiv w^m \pmod{\pi}$ donde m es único y

$m \in \{0,1,2\}$. ∎

Con base en este resultado hacemos la siguiente definición.

Definición.

$$\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & \text{si } \pi \mid \alpha \\ \bar{\omega}^m & \text{si } \pi \nmid \alpha. \end{cases}$$

Donde $\bar{\omega}^m$ denota la clase de ω^m módulo π.

Observaciones:

1) $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$ se leera como: el carácter residual cúbico de α módulo π. Esto será un camino viable para caracteres cúbicos.

2) Si $\pi \nmid \alpha$ entonces por 3.1.2 $\left(\frac{\alpha}{\pi}\right)_3 \equiv \omega^m \pmod{\pi}$ sólo para un valor de $m = 0, 1, 2$.

3) Así como el símbolo de Legendre es importante en reciprocidad cuadrática, tenemos que el carácter residual cúbico es importante en reciprocidad cúbica.

PROPOSICION 3.1.3.

I) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ sii $X^3 \equiv \alpha \pmod{\pi}$ es soluble, es decir, α es residuo cúbico.

II) $\alpha^{\frac{N\pi - 1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$.

III) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

III) Si $\alpha \equiv \beta \pmod{\pi}$, entonces $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Demostración

I) $\Leftarrow$] Sea $\langle \gamma \rangle := \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*$ generador, además sea $\gamma^a = \alpha$ y $x = \gamma^y$ (por ser soluble).

Como $x^3 \equiv \alpha \pmod{\pi}$ soluble entonces se trasforma en:

$\gamma^{3y} \equiv \gamma^a \pmod{\pi}$ soluble $\Leftrightarrow \gamma^{3y-a} \equiv 1 \pmod{\pi} \Leftrightarrow$

$N\pi - 1 \mid 3y - a \Leftrightarrow 3y \equiv a \pmod{N\pi - 1}$ soluble $\Leftrightarrow (N\pi - 1, 3) \mid a$.

Como $(N\pi - 1, 3) = 3$ entonces $3 \mid a \Leftrightarrow a = 3k$, para algún $k \in \mathbb{Z}$. Luego $\alpha \equiv \gamma^a \pmod{\pi} \Rightarrow \alpha^{\frac{N\pi-1}{3}} \equiv \gamma^{a\left(\frac{N\pi-1}{3}\right)} \pmod{\pi}$

$\Rightarrow \alpha^{\frac{N\pi-1}{3}} \equiv \left(\gamma^{N\pi-1}\right)^k \pmod{\pi} \Rightarrow \alpha^{(N\pi-1)/3} \equiv 1 \pmod{\pi}$, por ser γ generador y $o(\gamma) = N\pi - 1$, entonces $\left(\frac{\alpha}{\pi}\right)_3 = 1$.

$\Rightarrow$] Si $\left(\frac{\alpha}{\pi}\right)_3 = 1$, por demostrar que: $x^3 \equiv \alpha \pmod{\pi}$ soluble.

Por lo anterior basta ver que $3 \mid a$. Ya que "casi" es sii en la demostración anterior.

Como $\gamma^a = \alpha \Rightarrow \gamma^{a\left(\frac{N\pi-1}{3}\right)} \equiv \alpha^{\frac{N\pi-1}{3}} \pmod{\pi}$, y por hipótesis $\left(\frac{\alpha}{\pi}\right)_3 = 1$, es decir, $\alpha^{\frac{N\pi-1}{3}} \equiv 1 \pmod{\pi}$, entonces

$\gamma^{a\left(\frac{N\pi-1}{3}\right)} \equiv 1 \pmod{\pi}$ ..... (1)

y $\left|\left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^*\right| = N\pi - 1$ entonces de (1) tenemos que

$N\pi - 1 \Big| a\left(\frac{N\pi-1}{3}\right) \Rightarrow a\left(\frac{N\pi-1}{3}\right) = (N\pi-1)\, q$, para algún $q \in \mathbb{Z}$, $\Rightarrow$

$\frac{a}{3} = q \Rightarrow a = 3q \Rightarrow 3 \mid a$.

Así como $\gamma^a \equiv \alpha \pmod{\pi}$ y $a = 3k \Rightarrow (\gamma^k)^3 \equiv \alpha \pmod{\pi}$,

definimos $\underline{X = \gamma^k}$ como solución de $X^3 \equiv \alpha \pmod{\pi}$.

Por tanto $X^3 \equiv \alpha \pmod{\pi}$ es soluble.

II) Se sigue de la definición y por 3.3.2.

III) $\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\overline{\alpha\beta})^{\frac{N\pi-1}{3}} \equiv [\alpha^{\frac{N\pi-1}{3}}][\beta^{\frac{N\pi-1}{3}}] \pmod{\pi}$, por tanto

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

IV) Si $\alpha \equiv \beta \pmod{\pi} \Rightarrow \alpha^{\frac{N\pi-1}{3}} \equiv \beta^{\frac{N\pi-1}{3}} \pmod{\pi}$, es decir,

$\left(\frac{\alpha}{\pi}\right)_3 \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$ ..... (2)

Recordando que $\left(\frac{\alpha}{\pi}\right)_3 = 1$ ó ω ó $\omega^2 = \left(\frac{\beta}{\pi}\right)_3$ y $1, \omega$ y ω^2 son

diferentes en $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. Entonces de (2) obtenemos que $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$. ∎

PROPOSICION 3.1.4

I) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.

II) $\overline{\chi_\pi(\alpha)} = \chi_{\bar{\pi}}(\bar{\alpha})$

Demostración.

I) Como $\chi_\pi(\alpha) = 1$ ó ω ó ω^2 y $1^2 = 1$, $\omega^2 = \bar{\omega}$ y $(\omega^2)^2 = \bar{\omega}^2 = \bar{\bar{\omega}} = \omega$, $(\bar{\omega}^2 = \bar{\bar{\omega}} = \omega)$. Entonces $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2$ y

$\chi_\pi(\alpha^2) = \chi_\pi(\alpha)\chi_\pi(\alpha)$, por 3.1.3.III. así $\chi_\pi(\alpha^2) = 1$ ó ω ó ω^2.

Por tanto $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha^2) = \chi_\pi(\alpha^2)$.

