UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

METODOS CICLOTOMICOS EN LA TEORIA DE LOS NUMEROS

TESIS

Que para obtener el título de

M A T E M A T I C O

P R E S E N T A

MA. DEL CARMEN H. GOMEZ LAVEAGA

MEXICO, D. F. MARZO 1971

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

METODOS CICLOTOMICOS EN LA TEORIA DE LOS NUMEROS

Tesis Profesional que para obtener el título de Matemático presenta:

Ma. del Carmen H. Gómez Laveaga

Marzo de 1971.

A MIS PADRES.

Este trabajo fue realizado bajo la dirección del Dr. Raymundo Bautista Ramos, a quien agradezco sinceramente su valiosa ayuda.

I N D I C E

INTRODUCCION

Uno de los más famosos problemas en la Teoría de Números es el llamado problema de Waring, y es el siguiente:

Dado un entero fijo $k \geq 2$, encontrar un natural s (que depende de k), tal que cada n se puede expresar, por lo menos en una forma, de la siguiente manera:

$$n = a_1^k + a_2^k + \cdots + a_s^k$$

donde $a_1, \ldots, a_s$ son enteros no negativos, no necesariamente distintos.

La solución a este problema fue dada por Hilbert, un siglo después, y fue un triunfo más para el análisis que para la teoría de números, aunque Hilbert solo demostró la existencia de tal solución. Es conocido que para resolver el problema de Waring es necesario conocer el número de soluciones de la congruencia

$$x^e + y^e + 1 \equiv 0 \qquad (\text{mod. } p = ef + 1)$$

Ahora bien, éste número se puede poner en función del número de soluciones de

$$1 + g^{et+k} \equiv g^{ez+h}$$

donde $0 \leq t, \quad z \leq f - 1, \quad 0 \leq k, \quad h \leq e - 1$ y g es una raiz primitiva de p.

Estos números se pueden calcular, como lo haremos, para

$$e = 2, 3, 4, 5$$

Para esto introducimos las siguientes sumas

$$\eta_k = \sum_{t=0}^{f-1} R^{g^{et+k}}$$

a las que llamaremos períodos, siendo $R \neq 1$ una raiz primitiva p-ésima de la unidad, y con ésto llegamos al siguiente resultado:

$$\eta_m \eta_{m+k} = \sum_{h=0}^{e-1} (k,h) \eta_{m+h+fs_k}$$

donde (k,h) es la constante ciclotómica definida en el capítulo I y s_k se define en el capítulo II.

Posteriormente se llega a la siguiente igualdad:

$$\sum_{h=0}^{e-1} (k,h) = f - s_k$$

muy importante para resolver nuestro problema.

Para los casos $e = 3, 4, 5$ es necesario obtener más relaciones, y para esto introducimos la función de Jacobi

$$F(\alpha) = \sum_{k=0}^{p-2} \alpha^k R^{g^k}$$

con $\alpha \neq 1$ una raiz de $x^{p-1} = 1$ y si $R(m,n)$ se define como

$$R(m,n) = \frac{F(\beta^m)\ F(\beta^n)}{F(\beta^{m+n})}$$

con β una raiz primitiva e-ésima de la unidad, se llega a que

$$R(m,n)\ R(-m,-n) = p$$

con m y n no divisibles por e. Además $R(m,n)$ está en función de las constantes ciclotómicas.

Finalmente se ve el teorema de Jacobi en el que se demuestra una propiedad de la función de Jacobi.

CAPITULO I

El problema principal del presente trabajo es encontrar el número de soluciones de la siguiente ecuación:

$$x^e + y^e + 1 \equiv 0 \pmod{p}$$

donde p es un primo de la forma $p = ef + 1$ con $1 < e < p - 1$.

Nota: El caso $e = 1$ es trivial.

Trataremos en primer lugar la ecuación más general:

$$(1) \quad \sum_{i=1}^{n} c_i x_i^e \equiv d \pmod{p}, \quad p = ef + 1.$$

Veremos que el número de soluciones de esta congruencia está en función del número de conjuntos de valores $z_1, z_2, \ldots, z_n$ entre $0, \ldots, f - 1$ que satisfacen

$$(2) \quad \sum_{i=1}^{n} g^{ez_i + a_i} \equiv d \pmod{p}$$

donde g es una raíz primitiva de p y $c_i \equiv g^{a_i} \pmod{p}$.

Con mayor precisión tenemos el siguiente teorema:

TEOREMA 1. Si ninguna c_i es divisible por el primo $p = ef+1$, el número de soluciones $x_1, \ldots, x_n$ todos primos a p, de

$$\sum_{i=1}^{n} c_i x_i^e \equiv d \pmod{p}$$

es e^n veces el número de conjuntos de valores $z_1, \ldots, z_n$, escogidos de $0, 1, \ldots, f-1$, que satisfacen

$$\sum_{i=1}^{n} g^{ez_i + a_i} \equiv d \pmod{p}$$

donde g es una raíz primitiva de p y $c_i \equiv g^{a_i} \pmod{p}$.

Demostración.

Sean $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} c_i x_i^e - d$

$$g(y_1, \ldots, y_n) = \sum_{i=1}^{n} g^{ey_i + a_i} - d$$

Tomemos una solución $(x_1, \ldots, x_n)$ de $f(x_1, \ldots, x_n) \pmod{p}$ y $x_i \neq 0 \ (i=1, \ldots, n)$. Para cada x_i tenemos

$$x_i \equiv g^{y_i} \pmod{p} \quad \text{con} \quad 0 \leq y_i \leq p-2,$$ ya que $g, g^2, \ldots, g^{p-1}$ forma un sistema reducido de residuos módulo p.

Consideremos $(y_1, \ldots, y_n)$ determinada por $(x_1, \ldots, x_n)$

$$\sum_{i=1}^{n} g^{a_i + ey_i} - d \equiv \sum_{i=1}^{n} g^{a_i} g^{ey_i} - d \equiv \sum_{i=1}^{n} c_i y_i^e - d \equiv 0 \pmod{p}$$

$\therefore (y_1, \ldots, y_n)$ es una solución de $g(y_1, \ldots, y_n)$.

Entonces el número de soluciones de f es igual al número de

soluciones $(y_1, \ldots, y_n)$ tomadas módulo $(p-1)$ de g.

Ahora, sea $(y_1, \ldots, y_n)$ una solución de g.

Para cada y_i se tiene:

$$y_i = q_i f + z_i, \qquad 0 \leq z_i \leq f-1 \qquad y \qquad 0 \leq q_i \leq e-1$$

$$0 \equiv \sum_{i=1}^{n} g^{a_i + e y_i} - d \equiv \sum_{i=1}^{n} g^{a_i + e(q_i f + z_i)} - d \equiv \sum_{i=1}^{n} g^{a_i + e z_i} - d \pmod{p}$$

$$\therefore \quad \sum_{i=1}^{n} g^{e z_i + a_i} - d \equiv 0 \pmod{p} \qquad (*)$$

$\therefore$ cada $(y_1, \ldots y_n)$ determina una solución $(z_1, \ldots, z_n)$ de $(*)$.

Si $(z_1, \ldots, z_n)$ es una solución de $(*)$, tenemos:

$$g^{e z_i + a_i} \equiv g^{e(q_i f + z_i) + a_i} \pmod{p} \quad \text{donde} \quad 0 \leq q_i \leq e-1$$

Hay e posibilidades para q_i

$\therefore$ $(z_1, \ldots, z_n)$ determina e^n soluciones de $g(y_1, \ldots, y_n)$.

Por lo tanto se tiene que el número de soluciones $f(x, \ldots, x_n)$ es e^n veces el número de conjuntos de valores $z_1, \ldots, z_n$ escogidos entre 0 y $f-1$ que satisfacen

$$\sum_{i=1}^{n} g^{e z_i + a_i} \equiv d \pmod{p}$$

COROLARIO: El número de soluciones primas a $p = ef+1$ de

$$x^e + y^e \equiv 1 \pmod{p}$$

es e^2 veces el número de conjuntos de valores $z_1, \ldots, z_n$ escogidos de $0, \ldots, f-1$ que satisfacen

$$g^{ez_1} + g^{ez_2} \equiv 1 \pmod{p}$$

En este caso $n = 2$, $1 \equiv g^{a_i}$ y por lo tanto $a_i = 0$, $i = 1, 2$.

Ahora, consideremos $N = 1 + g^{et+k}$, con $0 \leq t \leq f-1$ y $0 \leq k \leq e-1$.

Si $N \not\equiv 0 \pmod{p}$, entonces N es congruente a una potencia de la raíz primitiva g:

$$1 + g^{et+k} \equiv g^{ez+h} \pmod{p = ef+1} \tag{3}$$

donde $0 \leq h \leq e-1$, $0 \leq z \leq f-1$.

DEFINICION: Para k y h fijas, sea (k,h) el número de conjuntos de valores de t y z, cada uno escogidos de $0, 1, \ldots, f-1$, para los cuales (3) es válida.

A (k,h) se le llama constante ciclotómica.

Si incrementamos k ó h por un múltiplo de e, (k,h) no se altera.

TEOREMA 2. Para k y h escogidos entre 0,1,...,e-1, la congruencia

$$1 + g^{k} x^{e} \equiv g^{h} y^{e} \pmod{p = ef+1} \tag{4}$$

tiene exactamente:

i) $e^2(k,h)$ soluciones si $h \neq 0$ y $k \neq 0$ si f es par, $k \neq e/2$ si f es impar.

ii) $e + e^2(k,h)$ soluciones si $h = 0$ y $k \neq 0$ si f es par, $k \neq e/2$ si f es impar.o si $h \neq 0$ y $k = 0$ si f es par, $k = e/2$ si f es impar.

iii) $2e + e^2(k,h)$ soluciones si $h = 0$ y $k = 0$ si f es par, $k = e/2$ si f es impar.

Demostración

Por el teorema anterior, (4) tiene $e^2(k,h)$ soluciones primas a p.

i) Si $h \neq 0$ y $k \neq 0$ si f es par, $k \neq e/2$ si f es impar.

Las soluciones (x,y) con $x = 0$ satisfacen:

$$1 \equiv g^{h} y^{e} \pmod{p}$$

$$g^{-h} \equiv y^{e} \pmod{p}$$

$$\therefore \quad -h \equiv e \operatorname{ind}_{g} y \pmod{ef}$$

$\Rightarrow \qquad e \mid h$

que es una contradicción, ya que $0 < h \leq e-1$

$\therefore$ no tiene soluciones con $x \neq 0$

Las soluciones con $y = 0$ satisfacen:

$$1 + g^k x^e \equiv 0 \pmod{p}$$

$$x^e \equiv -g^k \pmod{p}$$

$x \equiv g^s$, para alguna s tal que $0 \leq s \leq p-2$

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

$$g^{es} \equiv g^{k+\frac{1}{2}(p-1)} \pmod{p}$$

$$es \equiv k+\tfrac{1}{2}(p-1) \pmod{ef}$$

$$es = k+\tfrac{1}{2}(ef)+(ef)m$$

Si f es par, entonces $e \mid k$, lo que no puede ser pues $0 < k \leq e-1$.

Si f es impar, entonces e es par y por lo tanto $e/2 \mid k$, lo que implica que $k = e/2$, que no es posible pues $k \neq e/2$ si f es impar.

$\therefore$ (4) no tiene soluciones con $y = 0$.

Por lo tanto, (4) tiene $e^2(k,h)$ soluciones en éste caso.

ii) Si $h = 0$ y $k \neq 0$ si f es par, $k \neq e/2$ si f es impar.

Si (x,y) es solución tal que $x = 0$, se tiene

$$1 \equiv g^h y^e \equiv y^e \pmod{p}$$

Pero la congruencia $1 \equiv y^e \pmod{p}$ tiene e soluciones.

$\therefore$ (4) tiene e soluciones con $x = 0$.

Si (x,y) es tal que $y = 0$, entonces $e \mid k$ si f es par ó $e/2 = k$ si f es impar.

Ahora, si $h \neq 0$ y $k = 0$ si f es par, $k = e/2$ si f es impar no tiene soluciones con $x = 0$ ya que $e \nmid h$.

Si $y = 0$ cumple la condición de que $k = 0$ si f es par y $k = e/2$ si f es impar.

$\therefore$ tiene $e + e^2(k,h)$ soluciones.

iii) Si $h = 0$ y $k = 0$ si f es par, $k = e/2$ si f es impar tiene e soluciones con $x = 0$ y e soluciones con $y = 0$.

$\therefore$ tiene $2e + e^2(k,h)$ soluciones.

q.e.d.

TEOREMA 3. Cuando f es par, la congruencia

$$1 + g^k x^e \equiv -g^h y^e \pmod{p = ef+1} \qquad (5)$$

tiene el mismo número de soluciones que (4).