II) Sabemos que: $\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}$, entonces

$\bar{\alpha}^{\left(\frac{N\pi-1}{3}\right)} \equiv \overline{\chi_\pi(\alpha)} \pmod{\bar{\pi}}$ ..... (1).

Por otro lado $\bar{\alpha}^{\left(\frac{N\bar{\pi}-1}{3}\right)} \equiv \chi_{\bar{\pi}}(\bar{\alpha}) \pmod{\bar{\pi}}$ y como $N\pi = N\bar{\pi}$,

entonces $\bar{\alpha}^{\left(\frac{N\pi-1}{3}\right)} \equiv \chi_{\bar{\pi}}(\bar{\alpha}) \pmod{\bar{\pi}}$ .....(2).

De (1) y (2): $\chi_{\bar{\pi}}(\bar{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\bar{\pi}}$ .....(3), y por (I)

$\chi_{\bar{\pi}}(\bar{\alpha}) = \overline{\chi_\pi(\alpha)}$.

COROLARIO.

I) $\chi_q(\bar{\alpha}) = \chi_q(\alpha^2)$.

II) $\chi_q(n) = 1$, si $(n,q)=1$ (n entero racional primo con q).

Demostración: I) $\chi_q(\bar{\alpha}) = \chi_{\bar{q}}(\bar{\alpha})$, ya que $q = \bar{q}$,

$= \overline{\chi_q(\alpha)}$, por 3.1.Y.III,

$= \chi_q(\alpha^2)$, por 3.1.Y.I.

II) $\chi_q(n) = \chi_q(\bar{n})$, $n = \bar{n}$,

$= \chi_q(n^2)$, parte la parte (I),

$= \chi_q(n)^2$, por 3.1.Y.I.

Por tanto $\chi_q(n)[1-\chi_q(n)] = 0$ y como $(q,n)=1$, es decir $q \nmid n$, entonces $\chi_q(n) \neq 0$ por definición de carácter residual cúbico. Así, $1-\chi_q(n)=0$ implica $\chi_q(n)=1$. ∎

Nota: El corolario establece que n es residuo cúbico módulo q.

Si $q_1 \neq q_2$ primos y $q_1 \equiv q_2 \equiv 2 \pmod 3$, entonces $\chi_{q_1}(q_2) = \chi_{q_2}(q_1) = 1$, inmediato de corolario. Este re

sultado es un caso especial de la ley de Reciprocidad Cúbica.

Ya hemos distinguido a un primo racional de un primo, a continuación distinguiremos a un primo de un primo-primario

Definición. Sea π primo en $\mathbb{Z}[w]$, diremos que π es primario si $\pi \equiv 2 \pmod 3$.

Observaciones.

I) Si $\pi = q$ es un primo racional, como es primo en $\mathbb{Z}[w]$ se tiene que $\pi = q \equiv 2 \pmod 3$, entonces π es primario.

II) Si $\pi = a+bw$ es un primo complejo en $\mathbb{Z}[w]$ y si π es primario, entonces Tenemos que $\pi = a+bw \equiv 2 \pmod 3$.

III) La definición de primo primario es equivalente a:

π es primo primario, $\pi = a+bw$ en $\mathbb{Z}[w]$ si i $\begin{cases} a \equiv 2 \pmod 3 \\ b \equiv 0 \pmod 3 \end{cases}$.

Demostración:

$\pi \equiv 2 \pmod 3 \iff 3 \mid \pi - 2 \iff \pi - 2 = 3(a'+b'w)$, para algún $a'+b'w$ en $\mathbb{Z}[w]$ y con algún $a', b' \in \mathbb{Z}$, $\iff$

$a+bw-2 = 3a'+3b'w \iff (a-2) = 3a'$ y $bw = 3b'w$

$\iff a \equiv 2 \pmod 3$ y $b \equiv 0 \pmod 3$. ■

PROPOSICION 3.1.5. Si $N\pi = p \equiv 1 \pmod 3$, p primo racional, entonces entre los asociados de π hay sólo un primario.

Demostración. Sea $\pi = a+bw$, entonces los asociados de π son $\pm\pi$, $\pm\pi w$ y $\pm\pi w^2$, es decir, sus asociados son:

1) $\pi = a+bw$. 2) $\pi w = -b+(a-b)w$.

3) $\pi w^2 = (b-a)-aw$. 4) $-\pi = -a-bw$.

5) $-\pi w = b+(b-a)w$. 6) $-\pi w^2 = (a-b)+aw$.

Como $N\pi = p \equiv 1 \pmod 3$ y $N\pi = a^2-ab+b^2$, $3 \nmid p = a^2-ab+b^2$, lo que significa que tanto a como b no son divisibles por 3 al mismo tiempo. Así supongamos que $3 \nmid a$, entonces $\begin{cases} (i)\ a = 3k+1 \\ (ii)\ a = 3k+2 \end{cases}$, para algún $k \in \mathbb{Z}$.

Empezaremos a analizar los casos anteriores.

i) Si $a = 3k+1 \Rightarrow$ (1) no es primario, ya que tendríamos $a \equiv 1 \pmod 3$ lo cual no es lo que buscamos; también (3) no es primario, ya que si fuese tendríamos que $b-a \equiv 2 \pmod 3$ y $-a \equiv 0 \pmod 3$ ↯.

(6) tampoco es primario. Si lo fuese entonces

$a-b \equiv 2 \pmod 3$ y $a \equiv 0 \pmod 3$ ¡¡.

(5) Tampoco es primario, porque si lo fuera entonces $\begin{cases} b \equiv 2 \pmod 3 \\ b-a \equiv 0 \pmod 3 \end{cases} \Rightarrow 2-a \equiv 0 \pmod 3 \Rightarrow a \equiv 2 \pmod 3$ ¡¡.

Falta analizar (2) y (4) para el caso (i) $a = 3k+1$.

(*) Como $a = 3k+1$, para algún $k \in \mathbb{Z}$, entonces $a \equiv 1 \pmod 3$, $a \equiv -2 \pmod 3$ y $-a \equiv 2 \pmod 3$ ..... (*).

Ahora si sucediera que $-b \equiv 0 \pmod 3$ ..... (**).