Cuando f es impar, el número de soluciones es $N = e^2(k, h+\frac{1}{2}e)$ si $h \neq \frac{1}{2}e$, $k \neq \frac{1}{2}e$; $e+N$ si $h \neq \frac{1}{2}e$, $k = \frac{1}{2}e$ ó $h = \frac{1}{2}e$, $k \neq \frac{1}{2}e$; $2e+N$ si $h = k = \frac{1}{2}e$.

Demostración.

Si f es par, existe $w \in \mathbb{Z}$ tal que $\operatorname{ord}_p w = 2e$ porque

$$p - 1 = 2e\, f/2 \quad \text{y} \quad \operatorname{ord}_p g^{f/2} = 2e$$

$$\therefore \quad w^{2e} \equiv 1 \pmod{p}$$

$$\text{y} \quad w^{e} \equiv -1 \pmod{p}$$

Entonces

$$1 + g^k x^e \equiv -g^h y^e \equiv g^h w^e y^e \equiv g^h (wy)^e \pmod{p}$$

$$\therefore \quad 1 + g^k x^e \equiv g^h (wy)^e \pmod{p}$$

Esta última congruencia tiene el mismo número de soluciones que (5) y además es de la forma (4).

$\therefore$ tiene el mismo número de soluciones que (4).

Si f es impar, tenemos:

$$1 + g^k x^e \equiv -g^h y^e \pmod{p}$$

$$-g^h \equiv g^h \, g^{\frac{1}{2}(p-1)} \equiv g^{h-\frac{1}{2}e+e(\frac{f+1}{2})} \equiv g^{h-\frac{1}{2}e} \, g^{\frac{1}{2}(f+1)e} \pmod{p}$$

$\therefore$ (5) es equivalente a

$$1 + g^k x^e \equiv g^{h-\frac{1}{2}e} \left(g^{\frac{1}{2}(f+1)} y\right)^e \pmod{p}$$

y esta congruencia es de la forma (4).

Utilizando el teorema (2) tenemos que si $h - \frac{1}{2}e \neq 0$ y $k \neq \frac{1}{2}$ entonces tiene $N = e^2(k, h \pm \frac{1}{2}e)$ soluciones; si $h \neq \frac{1}{2}e$ y $k = \frac{1}{2}e$ ó $h = \frac{1}{2}e$, y $k \neq \frac{1}{2}e$ tiene $e + N$ soluciones; si $h = k = \frac{1}{2}e$ tiene $2e + N$ soluciones.

TEOREMA 4: Si f es impar, el número de soluciones de

$$1 + x^e + y^e \equiv 0 \pmod{p = ef+1}$$

es $e^2(0, \frac{1}{2}e)$. Si f es par, tiene el mismo número de soluciones que (2).

Demostración.

$$1 + x^e \equiv -y^e \equiv g^{\frac{1}{2}ef} \, y^e \equiv g^{e/2} \left(g^{\frac{1}{2}(f-1)} y\right)^e \pmod{p}$$

$\therefore$ si f es impar tiene $e^2(0, \frac{1}{2}e)$ soluciones, por el teorema 2.

Si f es par tiene el mismo número de soluciones que (2).

CAPITULO II

Caso $e = 2$

Hemos visto en el capítulo anterior que el número de soluciones de las congruencias que se dan, está en función de las constantes ciclotómicas (k, h).

Es conveniente, por lo tanto, obtener relaciones que nos permitan de una manera relativamente fácil, encontrar éstas e^2 constantes ciclotómicas.

Para esto introduciremos la siguiente definición:

Sea g una raíz primitiva de un primo p, e un divisor de $p-1$ y $R \neq 1$ una raíz cualquiera de $x^p - 1 = 0$.

DEFINICION: A las sumas

$$(6) \qquad \eta_k = \sum_{t=0}^{f-1} R^{g^{et+k}} \qquad (k = 0, 1, \ldots, e-1)$$

se les llama <u>períodos</u>.

<u>Ejemplo</u>: $p = 5$, $e = 2$; $f = 2$; $g = 3$

$$\eta_0 = \sum_{t=0}^{1} R^{g^{et}} \qquad \eta_1 = \sum_{t=0}^{1} R^{g^{et+1}}$$

$$\eta_0 = R + R^9 = R + R^4 \qquad \eta_1 = R^3 + R^{27} = R^3 + R^2$$

Los períodos son: $\eta_0 = R + R^4$ y $\eta_1 = R^3 + R^2$.

Ahora, consideremos $\eta_0 \eta_k$:

$$\eta_0 \eta_k = \sum_{s=0}^{f-1} R^{g^{es}} \sum_{t=0}^{f-1} R^{g^{et+k}} = \sum_{s=0}^{f-1} \sum_{t=0}^{f-1} R^{g^{es}(1+g^{e(t-s)+k})}$$

Para una s fija podemos sustituir t por $t+s$, donde t varía entre $0, 1, \ldots, f-1$ (i.e. t corre sobre un sistema completo de residuos módulo f).

$$(7) \qquad \eta_0 \eta_k = \sum_{s=0}^{f-1} \sum_{t=0}^{f-1} R^{g^{es}} N \quad \text{donde} \quad N = 1 + g^{et+k}$$

1o./ Sea $N \equiv 0 \pmod{p}$.

Se tiene que $0 \leq et + k \leq e(f-1)$ $e-1 = ef - 1 = p - 2$

$$0 \leq et + k \leq p-2$$

Si $et + k < \frac{1}{2}(p-1)$ entonces $2(et+k) < p-1$

$g^{2(et+k)} \equiv 1 \pmod{p}$ ya que $g^{et+k} \equiv -1 \pmod{p}$

$\Rightarrow$ $\operatorname{ord}_p g = p-1 \leq 2(et+k)$ que es una contradicción

$\therefore$ $et + k \geq \frac{1}{2}(p-1)$.

Si $et+k > \frac{1}{2}(p-1)$ entonces

$$\frac{1}{2}(p-1) < et+k < p-1$$

$$p-1 < 2(et+k) < 2(p-1)$$

$$0 < 2(et+k)-(p-1) < p-1$$

Pero $g^{2(et+k)-(p-1)} \equiv g^{2(et+k)}\, g^{-(p-1)} \equiv 1 \pmod{p}$

$\Rightarrow \operatorname{ord}_p g = p-1 < 2(et+k) - (p-1)$

lo cual es imposible.

$\therefore$ $et+k = \frac{1}{2}(p-1)$.

Si f es par, se tiene

$et+k = f/2\ e \Rightarrow e \mid k \Rightarrow k = 0 \Rightarrow t = f/2$.

Si f es impar, se tiene

$et+k = e/2\ f \Rightarrow e/2 \mid k \Rightarrow k = e/2 \Rightarrow t = 1/2(f-1)$.

DEFINICION:

$$(8) \qquad \begin{cases} s_k = 1 \quad \text{si} \quad f \text{ es par y } k = 0 \text{ ó si } f \text{ es impar y } k = e/2 \\ s_k = 0 \quad \text{en los casos restantes.} \end{cases}$$

Por lo tanto, $N \equiv 0 \pmod{p}$ es válida para exactamente s_k valores de t, y la correspondiente parte de (7) es fs_k.

2o./ Sea $N \not\equiv 0 \pmod{p}$. Por (3), en el capítulo I

$$N = 1 + g^{et+k} \equiv g^{ez+h} \qquad (0 \leq h \leq e-1,\ 0 \leq z \leq f-1)$$

Si t y z son valores fijos que satisfacen (3), la correspondiente parte de (7) es:

$$\sum_{s=0}^{f-1} R^{g^{es}} N = \sum_{s=0}^{f-1} R^{g^{es} g^{ez+h}} = \sum_{s=0}^{f-1} R^{g^{e(s+z)+h}} = \sum_{s=0}^{f-1} R^{g^{es+h}} = \eta_h$$

$$(9) \quad \therefore \eta_0 \eta_k = \sum_{h=0}^{e-1} (k,h) \eta_h + f s_k \qquad (k = 0, \ldots, e-1)$$

Ahora, reemplacemos R por R^{g^m}. Entonces η_k se convierte en η_{k+m}, en el cual debemos reducir el índice de η módulo e.

$$\therefore \quad (10) \quad \eta_m \eta_{m+k} = \sum_{h=0}^{e-1} (k,h) \eta_{m+h} + f s_k .$$

La ecuación Período.

Los e períodos (6) contienen sin repetición a $R, R^2, \ldots, R^{p-1}$

$$R + R^2 + \ldots + R^{p-1} = -1$$

$$\therefore \quad 1 + \eta_0 + \eta_1 + \ldots + \eta_{e-1} = 0$$

Por (9)

$$\eta_0\eta_1 = (1,0)\eta_0 + fs_1 + (1,1)\eta_1 + \ldots + (1,e-1)\eta_{e-1}$$

$$\eta_0\eta_2 = (2,0)\eta_0 + fs_2 + (2,1)\eta_1 + \ldots + (2,e-1)\eta_{e-1}$$

$$\eta_0\eta_{e-1} = (e-1,0)\eta_0 + fs_{e-1} + (e-1,1)\eta_1 + \ldots + (e-1,e-1)\eta_{e-1}$$

Tenemos el siguiente sistema de ecuaciones lineales homogéneas en $1, \eta_1, \ldots, \eta_{e-1}$. (Se toma η_0 como constante).

$$1 + \eta_0 + \eta_1 + \ldots + \eta_{e-1} = 0$$

$$(1,0)\eta_0 + fs_1 + \left[(1,1) - \eta_0\right]\eta_1 + \ldots + (1,e-1)\eta_{e-1} = 0$$

$$(e-1,0)\eta_0 + fs_{e-1} + (e-1,1)\eta_1 + \ldots + \left[(e-1,e-1) - \eta_0\right]\eta_{e-1} = 0$$

$$(11) \qquad \begin{vmatrix} 1+\eta_0 & 1 & \cdots & 1 \\ (1,0)\eta_0 + fs_1 & (1,1)-\eta_0 & \cdots & (1,e-1)\eta_{e-1} \\ \cdots & \cdots & \cdots & \cdots \\ (e-1,0)\eta_0 + fs_{e-1} & (e-1,1)\eta_1 & \cdots & (e-1,e-1)-\eta_0 \end{vmatrix} = 0$$

es la ecuación período que satisface cada η_k $(k = 0, \ldots, e-1)$.

Congruencias auxiliares.

DEFINICION: denotaremos por $\{k,h\}$ al número de conjuntos de valores t y z escogidos de $0,1,\ldots,f-1$ que satisfacen

$$(12) \qquad 1+g^{et+k}+g^{ez+h}\equiv 0 \pmod{p}$$

$\{k,h\} = \{h,k\}$ no se altera si incrementamos h y k por múltiplos de e.

Otra propiedad es que $\{-k,h-k\} = \{k,h\}$ porque multiplicando (12) por g^{-et-k} se tiene

$$g^{-et-k}+1+g^{e(z-t)+(h-k)}\equiv 0 \pmod{p}$$

y como $-t$ y $z-t$ determinan únicamente a t y z (mod. f) entonces $\{-k,\ h-k\} = \{k,h\}$ - (13).

Ahora procederemos a expresar $\{k,h\}$ en términos de (i,j)

lo./ Sea f par.

$$p-1 = ef = 2ef/2\,, \qquad \frac{p-1}{2} = e\,f/2$$

$$g^{e\,f/2}\equiv -1 \pmod{p}$$

$$1+g^{et+k}\equiv -g^{ez+h}\equiv g^{e(z+f/2)+h} \pmod{p}$$

$$(14) \qquad \{k,h\} = (k,h) \quad si \quad f \quad es\ par.$$

Una consecuencia inmediata es que para f par $(k,h) = (h,k)$.

2o./ Sea f impar.

$$1 + g^{et+k} \equiv -g^{ez+h} \equiv g^{e/2\, f}\, g^{ez+h} = g^{e(z+1/2(f-1))+(h+1/2\,e)} \pmod{p}$$

(15) $\quad \{k,h\} = (k, h+\tfrac{1}{2}e)$ si f es impar.

De $\{k,h\} = \{h,k\}$, (13),(14) y (15) deducimos que

(16) $\quad (k,h) = (h,k)$, $(e-k,\ h-k) = (k,h)$ si f es par

(17) $\quad (k,h) = (h+\tfrac{1}{2}e,\ k+\tfrac{1}{2}e)$, $(e-k,\ h-k) = (k,h)$ si f es impar

Para (16) tenemos:

$$(k,h) = \{k,h\} = \{-k, h-k\} = (-k,\ h-k) = (e-k,\ h-k)$$

y para (17) tenemos:

$$(k,h) = \{k, h-\tfrac{1}{2}e\} = \{k, h+\tfrac{1}{2}e\} = \{h+\tfrac{1}{2}e,\ k\} = (h+\tfrac{1}{2}e,\ k+\tfrac{1}{2}e)$$

$$(e-k,\ h-k) = (-k,\ h-k) = \{-k,\ h-k-\tfrac{1}{2}e\} = \{k, h-\tfrac{1}{2}e\} = (k,h)$$

Por (14) y (15), los sistemas (16) y (17) son permutados cuando (k,h) corresponde a $(k, h+\tfrac{1}{2}e)$ — (18).