De (*) y (**) tendríamos que $-a-bw \equiv 2 \pmod 3$, que es lo mismo que (4), entonces (4) sería primario

(++) Por otro lado $a \equiv -2 \pmod 3$ y $a+2 \equiv 0 \pmod 3$ ..... (•)

Ahora si ocurriera que $-b \equiv 2 \pmod 3$ ..... (••)

tendríamos que $a-b \equiv 0 \pmod 3$, sustituyo (••) en (•),

por tanto $\begin{cases} -b \equiv 2 \pmod 3 \\ a-b \equiv 0 \pmod 3 \end{cases} \Rightarrow -b+(a-b)w \equiv 2 \pmod 3$

que es lo mismo que (2), entonces (2) es primario.

De lo anterior tenemos que sólo ocurre (+) ó (++).

Supongamos que ambos son primarios (es decir que (2) y (4) sean primarios).

De (1) tendríamos que $\begin{matrix} a\equiv 1 \pmod 3 \\ b\equiv 0 \pmod 3 \end{matrix}$ entonces $b\equiv 0 \pmod 3$ —(*)

De (2) tendríamos $\begin{matrix} -b\equiv 2 \pmod 3 \\ a-b\equiv 0 \pmod 3 \end{matrix}$ entonces $b\equiv 1 \pmod 3$ —(*)'

observando (*) y (*)' tenemos que sólo ocurre uno y sólo uno de los casos anteriores, es decir, (1) ó (2) es primario. Así (1) es primario, entonces (2) no es primario; o bien (2) es primario, entonces (1) no es primario.

Resumiendo: Si $a=3k+1$, para algún $k\in\mathbb{Z}$, $\pi=a+bw$ y $N\pi=p\equiv 1 \pmod 3$, entonces entre los asociados de π sólo hay un primario.

Veamos el otro caso

ii) Si $a=3k+2$, para algún $k\in\mathbb{Z}$, $a\equiv 2 \pmod 3$ —(*)

Como $N\pi=p=a^2-ab+b^2\equiv 1 \pmod 3$, $1\equiv(4-2b+b^2) \pmod 3$, por (*), entonces $b^2-2b\equiv 0 \pmod 3$, así $3\mid b(b-2)$, por tanto $3\mid b$ ó $3\mid b-2$.

Si $3\mid b$, entonces $b\equiv 0 \pmod 3$ y π es primario

Si $3\mid b-2$, entonces $b\equiv 2 \pmod 3$.

Por tanto $\begin{matrix} (\text{I})' \ a\equiv 2 \pmod 3 \\ (\text{II})' \ b\equiv 2 \pmod 3 \end{matrix} \Rightarrow b-a\equiv 0 \pmod 3$.

Así que $-\pi w = a+(b-a)w \equiv 2 \pmod 3$, entonces $-\pi w$ es primario. De ello se deduce que los demás casos no son primarios.

Si (2) es primario, entonces $-b+(a-b)w \equiv 2 \pmod 3$, entonces $-b \equiv 2 \pmod 3$ ↯ (por (II)').

Si (3) fuera primario, entonces $(b-a)-aw \equiv 2 \pmod 3$, $b-a \equiv 2 \pmod 3$ y $-a \equiv 0 \pmod 3$, $a \equiv 0 \pmod 3$ ↯ (por (I)').

Si (4) fuese primario, entonces $-a-bw \equiv 2 \pmod 3$, $-a \equiv 2 \pmod 3$ y $a \equiv 1 \pmod 3$ ↯ (por (I)').

Si (6) fuera primario, entonces $(a-b)+aw \equiv 2 \pmod 3$, $a \equiv 0 \pmod 3$ ↯ (por (I)'). Con esto "acabamos."

Es decir: $3 \mid b(b-2)$ implica que π ó $-\pi w$ son primarios. Pero π primario, si $b \equiv 0 \pmod 3$; & $-\pi w$ primario, si $b \equiv 2 \pmod 3$, de ello obtenemos que sólo hay un primario entre los asociados de π en el caso (ii).

Así juntando (i) ó (ii) tenemos que entre los asociados de π sólo hay un primario. ∎

Ejemplo.

$\pi = 3+w$ es primo porque $N(3+w) = 7$ y $7 \equiv 1 \pmod 3$.

Así, por la proposición anterior, tenemos que sólo hay un primario entre los asociados de $\pi = 3+w$.

Como $-w^2(3+w) = 2+w$, entonces $-w^2\pi = (2+w)$ es el primo primario asociado a π. ∎

Nota 1. Sea π primario. Si $N\pi \neq 3$ y χ_π carácter cúbico entonces por 3.1.3 II tenemos que:

$$\chi_\pi(w) = w^{\frac{N\pi-1}{3}} = w^n$$

Afirmación (1): $N\pi = 1$ ó 4 ó $7 \pmod 9$

Afirmación (2): $n = 0$ ó 1 ó 2.

Demostración.

1)(i) Si $N\pi \equiv 0 \pmod 9$, $9 \mid N\pi$ y $3 \mid 9$, entonces $3 \mid N\pi$ ↯ por ser π primario ya que $N\pi \equiv 1 \pmod 3$.

(ii) Si $N\pi \equiv 2 \pmod 9$, $N\pi = 2+9k$, para algún $k \in \mathbb{Z}$, luego $\frac{N\pi-1}{3} = \frac{9k+2-1}{3} = \frac{9k+1}{3} = 3k+\frac{1}{3} \notin \mathbb{Z}$, por lo tanto $N\pi \neq 2 \pmod 9$.

(iii) Si $N\pi \equiv 3 \pmod 9$ entonces $N\pi = 3(1+3k)$, para algún

en $\mathbb{Z}$, y $3 \mid 3(1+3k)$ implica $3 \mid N\pi$ ¡ vea (i). Por tanto $N\pi \not\equiv 3 \pmod 9$.

iv) Si $N\pi \equiv 5 \pmod 9$, entonces $N\pi = 5+9k$, para algún $k \in \mathbb{Z}$, $\frac{N\pi-1}{3} = \frac{9k+5-1}{3} = \frac{9k+4}{3} = (3k+1)+\frac{1}{3} \notin \mathbb{Z}$, por tanto $N\pi \not\equiv 5 \pmod 9$

v) Si $N\pi \equiv 6 \pmod 9$, $N\pi = 3(2+3k)$, para algún $k \in \mathbb{Z}$, entonces $3 \mid N\pi$ ¡ vea(i), por tanto $N\pi \not\equiv 6 \pmod 9$.

vi) Si $N\pi \equiv 8 \pmod 9$, entonces $N\pi = 8+9k$, con $k \in \mathbb{Z}$, Sabemos $\frac{N\pi-1}{3} \in \mathbb{Z}$ y sin embargo tenemos que $\frac{N\pi-1}{3} = \frac{9k+8-1}{3} = (3k+2)+\frac{1}{3} \notin \mathbb{Z}$, por tanto tenemos que $N\pi \not\equiv 8 \pmod 9$.

vii) Si $N\pi \equiv 1 \pmod 9$, $N\pi = 1+9k$, para algún $k \in \mathbb{Z}$, luego $\frac{N\pi-1}{3} = \frac{9k}{3} = 3k$. Asi $N\pi \equiv 1 \pmod 9$, entonces $\chi_\pi(w) = W^{\frac{N\pi-1}{3}} = (w^3)^k = 1^k = 1$, ya que $w^3 = 1$, por tanto $\boxed{\chi_\pi(w) = 1 \quad si \quad N\pi \equiv 1 \pmod 9}$

viii) Si $N\pi \equiv 4 \pmod 9$, $N\pi = 4+9k$, para algún $k \in \mathbb{Z}$, asi que $\frac{N\pi-1}{3} = \frac{3+9k}{3} = (1+3k) \in \mathbb{Z}$, por tanto $N\pi \equiv 4 \pmod 9$, entonces $\chi_\pi(w) = w^{\frac{N\pi-1}{3}} = w^{1+3k} =$

$= w(w^3)^k = w$, y asi:

$\chi_\pi(w) = w$ si $N\pi \equiv 4 \pmod 9$.

ix) Si $N\pi \equiv 7 \pmod 9$, $N\pi = 7+9k$, para algún $k \in \mathbb{Z}$, por tanto $\frac{N\pi-1}{3} = (2+3k) \in \mathbb{Z}$, por tanto $N\pi \equiv 7 \pmod 7$, entonces:

$\chi_\pi(w) = w^{\frac{N\pi-1}{3}} = w^{2+3k} = w^2(w^3)^k = w^2$, y asi

$\chi_\pi(w) = w^2$ si $N\pi \equiv 7 \pmod 9$. ∎

A continuación enunciaremos la ley de reciprocidad cúbica.

TEOREMA 1 (LEY DE RECIPROCIDAD CUBICA).
π_1, π_2 primarios, $N\pi_1 \neq 3$, $N\pi_2 \neq 3$ y $N\pi_1 \neq N\pi_2$.
Entonces $\chi_{\pi_2}(\pi_1) = \chi_{\pi_1}(\pi_2)$.

Antes de su demostración veamos algunas observaciones:

OBSERVACION(1).

El carácter cúbico valuado en las unidades es importante. Si χ_π carácter cúbico entonces tenemos que $\chi_\pi(-1)=1 \quad \forall \pi$ primo, porque $-1=(-1)^3$.

Ahora, si $N\pi \neq 3$ tenemos que: $\chi_\pi(w)=w^{\frac{N\pi-1}{3}}$, entonces $\chi_\pi(w)=1$ ó w ó w^2 dependiendo de que la norma de π sea igual a 1 ó 4 ó 7 módulo 9 respectivamente (vea nota1 anterior).

OBSERVACION(2).

Si $1-w$ es primo y si $N\pi\neq 3$, entonces ¿cuál es el valor de $\chi_\pi(1-w)$?. El siguiente resultado nos dice como evaluarlo.

TEOREMA 1' (COMPLEMENTO DE LA LEY DE RECIPROCIDAD CÚBICA)

Supongamos que π primo y $N\pi\neq 3$.

I) Si $\pi=q$, racional, con $q=3m-1$, entonces

$$\chi_\pi(1-w)=w^{2m}.$$

II) Si $\pi=a+bw$ complejo(primario), con $a=3m-1$, entonces $\chi_\pi(1-w)=w^{2m}$.

Demostración.

I) Sabemos que $3 = -w^2(1-w)^2$, por 1.3.3. III,

entonces $-3 = (1-w)^2$, $w^3 = 1$. Como $\pi = q$,

tenemos: $\chi_q(1-w)^2 = \chi_q(-3w) = \chi_q(-3)\,\chi_q(w) =$

$= \chi_q(w)$, por corolario de 3.1.4.

Por tanto $\chi_q(1-w)^2 = \chi_q(w)$

$= w^{\frac{Nq-1}{3}} = w^{\frac{Nq-1}{3}}$, por obs.(1), así que

$\chi_q(1-w)^2 = w^{\frac{Nq-1}{3}}$, entonces elevando al cuadrado tenemos

$\chi_q(1-w)^q = w^{\frac{2}{3}(Nq-1)}$ ..... (*)

y $\chi_q(1-w)^4 = \chi_q(1-w)^3\chi_q(1-w) = \chi_q(1-w)$ por ser χ_q carácter

cúbico. Por lo tanto (*) es de la forma $\chi_q(1-w) = w^{\frac{2}{3}(Nq-1)}$ ..... (*)'

Por hipótesis, $q^2-1 = (3m-1)^2-1 = 9m^2-6m$, entonces

$\frac{2}{3}[Nq-1] = \frac{2}{3}[q^2-1] = \frac{2}{3}[3(3m^2-2m)] = 6m^2-4m \equiv -4m \equiv 2m \pmod 3$,

por tanto $\frac{2}{3}[Nq-1] \equiv 2m \pmod 3$, es decir, $\frac{2}{3}[Nq-1] = 2m+3k$,

para algún $k \in \mathbb{Z}$. Sustituyendolo en (*)' tenemos que:

$\chi_\pi(1-w) = w^{2m+3k} = w^{2m}(w^3)^k = w^{2m}$ ya que $w^3 = 1$, así

$\chi_\pi(1-w) = w^{2m}$ y con esto terminamos (I).

II) Primero afirmamos que $\pi \nmid 3$.