Relaciones lineales.

La suma (7) contiene f^2 potencias de R.

En (9) el número de potencias de R (incluyendo a 1) es

$$\sum_{h=0}^{e-1} (k,h)\, f + f\, s_k$$

$$\therefore \quad \sum_{h=0}^{e-1} (k,h) f + f\, s_k = f^2 .$$

$$(19) \qquad \sum_{h=0}^{e-1} (k,h) = f - s_k$$

Caso e = 2.

$p = 2f+1$

Por (19) tenemos $\sum_{h=0}^{1} (k,h) = f - s_k \qquad k = 0,1$

Si f es par

$$(0,0) + (0,1) = f-1 , \quad (1,0) + (1,1) = f$$

(20)

$$(1,1) = (1,0) = (0,1) = f/2 , \quad (0,0) = 1/2\, f-1 \text{ por (14) y (15).}$$

Si f es impar

$$(0,0)+(0,1)=f\ ,\qquad (1,0)+(1,1)=f-1$$

(21)

$$(0,0)=(1,1)=(1,0)=1/2(f-1),\quad (0,1)=1/2(f+1)$$

por (14) y (15).

Entonces para cada f, las (i, j) están determinadas por $p=2f+1$.

La ecuación período (11) es:

$$\begin{vmatrix} 1+\eta_0 & 1 \\ fs_1+(1,0) & (1,1)-\eta_0 \end{vmatrix} = 0$$

$$(1+\eta_0)\left[(1,1)-\eta_0\right]-\left[fs_1+(1,0)\eta_0\right]=0$$

$$(1,1)-\eta_0+(1,1)\eta_0-\eta_0^2-fs_1-(1,0)\eta_0=0$$

Pero $(1,1)=(1,0)$ (en ambos casos: f par e impar).

$$\eta_0^2+\eta_0+fs_1+(1,1)=0$$

$$\eta^2+\eta+c=0 \quad \text{donde} \quad c=fs_1-(1,1)$$

$c=-1/4\,(p-1)$ si f es par y $c=1/4\,(p+1)$ si f es impar.

Cuando $e\geq 3$, (16) – (19) no determinan las constantes ciclotómicas (k, h), pero pueden ser suplementadas por relaciones obtenidas por

la siguiente teoría avanzada:

Por (10) $$\eta_j \eta_{j+k} = \sum_{h=0}^{e-1} (k,h) \eta_{j+h} + f s_k$$

$$\sum_{j=0}^{e-1} \eta_j \eta_{j+k} = \sum_{j=0}^{e-1} \sum_{h=0}^{e-1} (k,h) \eta_{j+h} + ef\, s_k$$

Para una h fija podemos reemplazar j por $j-h$. Por (17) y utilizando que $1 + \eta_0 + \ldots + \eta_{e-1} = 0$ tenemos:

$$\sum_j \left[\sum_h (k,h)\right] \eta_j = \sum_j (f-s_k) \eta_j = (f-s_k) \sum_j \eta_j = -(f-s_k)$$

$$\therefore\ ef\, s_k - f + s_k = (ef+1) s_k - f = p\, s_k - f$$

(22) $$\sum_{j=0}^{e-1} \eta_j \eta_{j+k} = p\, s_k - f \qquad (k = 0, 1, \ldots, f-1)$$

CAPITULO III

Caso e = 3

Funciones de Jacobi.

Sea $\alpha \neq 1$ cualquier raíz de $x^{p-1} = 1$, $p = ef+1$. Sea

$$F(\alpha) = \sum_{k=0}^{p-2} \alpha^k R^{g^k} \tag{23}$$

Sea β una raíz primitiva de $x^e = 1$.

Consideremos en (23) $\alpha = \beta^m$ y $k = et + j$ y de la definición de período η_k tenemos:

$$F(\beta^m) = \sum_{k=0}^{p-2} \beta^{mk} R^{g^k} = \sum_{j=0}^{e-1} \sum_{t=0}^{f-1} \beta^{m(et+j)} R^{g^{(et+j)}} = \sum_{j=0}^{e-1} \beta^{mj} \sum_{t=0}^{f-1} R^{g^{(et+j)}} =$$

$$= \sum_{j=0}^{e-1} \beta^{mj} \eta_j$$

$$F(\beta^m) = \sum_{j=0}^{e-1} \beta^{mj} \eta_j \tag{24}$$

Consideremos el producto $F(\beta^m)\, F(\beta^n)$

$$F(\beta^m)\, F(\beta^n) = \sum_{j=0}^{e-1} \beta^{mj} \eta_j \sum_{t=0}^{e-1} \beta^{nt} \eta_t$$

tomando $t = j + k$ donde k corre sobre un sistema completo de residuos módulo e, tenemos:

$$F(\beta^m)F(\beta^n) = \sum_{j=0}^{e-1} \beta^{mj} \eta_j \sum_{k=0}^{e-1} \beta^{n(j+k)} \eta_{j+k} =$$

$$= \sum_{k=0}^{e-1} \sum_{j=0}^{e-1} \beta^{mj} \beta^{n(j+k)} \eta_j \eta_{j+k} = \sum_{k=0}^{e-1} \sum_{j=0}^{e-1} \beta^{(m+n)j} \beta^{nk} \eta_j \eta_{j+k} =$$

$$= \sum_{k=0}^{e-1} \beta^{nk} M_k$$

$$M_k = \sum_{j=0}^{e-1} \beta^{(m+n)j} \eta_j \eta_{j+k}$$

$$F(\beta^m) F(\beta^n) = \sum_{k=0}^{e-1} \beta^{nk} M_k \tag{25}$$

lo. / Sea $m = -n$, donde n no es un múltiplo de e.

Entonces $M_k = \sum_{j=0}^{e-1} \eta_j \eta_{j+k} = p s_k = f$

$$\sum_{k=0}^{e-1} \beta^{nk} = 0 \tag{26}$$

Recordando la definición de s_k y notando que si f es impar entonces e es par y $\beta^{e/2} = -1$.

$$F(\beta^n)F(\beta^{-n}) = \sum_{k=0}^{e-1} \beta^{nk} M_k = \sum_{k=0}^{e-1} \beta^{nk}(p s_k - f) = \sum_{k=0}^{e-1} \beta^{nk} p s_k - f \sum_{k=0}^{e-1} \beta^{nk}$$

$$= p \sum_{k=0}^{e-1} \beta^{nk} s_k = (-1)^{nf} p$$

(27) $\qquad F(\beta^n)F(\beta^{-n}) = (-1)^{nf} p$, $\quad n$ no divisible por e.

2o./ Sean n, m y $m+n$ no divisibles por e

Sea $\quad N_k = \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} (k,h) \eta_{j+h}$

Por (10) con m reemplazada por j y (26)

$$M_k - N_k = \sum_{j=0}^{e-1} \beta^{(m+n)j} \eta_j \eta_{j+k} - \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} (k,h) \eta_{j+h}$$

$$= \sum_{j=0}^{e-1} \beta^{(m+n)j} \left(\sum_{h=0}^{e-1} (k,h) \eta_{j+h} + f s_k\right) - \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} (k,h) \eta_{j+h}$$

$$= \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} (k,h) \eta_{j+h} \sum_{j=0}^{e-1} \beta^{(m+n)j} f s_k - \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} (k,h) \eta_{j+h}$$

$$= f s_k \sum_{j=0}^{e-1} \beta^{(m+n)j} = 0$$

$$\therefore \quad M_k = N_k$$

N_k es el producto de

$$F(\beta^{m+n}) = \sum_{j=0}^{e-1} \beta^{(m+n)j+h} \eta_{j+h} \quad y \quad \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k,h) = \Omega$$

$$\frac{F(\beta^m)\,F(\beta^n)}{F(\beta^{m+n})} = \frac{\sum_{k=0}^{e-1} \beta^{nk} M_k}{F(\beta^{m+n})} = \frac{\sum_{k=0}^{e-1} \beta^{nk}(F(\beta^{m+n}) \cdot \Omega)}{F(\beta^{m+n})}$$

$$= \frac{F(\beta^{m+n}) \sum_{k=0}^{e-1} \beta^{nk} \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k,h)}{F(\beta^{m+n})}$$

$$= \sum_{k=0}^{e-1} \beta^{nk} \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k,h) \equiv R(m,n)$$

$$(28) \qquad \frac{F(\beta^m)F(\beta^n)}{F(\beta^{m+n})} = \sum_{k=0}^{e-1} \beta^{nk} \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k,h) \equiv R(m,n)$$

Ahora, trataremos de encontrar el camino más corto para la obtención de $R(m,n)$.

Por (16) y (17) de la segunda relación tenemos:

$$(e-j,h) = (j, j+h)$$

La parte de (28) dada por $k = e-j$ con $j \geq 1$ es

$$\beta^{n(e-j)} \sum_{h=0}^{e-1} \beta^{-(m \quad n)h} (j, j+h)$$

Reemplazando el índice h por $h-j$ obtenemos

$$\beta^{n(e-j)} \sum_{h=0}^{e-1} \beta^{-(m+n)(h-j)} (j, h+h) = \beta^{ne} \beta^{-nj} \sum_{h=0}^{e-1} \beta^{-(m \quad n)h} \beta^{(m+n)j} (j, j+h-j)$$

$$= \beta^{mj} \sum_{h=0}^{e-1} \beta^{-(m+n)h} (j, h)$$

Ahora, si $j < e/2$ debemos combinar esto con el nuevo término de R, dado por $k = j$.

Sea $E = e/2$ si e es par, $E = 1/2\,(e-1)$ si e es impar.

Entonces

$$(29)\quad R(m, n) = \sum_{j=1}^{E} (\beta^{mj} + \beta^{nj}) \sum_{h=0}^{e-1} \beta^{-(m+n)h} (j, h) + \sum_{h=0}^{e-1} \beta^{-(m+n)h} (0, h) \quad \text{si e es impar.}$$

Pero para e par, (29) es vália si reemplazamos en el término dado por $j=E$, $\beta^{mj} + \beta^{nj}$ por β^{mE} si $m \equiv n \pmod 2$ y por cero si $m \not\equiv n \pmod 2$.

Por (27) y (28) tenemos:

$$R(m,n) = \frac{F(\beta^m)\,F(\beta^n)}{F(\beta^{m+n})}, \qquad R(-m,-n) = \frac{F(\beta^{-m})\,F(\beta^{-n})}{F(\beta^{-(m+n)})}$$

donde $R(-m,-n)$ se deduce de $R(m,n)$ reemplazando β por β^{-1}

$$R(m,n)\,R(-m,-n) = \frac{F(\beta^m)\,F(\beta^n)\,F(\beta^{-m})\,F(\beta^{-n})}{F(\beta^{m+n})\,F(\beta^{-(m+n)})} = \frac{(-1)^{mf}\,p\,(-1)^{nf}\,p}{(-1)^{m+n}\,p} = p$$

(30) $R(m,n)\,R(-m,-n) = p$ si m, n y $m+n$ no son divisibles por p.

Caso $e = 3$

$p = 3f+1$ y f tiene que ser par.

Por (16)

(31) $(1,0) = (0,1) = (2,2)$, $(1,1) = (0,2) = (2,0)$ y $(2,1) = (1,2)$

Entonces las 9 (i,j) se reducen a $(0,0)$, $(0,1)$, $(0,2)$, $(1,2)$

Por (19) y (29)

$(0,0)+(0,1)+(0,2) = f-1$ $\qquad$ $(1,0)+(1,1)+(1,2) = f$

(32) $(0,0)+(0,1)+(0,2) = f-1$, $\qquad$ $(0,1)+(0,2)+(1,2) = f$

β una raiz cúbica de 1.

$$\beta^3 = 1, \quad \beta^2 = \beta^{-1}, \quad \beta = \beta^{-2}, \quad 1+\beta+\beta^2 = 0$$