Supongamos que si $\pi \mid 3$ entonces $N\pi \mid 3^2$ implica $3^2 = (N\pi)m$, para algún $m \in \mathbb{N}$, de ello se sigue:

1) $N\pi = 3^2$ y $m = 1$ ó
2) $N\pi = 3$ y $m = 3$ ó
3) $N\pi = 1$ y $m = 3^2$.

De lo cuál la única posibilidad es que $N\pi = 3^2$, ya que los otros casos no pueden ser porque $N\pi \neq 3$ y π es primario-complejo, es decir, $N\pi \neq 1$.

Luego $N\pi = 3^2$, entonces $N\pi = 0 \pmod 9$ ∇_0 por la nota 1, afirmación (1).

O bien $3 \mid N\pi$, así $N\pi \equiv 0 \pmod 3$ ∇_0 pues $\pi \equiv 2 \pmod 3$ y $\overline{\pi} \equiv 2 \pmod 3$ implica $N\pi = \pi\overline{\pi} \equiv 1 \pmod 3$.

Por tanto $\pi \nmid 3$ ..... (1).

Ahora afirmamos : $\chi_\pi(-3) = 1$.

tenemos que $\chi_\pi(-3) = \chi_\pi(-1)\chi_\pi(3) = \chi_\pi(3)$, por corolario de 3.1.4, y $\chi_\pi(3) = 3^{\frac{N\pi - 1}{3}}$, por 3.1.3.II, ... (2)

por tanto $\chi_\pi(-3) = 3^{\frac{N\pi - 1}{3}}$

$= w^n$, por (1) y por 3.1.2 ..... (3)

donde $n=0,1,2$.

De (2) tenemos que $\frac{N\pi-1}{3} \in \mathbb{Z}$, por tanto $3^{\frac{N\pi-1}{3}} \in \mathbb{Z}$, y esto es igual a w^n ($n=0,1,2$ y $w \in \mathbb{C}$), así $n=0$, es decir, que de (3) tenemos que:

$\chi_\pi(-3) = w^0 = 1$, como afirmamos, ...(*).

Por otra parte tenemos que:

$-3w = (1-w)^2$, entonces $\chi_\pi(-3w) = \chi_\pi(1-w)^2$, así que

$\chi_\pi(1-w)^2 = \chi_\pi(-3)\chi_\pi(w) = \chi_\pi(w)$ por (*). Por tanto

$\chi_\pi(1-w)^2 = \chi_\pi(w)$ y $\chi_\pi(1-w) = \left(\chi_\pi(w)\right)^2$ ya que

$\chi_\pi(1-w)^3 = 1$ por ser χ_π caracter cúbico.

Así, $\chi_\pi(1-w) = \left(\chi_\pi(w)\right)^2 = \left(w^{\frac{N\pi-1}{3}}\right)^2$ por obs.(1),

$\chi_\pi(1-w) = w^{\frac{2}{3}(N\pi-1)}$ .....(**).

Ahora de la hipótesis obtenemos dos consecuencias, a saber:

(a) $a \equiv 2 \pmod 3$ y $N\pi \equiv 1 \pmod 3$, entonces $N\pi - 1 \equiv (a^2-1) \pmod 3$.

(b) $\frac{2}{3}[a^2-1] = \frac{2}{3}[(3m-1)^2-1] = \frac{2}{3}[3(3m^2-2m)] = 6m^2 - 4m \equiv 2m \pmod 3$.

Por tanto

$\frac{2}{3}[N\pi-1] \equiv \frac{2}{3}[a^2-1] \equiv 2m \pmod 3$, entonces $\frac{2}{3}[N\pi-1] = 2m+3k$,

para algún $k \in \mathbb{Z}$, sustituyendo esto en (**) obtenemos:

$\chi_\pi(1-w) = w^{2m+3k} = w^{2m}(w^3)^k = w^{2m}$, entonces

$\chi_\pi(1-w) = w^{2m}$. ∎

§ 2 PRUEBA DE LA LEY DE RECIPROCIDAD CUBICA.

Si π primo complejo tal que $N\pi = p \equiv 1 \pmod 3$, entonces

$\left| \frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]} \right| = p$ & $\left| \frac{\mathbb{Z}}{p\mathbb{Z}} \right| = p$, es decir,

$$\frac{\mathbb{Z}[w]}{\pi\mathbb{Z}[w]} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}} \left(:= \mathbb{F}_p\right).$$

Por tanto, podemos considerar a χ_π como carácter cúbico sobre $\mathbb{Z}/p\mathbb{Z}$ y de esta forma trabajar con sumas de Gauss, $g_a(\chi_\pi)$, y sumas de Jacobi, $J(\chi_\pi, \chi_\pi)$.

Si χ es carácter cúbico, entonces por el corolario de 2.3.3 y por 2.3.4 tenemos que (observaciones):

I) $g(\chi)^3 = p J(\chi,\chi)$ donde $N\pi = p \equiv 1 \pmod 3$.

II) Si: $J(\chi,\chi) = a + b\omega$ entonces $a \equiv -1 \pmod 3$ & $b \equiv 0 \pmod 3$.

Como $|J(\chi,\chi)| = \sqrt{p}$, entonces $N J(\chi,\chi) = p$ y por tanto $J(\chi,\chi)$ es primo en $\mathbb{Z}[\omega]$. Por otro lado $a \equiv -1 \pmod 3$ y $b \equiv 0 \pmod 3$, es decir, $a \equiv 2 \pmod 3$ y $b \equiv 0 \pmod 3$, entonces $J(\chi,\chi)$ es primario de norma p.

LEMA. $J(\chi_\pi, \chi_\pi) = \pi$

Demostración. Como χ_π es carácter cúbico entonces por obs. (II), $J(\chi_\pi, \chi_\pi) = \pi^*$. Pero $N J(\chi_\pi, \chi_\pi) = \pi\bar{\pi} = p = \pi^*\bar{\pi}^*$, entonces $\pi\bar{\pi} = \pi^*\bar{\pi}^*$, por tanto $\pi = \pi^*$. Si este no es entonces le ponemos etiqueta al otro de tal forma que $\pi = \pi^*$.

COROLARIO. $g(\chi_\pi)^3 = p\pi$.

LEMA 2. Si p primo en $\mathbb{Z}-\{2,3\}$, entonces

$$1^k+2^k+\cdots+(p-1)^k \equiv \begin{cases} -1 \pmod p. & \text{si } p-1 \mid k \quad \cdots\cdots (I) \\ 0 \pmod p & \text{. si } p-1 \nmid k \quad \cdots\cdots (II) \end{cases}$$

Demostración.

I) Si $p-1 \mid k$, entonces $k=(p-1)r$ para algún $r\in\mathbb{Z}$, éste implica que

$$1^k+2^k+\cdots+(p-1)^k=\left(1^{p-1}\right)^r+\left(2^{p-1}\right)^r+\cdots+\left([p-1]^{p-1}\right)^r \equiv (p-1) \pmod p,$$

ya que $(i,p)=1$ con $1\le i\le p-1$ entonces $i^{p-1}\equiv 1 \pmod p$,

por tanto $$1^k+2^k+\cdots+(p-1)^k \equiv -1 \pmod p.$$

II) Si $p-1 \nmid k$, sea $\langle g\rangle = \mathbb{F}_p^*$ entonces

$\mathbb{F}_p^*=\{g^0, g^1, \ldots, g^{p-2}\}=\{\bar{1},\bar{2},\ldots,\overline{p-1}\}$, por tanto

$$1^k+2^k+\cdots+(p-1)^k \equiv 1^{0k}+g^k+g^{2k}+\cdots+g^{(p-2)k} \equiv$$

$$\equiv 1+g^k+(g^k)^2+\cdots+(g^k)^{p-2} \equiv$$

$$\equiv \frac{(g^k)^{p-1}-1}{g^k-1} \pmod p \quad \text{---------- (**)}$$

Como $p-1 \nmid k$, entonces $g^k\neq 1$ y $g^k-1\neq 0$ y como $|\langle g\rangle|=p-1$ entonces $(g^k)^{p-1}=1$ y $(g^k)^{p-1}-1=0$, por tanto

$$\frac{(g^k)^{p-1}-1}{g^k-1} \equiv 0 \pmod{p}. \blacksquare$$

TEOREMA 1 (LEY DE RECIPROCIDAD CUBICA).

Sean π_1, π_2 primarios, $N\pi_1 \neq 3$, $N\pi_2 \neq 3$ y $N\pi_1 \neq N\pi_2$.

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

Demostración. La demostración consta de varios casos:

I) Si π_1 y π_2 son racionales.

II) Si π_1 racional y π_2 complejo.

III) Si π_1 y π_2 complejos.

Prueba:

I) Inmediato del corolario de 3.3.4

II) Sea $\pi_1 = q \equiv 2 \pmod 3$ y $\pi_2 = \pi$ con $N\pi = p$.

Observación: $N\pi \neq p^2$, pues si $N\pi = p^2$ entonces sea $\pi = a+bw$ y tendríamos que: $N\pi = (a+bw)\overline{(a+bw)} = p^2$ y $(a+bw)(a+b\bar{w}) = p \cdot p$, así $a+bw = p$ y $a+b\bar{w} = p$, entonces $w = \bar{w}$ y $\bar{w} = w^2$, por tanto $w = w^2$ ∇ ya que son diferentes en $\mathbb{Z}[w]/\pi\mathbb{Z}[w]$.

Ahora por el corolario del lema 1 tenemos que:

$g(\chi_\pi)^3 = p\pi$ y si lo elevamos a la $\frac{Nq-1}{3}$ tenemos

$g(\chi_\pi)^{Nq-1} = (p\pi)^{\frac{Nq-1}{3}}$, asi $g(\chi_\pi)^{Nq} = (p\pi)^{\frac{Nq-1}{3}} g(\chi_\pi)$.

Por tanto $g(\chi_\pi)^{Nq} = (p\pi)^{\frac{Nq-1}{3}} g(\chi_\pi)$, $Nq = q^2$,

$g(\chi_\pi)^{q^2} \equiv \chi_q(p\pi)\, g(\chi_\pi) \pmod{q}$, por 3.1.3.II, ... (*)

$\chi_q(p\pi) = \chi_q(p)\,\chi_q(\pi)$

$= \chi_q(\pi)$ por corolario de 3.1.4.

Entonces (*) se trasforma en:

$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)\, g(\chi_\pi) \pmod{q}$ ..... (1)

Ahora, desarrollando $g(\chi_\pi)^{q^2}$ por medio de sumas gaussianas,

$g(\chi_\pi)^{q^2} = \left(\sum \chi_\pi(t) \zeta^t\right)^{q^2}$ (por definición)

$\equiv \sum \chi_\pi(t)^{q^2} \zeta^{tq^2} \pmod{q}$ ..... (*)'

como $q \equiv 2 \pmod 3$, entonces $q^2 \equiv 1 \pmod 3$ y $q^2 = 1 + 3k$, para algún $k \in \mathbb{Z}$, sustituyendo en (*)' tenemos que:

$$g(\chi_\pi)^{q^2} \equiv \sum \chi_\pi(t)^{1+3k} \zeta^{q^2 t} \pmod{q}$$

$$\equiv \sum \chi_\pi(t)\, \chi_\pi(t)^{3k} \zeta^{q^2 t} \pmod{q}$$

$$\equiv \sum \chi_\pi(t) \zeta^{q^2 t} \pmod{q} \quad \text{por ser } \chi_\pi \text{ carác}$$

$$\underline{t}\text{er cúbico}$$

$$\equiv g_{q^2}(\chi_\pi) \pmod{q} \quad \text{(definición de suma)} \ldots\ldots (2).$$

Ahora analizando a $g_{q^2}(\chi_\pi)$.

$$g_{q^2}(\chi_\pi) = \chi_\pi\left((q^2)^{-1}\right) g(\chi_\pi) = \text{por 2.2.1. I.}$$

$$= \chi_\pi(q)^{-2}\, g(\chi_\pi) = \text{y como } -2 = 1+3(-1)$$

$$= \chi_\pi(q)^{1+3(-1)}\, g(\chi_\pi) =$$

$$= \chi_\pi(q)\left(\left[\chi_\pi(q)\right]^3\right)^{-1} g(\chi_\pi)$$

$$= \chi_\pi(q)\, g(\chi_\pi) \quad \text{por ser } \chi_q \text{ carácter cúbico.}$$

Entonces

$$g_{q^2}(\chi_\pi) = \chi_\pi(q)\, g(\chi_\pi) \ldots\ldots\ldots\ldots (3),$$

sustituyendo (3) en (2) obtenemos:

$$g(\chi_\pi)^{q^2} \equiv \chi_\pi(q)\, g(\chi_\pi) \pmod{q} \ldots\ldots\ldots\ldots (4)$$

de (1) y (4) obtenemos que:

$\chi_\pi(q)\, g(\chi_\pi) \equiv \chi_q(\pi)\, g(\chi_\pi) \pmod{q}$ ..... (5),

multiplicando a (5) por $\overline{g(\chi_\pi)}$ Tenemos

$\chi_\pi(q)\left[g(\chi_\pi)\overline{g(\chi_\pi)}\right] \equiv \chi_q(\pi)\left[g(\chi_\pi)\overline{g(\chi_\pi)}\right] \pmod{q}$ y por

observación 2 de 2.2.2, tenemos que:

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

$[(p,q)=1]$. Como $\chi_\pi(q) = w^n$ para $n \in \{0,1,2\}$,

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

Veamos III.

III) Si π_1 y π_2 complejos. Sea $N\pi_1 = p_1 \equiv 1 \pmod{3}$,

$N\pi_2 = p_2 \equiv 1 \pmod{3}$ (por hipótesis, $p_1 \neq p_2$).

Si $\gamma_1 := \overline{\pi}_1$ & $\gamma_2 := \overline{\pi}_2$, entonces γ_1 y γ_2 son primarios ya que π_1 y π_2 lo son. Empezamos, (el razonamiento es **similar**) tenemos que:

$g(\chi_{\gamma_1})^3 = p_1 \gamma_1$, entonces $g(\chi_{\gamma_1})^{N\pi_2 - 1} = (p_1 \gamma_1)^{\frac{N\pi_2 - 1}{3}}$ y

$N\pi_2 = p_2$ por consiguiente

$$g(\chi_{\gamma_1})^{p_2-1} = (p_1\gamma_1)^{\frac{N\pi_2-1}{3}}, \quad g(\chi_{\gamma_1})^{p_2} g(\chi_{\gamma_1})^{-1} = (p_1\gamma_1)^{\frac{N\pi_2-1}{3}} \quad y$$

$$g(\chi_{\gamma_1})^{p_2} \equiv (p_1\gamma_1)^{\frac{N\pi_2-1}{3}} g(\chi_{\gamma_1}) \pmod{\pi_2}, \text{ así que}$$

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\pi_2}(p_1\gamma_1)\, g(\chi_{\gamma_1}) \pmod{\pi_2} \text{ (por 3.3.3 II)} \ldots\ldots (1)$$

Analizamos $g(\chi_{\gamma_1})^{p_2}$ vía sumas de Gauss.

$$g(\chi_{\gamma_1})^{p_2} = \left(\sum \chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \quad \text{(definición de suma)}$$

$$\equiv \sum \chi_{\gamma_1}(t)^{p_2} \zeta^{p_2 t} \pmod{\pi_2}$$

$$\equiv \sum \chi_{\gamma_1}(t)^{1+3k} \zeta^{p_2 t} \pmod{\pi_2} \quad (\text{ya que } p_2 \equiv 1 \pmod 3)$$

$$g(\chi_{\gamma_1})^{p_2} \equiv \sum \chi_{\gamma_1}(t)\, \zeta^{p_2 t} \pmod{\pi_2} \quad \text{(por ser } \chi_{\gamma_1} \text{ caracter}$$

cúbico), por tanto

$$g(\chi_{\gamma_1})^{p_2} \equiv g_{p_2}(\chi_{\gamma_1}) \pmod{\pi_2} \quad \text{(def de suma)} \ldots\ldots (2)$$

Por otro lado $g_{p_2}(\chi_{\gamma_1})$ se puede ver como

$$g_{P_2}(\chi_{\gamma_1}) = \chi_{\gamma_1}(P_2^{-1})\, g(\chi_{\gamma_1}) \quad \text{por 2.2.1.I}$$

$$= \chi_{\gamma_1}(P_2)^{-1} g(\chi_{\gamma_1})$$

$$= \chi_{\gamma_1}(P_2)^{2+3(-1)} g(\chi_{\gamma_1}) = \chi_{\gamma_1}(P_2)^2 \chi_{\gamma_1}(P_2)^{3(-1)} g(\chi_{\gamma_1}),$$

por tanto

$$g_{P_2}(\chi_{\gamma_1}) = \chi_{\gamma_1}(P_2)^2 g(\chi_{\gamma_1}) \quad \ldots\ldots\ldots\ldots\ldots (3)$$

sustituyendo (3) en (2) obtenemos:

$$g(\chi_{\gamma_1})^{P_2} \equiv \chi_{\gamma_1}(P_2^2)\, g(\chi_{\gamma_1}) \pmod{\pi_2} \quad \ldots\ldots\ldots\ldots (4)$$

de (1) y (4)

$$\chi_{\gamma_1}(P_2^2)\, g(\chi_{\gamma_1}) \equiv \chi_{\pi_2}(P_1\gamma_1)\, g(\chi_{\gamma_1}) \pmod{\pi_2} \quad \ldots\ldots\ldots (5)$$

multiplicando a (5) por $\overline{g(\chi_{\gamma_1})}$ tenemos

$$\chi_{\gamma_1}(P_2^2)\left[g(\chi_{\gamma_1})\,\overline{g(\chi_{\gamma_1})}\right] \equiv \chi_{\pi_2}(P_1\gamma_1)\left[g(\chi_{\gamma_1})\,\overline{g(\chi_{\gamma_1})}\right] \pmod{\pi_2}$$

$$\chi_{\gamma_1}(P_2^2)\, P_1 \equiv \chi_{\pi_2}(P_1\gamma_1)\, P_1 \pmod{\pi_2} \quad \text{por obs 2 en 2.2.2,}$$

$$\chi_{\gamma_1}(P_2^2) \equiv \chi_{\pi_2}(P_1\gamma_1) \pmod{\pi_2} \quad \text{por ser } \pi \text{ primo primario,}$$

Entonces $\chi_{\gamma_1}(P_2^2) = \chi_{\pi_2}(P_1\gamma_1)$ $\ldots\ldots\ldots\ldots\odot$

Ahora en forma análoga, saquemos un resultado para $g(\chi_{\pi_2})^3$:

Sabemos que

$$g(\chi_{\pi_2})^3 = p_2 \pi_2 \ , \ g(\chi_{\pi_2})^{p_1} \equiv \chi_{\pi_1}(p_2 \pi_2)\, g(\chi_{\pi_2}) \pmod{\pi} \quad \ldots\ldots (1)'$$

Por otro lado

$$g(\chi_{\pi_2})^{p_1} = \left(\sum \chi_{\pi_2}(t)\, \zeta^t\right)^{p_1} \quad (\text{def de suma de Gauss a } \chi_{\pi_2})$$

$$\equiv \sum \chi_{\pi_2}(t)^{p_1}\, \zeta^{t p_1} \pmod{\pi_1}$$

$$g(\chi_{\pi_2})^{p_1} \equiv \sum \chi_{\pi_2}(t)^{p_1}\, \zeta^{t p_1} \pmod{\pi_1} \quad y$$

$$g(\chi_{\pi_2})^{p_1} \equiv g_{p_1}(\chi_{\pi_2}) \pmod{\pi_1} \quad (\text{def de suma de Gauss}) \ldots (2)'$$

Analizamos: $g_{p_1}(\chi_{\pi_2}) = \chi_{\pi_2}(p_1^{-1})\, g(\chi_{\pi_2})$ por 2.2.1.I

$$= \chi_{\pi_2}(p_1)^{-1} g(\chi_{\pi_2}) \ , \text{ entonces}$$

$$g_{p_1}(\chi_{\pi_2}) = \chi_{\pi_2}(p_1)^{2+3(-1)}\, g(\chi_{\pi_2}) \ ,$$

$$= \chi_{\pi_2}(p_1)\, \chi_{\pi_2}(p_1)^{3(-1)}\, g(\chi_{\pi_2}) \ ,$$

$$g_{p_1}(\chi_{\pi_2}) = \chi_{\pi_2}(p_1)\, g(\chi_{\pi_2}) \quad \ldots\ldots (3)'$$

sustituyendo (3)' en (2)' obtenemos:

$$g(\chi_{\pi_2})^{P_1} \equiv \chi_{\pi_2}(P_1)\, g(\chi_{\pi_2}) \pmod{\pi_1} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (4)'$$

de (1)' y (4)' obtenemos:

$$\chi_{\pi_2}(P_1^2)\, g(\chi_{\pi_2}) \equiv \chi_{\pi_1}(P_2\pi_2)\, g(\chi_{\pi_2}) \pmod{\pi_1}, \text{ así}$$

$$\chi_{\pi_2}(P_1^2)\left[g(\chi_{\pi_2})\overline{g(\chi_{\pi_2})}\right] \equiv \chi_{\pi_1}(P_2\pi_2)\left[g(\chi_{\pi_2})\overline{g(\chi_{\pi_2})}\right] \pmod{\pi_1},$$

$$\chi_{\pi_2}(P_1^2)\, P_2 \equiv \chi_{\pi_1}(P_2\pi_2)\, P_2 \pmod{\pi_1} \quad \text{(por obs. 2 en 2.2.2)},$$

entonces $\chi_{\pi_2}(P_1^2) \equiv \chi_{\pi_1}(P_2\pi_2) \pmod{\pi_1}$. Por tanto

$$\chi_{\pi_2}(P_1^2) = \chi_{\pi_1}(P_2\pi_2) \quad \ldots\ldots\ldots\ldots\ldots \quad \odot'$$

Afirmo que: $\chi_{\gamma_1}(P_2^2) = \chi_{\pi_1}(P_2)$.

En efecto, pues

$$\begin{aligned}
\chi_{\gamma_1}(P_2^2) &= \overline{\chi_{\gamma_1}(P_2)} && \text{(por 3.1.4.I)}\\
&= \chi_{\overline{\gamma_1}}(\overline{P_2}) && \text{(por 3.1.4.II)}\\
&= \chi_{\overline{\gamma_1}}(P_2) && (\overline{P_2} = P_2)\\
&= \chi_{\pi_1}(P_2). && (\overline{\pi_1} = \gamma_1 \text{ y } \pi_1 = \overline{\overline{\pi_1}} = \overline{\gamma_1},\ \pi_1 = \overline{\gamma_1})
\end{aligned}$$

Finalmente consideramos:

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(P_1\gamma_1') &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1'}(P_2^2) && (\text{por } \odot)\\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(P_2) && (\text{por afirmación})\\
&= \chi_{\pi_1}(\pi_2 P_2) && (\text{por ser } \chi_{\pi_1} \text{ homomorfismo})\\
&= \chi_{\pi_2}(P_1^2) && (\text{por } \odot')\\
&= \chi_{\pi_2}(P_1 P_1)\\
&= \chi_{\pi_2}(P_1\gamma_1'\pi_1') && (P_1 = N\pi_1' = \pi_1\gamma_1')\\
&= \chi_{\pi_2}(\pi_1')\chi_{\pi_2}(P_1\gamma_1') && (\text{por ser } \chi_{\pi_2} \text{ hom.}).
\end{aligned}$$

Por tanto

$[\chi_{\pi_1}(\pi_2) - \chi_{\pi_2}(\pi_1')]\chi_{\pi_2}(P_1\gamma_1') = 0$ y como $P_1\gamma_1' \neq 0$,

entonces $\chi_{\pi_2}(P_1\gamma_1') \neq 0$, por lo que

$\chi_{\pi_1}(\pi_2) - \chi_{\pi_2}(\pi_1') = 0$ implica que $\boxed{\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1')}$. ∎

REFERENCIAS

1. Ireland. K, Rosen M., A classical introduction to Modern Number Theory. Springer Verlag 1981.

2. Lang S. Algebra . Addison Wesley 1984.

3. Leveque W.J. Elementary Number Theory, Vol.I. Addison Wesley 1956.

4. Van Dar Waerdern B.L. Algebra, Vol.I Frederick Unger 1970.