Por (29) para e impar

$$R(1,1) = \sum_{j=1}^{1} (\beta^j + \beta^j) \sum_{h=0}^{2} \beta^{-2h}\,(j,h) + \sum_{h=0}^{2} \beta^{-2h}\,(0,h)$$

$$R(1,1) = 2\beta \sum_{h=0}^{2} \beta^{-2h}(1,h) + \sum_{h=0}^{2} \beta^{-2h}(0,h)$$

$$R(1,1) = 2\beta\left[(1,0) + \beta^{-2}(1,1) + \beta^{-4}(1,2)\right] + (0,0) + \beta^{-2}(0,1) + \beta^{-4}(0,2)$$

$$= 2\beta(1,0) + 2\beta^{-1}(1,1) + 2\beta^{-3}(1,2) + (0,0) + \beta(0,1) + \beta^{2}(0,2)$$

$$= 2\beta(1,0) + 1\beta^{2}(1,1) + 2(1,2) + (0,0) + \beta(0,1) + \beta^{2}(0,2)$$

$$= 2\beta(0,1) + 2\beta^{2}(1,1) + 2(1,1) + (0,0) + \beta(0,1) + \beta^{2}(0,2)$$

$$= 3\beta(0,1) + (0,0) + 2(1,2) + \beta^{2}(2(1,1) + (0,2))$$

$$= 3\beta(0,1) + (0,0) + 2(1,2) + (-1-\beta)(2(1,1) + (0,2))$$

$$= 3\beta(0,1) + (0,0) + 2(1,2) - (1+\beta)(3(0,2))$$

$$= 3\beta(0,1) + (0,0) + 2(1,2) - 3(0,2) - 3\beta(0,2)$$

$$= (0,0) + 2(1,2) - 3(0,2) + 3\beta\left[(0,1) - (0,2)\right]$$

$R(1,1) = N + 3\beta M$, $N = (0,0) + 2(1,2) - 3(0,2)$, $M = (0,1) - (0,2)$.

Para encontrar $R(-1,-1)$ basta sustituir β por β^{-1} en $R(1,1)$

$$R(-1,-1) = N + 3\beta^{-1} M = N + 3\beta^{2} M$$

Por (30) se tiene

$$R(1,1)\ R(-1,-1) = p$$

$$\therefore\ 4p = 4(N + 3\beta M)(N + 3\beta^{2} M) = (2N - 3M)^{2} + 27M^{2}$$

De (32) multiplicando la primera ecuación por 2 y la segunda por 5 y restando se tiene

$$2(0,0)+2(0,1)+2(0,2) = 2(f-1)$$

$$-5(0,1)-5(0,2)-5(1,2) = -5f$$

$$2(0,0)-3(0,1)-3(0,2)-5(1,2) = -3f-2 = -(p+1)$$

$$L = 2N-3M = 2(0,0)+4(1,2)-6(0,2)-6(0,2)-3(0,1)+3(0,2)$$

$$= 2(0,0)-3(0,1)-3(0,2)-5(1,2)+9(1,2)$$

$$= -3f-2+9(1,2)$$

$$L = 9(1,2)-(p+1)$$

(33) $4p = L^2+27M^2, \quad L \equiv 1 \pmod 3$

(34) $9(1,2) = p+1+L, \quad 9(0,0) = p-8+L$

La segunda igualdad en (34) se obtiene de la manera siguiente:

Multiplicando las ecuaciones (32) por 9 y restando

$$9(0,0)+9(0,1)+9(0,1) = 9f-9$$

$$-9(0,1)-9(0,2)-9(1,2) = -9f$$

$$9(0,0)-9(1,2) = -9$$

$$9(0,0) = -9+9(1,2) = p+1+L-9 = p-8+L$$

$$\therefore\ 9(0,0) = p-8+L$$

Ahora, en (32) multiplicando la segunda ecuación por 9

$$9(0,1)+9(0,2)+9(1,2) = 9f = 3(p-1)$$

$$9(0,1) = 3(p-1)-9(0,2)-9(1,2)$$

$$18(0,1) = 3p-3+9(0,1)-9(0,2)-9(1,2)$$

$$= 3p-3+9((0,1)-(0,2))-(p\ 1\ L)$$

$$= 3p-3+9M-p-1-L$$

$$18(0,1) = 2p - 4 - L + 9M$$

Analogamente

$$9(0,2) = 3(p-1) - 9(0,1) - 9(1,2)$$

$$18(0,2) = 3(p-1) + 9(0,2) - 9(0,1) - 9(1,2)$$

$$18(0,2) = 2p - 4 - L - 9M$$

Hemos obtenido

(35) $18(0,1) = 2p - 4 - L \quad 9M, \qquad 18(0,2) = 2p - 4 - L - 9M$

De aquí por (31) todas las $9(i,j)$ están expresadas en términos de p, L y M. Por la teoría de formas cuadráticas binarias, L^2 y M^2 están únicamente determinadas por (33). El signo de L ha sido escogido de tal manera que (33) sea válida. Pero el signo de M depende de la raiz primitiva g empleada.

Teorema 5: Si r, s, A son todos primos a $p > 2$

(36) $r x^2 + Sy^2 \equiv A \pmod{p}$

tiene $p - N$ soluciones, donde $N = +1$ si $-rs$ es un residuo cuadrático y $N = -1$ si $-rs$ no es un residuo cuadrático.

Demostración

Puesto que la congruencia no se altera si multiplicamos r, s y A por el mismo entero primo a p, es suficiente probar el teorema para $A = -1$ porque:

Si $\beta \equiv -A^{-1} \pmod{p}$ entonces

$$\beta r x^2 + \beta s y^2 \equiv \beta A \equiv -1 \pmod{p}$$

El número de soluciones de (36) es igual al número de soluciones de esta última congruencia.

$$r x^2 + s y^2 \equiv -1 \pmod{p}$$

$$1 + r x^2 \equiv -s y^2 \equiv t y^2, \qquad -s \equiv t \pmod{p}$$

Por lo tanto basta probar que

(37) $$1 + r x^2 \equiv t y^2 \pmod{p}$$

tiene $p - N$ soluciones, donde $N = 1$ si rt es un residuo cuadrático de p, y $N = -1$ si rt no es un residuo cuadrático de p. Puesto que g no es un residuo cuadrático de p, entonces hay cuatro posibilidades:

1) $r \equiv t \equiv 1$, 2) $r \equiv 1$, $t \equiv g$, 3) $r \equiv g$, $t \equiv 1$, 4) $r \equiv t \equiv g$

porque:

$$r \equiv g^h, \quad t \equiv g^k \qquad 0 \leq h \leq p-2$$

si $h, k > 1$ entonces

i) $h \equiv 2h' + 1$, $k \equiv 2k' + 1$

y (37) es equivalente a

$$1 + g(g^{h'} x)^2 \equiv g\,(g^{k'} y)^2 \pmod{p}$$

ii) $h \equiv 2h'$, $k \equiv 2k'$ y (37) es equivalente a

$$1 + (g^{h'} x)^2 \equiv (g^{k'} y)^2 \pmod{p}$$

iii) $h \equiv 2h'$, $k \equiv 2k+1$ y (37) es equivalente a

$$1 + (g^{h'} x)^2 \equiv g(g^{k'} y)^2 \pmod{p}$$

iv) $h \equiv 2h' + 1$, $k \equiv 2k'$ y (37) es equivalente a

$$1 + g(g^{h'} x)^2 \equiv (g^{k'} y)^2 \pmod{p}$$

Entonces por teorema 2, Capítulo I, con $e \equiv 2$, el número de soluciones cuando f es impar es:

$2 + 4(0, 0)$ si $r \equiv t \equiv 1$

$4(0, 1)$ si $r \equiv 1$, $t \equiv g$

$4 + 4(1, 0)$ si $r \equiv g$, $t \equiv 1$

$2 + 4(1, 1)$ si $r \equiv t \equiv g$

Cuando f es par el número de soluciones es:

$4 + 4(0, 0)$ si $r \equiv t \equiv 1$

$2 + 4(0, 1)$ si $r = 1$, $t = g$

$2 + 4(1, 0)$ si $r = g$, $t = 1$

$4(1, 1)$ si $r = t = g$

Pero por (20) para f par

$$(1, 1) = (1, 0) = (0, 1) = f/2 \qquad (0, 0) = 1/2\, f - 1$$

por (21), par f impar

$$(0, 0) = (1, 1) = (1, 0) = 1/2(f - 1) \qquad (0, 1) = 1/2(f + 1)$$

Entonces el número de soluciones de (37) es

f impar

$2 + 4(1/2(f - 1)) = p - 1$ si $r = t = 1$

$4(1/2(f \quad 1)) = p + 1$ si $r = 1$, $t = g$

$4 + 4(1/2(f - 1)) = p + 1$ si $r = g$, $t = 1$

$2 + 4(1/2(f - 1)) = p - 1$ si $r = t = g$

f par

$4 + 4(1/2\, f - 1) = f - 1$ si $r = t = 1$

$2 + 4(1/2\, f) = p + 1$ si $r = 1$, $t = 1$

$2 + 4(1/2\, f) = p + 1$ si $r = g$, $t = 1$

$4(1/2\, f) = p - 1$ si $r = t = g$

$r = t = 1$ ó $r = t = g$ $\quad rt$ es un residuo cuadrático de p.

$r = g,\ t = 1,\ r = 1,\ t = g$ $\quad rt$ no es un residuo cuadrático de p.

$\therefore$ (37) tiene $p - 1$ soluciones si rt es un residuo cuadrático de p y $p+1$ soluciones si rt no es un residuo cuadrático de p.

Teorema 6: La congruencia

(38) $\quad x^3 + y^3 \equiv 1 \pmod{p}$

tiene $p = 2 + L$ soluciones. 2 es un residuo cúbico de $p \Leftrightarrow L$ es par y entonces $p = t^2 + 27\,m^2$ tiene solución.

Demostración

En el capítulo III vimos que $L = 9(1, 2) - (p+1)$ y $9(0, 0) = p - 8 + L$

$\therefore$ (38) tiene $p - 8 + L$ soluciones primas a p.

Ahora, en caso de que 2 sea un residuo cúbico de p, la ecuación $2y^3 \equiv 1 \pmod{p}$ tiene 3 soluciones puesto que $x^3 \equiv 2 \pmod{p}$ tiene solución y entonces

$(xy)^3 \equiv 1 \pmod{p}$ tiene 3 soluciones

$\therefore$ (38) tiene 9 soluciones con $x^3 \equiv y^3 \pmod{p}$.

Las soluciones primas a p con $x^3 \not\equiv y^3 \pmod{p}$ caen en conjuntos de $2 \times 3 \times 3$ elementos (se toman en cuenta también las soluciones permutadas).

$\therefore \quad p = 8 + L \equiv 9 \pmod{18}$ y L es par.

Si 2 no es un residuo cúbico de p,

$p = 8 + L \equiv 0 \pmod{18}$ y L es impar

Además (38) tiene 6 soluciones con $x \equiv 0$ ó $y \equiv 0 \pmod{p}$

$\therefore$ (38) tiene $p = 2 + L$ soluciones.

Se vió en el capítulo III, para $e = 3$ que

$$4p = L^2 + 27 M^2$$

$4 \mid L^2 + 27 M^2$ y como $4 \mid L^2$

entonces $2 \mid M$

$$\therefore \quad p = \left(\frac{L}{2}\right)^2 + 27 \left(\frac{M}{2}\right)^2$$

$\therefore \quad p = t^2 + 27 m^2$ tiene solución.

CAPITULO IV

Caso e = 4

$$p = 4f + 1, \quad \beta^4 = 1, \quad \beta^2 = -1, \quad \beta^3 = -\beta, \quad \beta^6 = \beta^2 = -1$$

Por (29)

$$R(m,n) = \sum_{j=1}^{E} (\beta^{mj} + \beta^{nj}) \sum_{h=0}^{e-1} \beta^{-(m+n)h} (j,h) + \sum_{h=0}^{e-1} \beta^{-(m\ \ n)h} (0,h), \quad E = e/2$$

$$R(1,1) = \sum_{j=1}^{2} (\beta^j + \beta^j) \sum_{h=0}^{3} \beta^{-2h} (j,h) + \sum_{h=0}^{3} \beta^{-2h} (0,h)$$

$$R(1,1) = 2\beta \left[(1,0) + \beta^{-2} (1,1) + \beta^{-4} (1,2) + \beta^{-6} (1,3) \right]$$

$$+ \beta^2 \left[(2,0) + \beta^{-2} (2,1) + \beta^{-4} (2,2) + \beta^{-6} (2,3) \right]$$

$$+ (0,0) + \beta^{-2} (0,1) + \beta^{-4} (0,2) + \beta^{-6} (0,3)$$

$$R(1,1) = (0,0) - (0,1) + (0,2) - (0,3) \quad - (2,0) + (2,1) - (2,2) + (2,3)$$

$$+ 2\beta \left[(1,0) - (1,1) + (1,2) - (1,3) \right]$$

Para f par:

$$(h,k) = (k,h) \qquad y \qquad (e-k,\ h-k) = (k,\ h)$$

$$(1,3) = (1,2) = (2,1) = (2,3) = (1,3) = (0,3) = (1,1)$$

$$(1,0) = (0,1) \tag{39}$$

$$(2,2) = (0,2) = (2,0)$$

Por (19)

$$L_1 : (0,0) + (0,1) + (0,2) + (0,3) = f - 1$$

$$L_2 : (0,1) + (0,2) + 2(1,2) = f \tag{40}$$

$$L_3 : (0,2) + (1,2) = 1/2\, f$$

$$L_1 - L_2 - L_3 : (0,0) + (0,1) + (0,2) + (0,3) - (0,1) - (0,3) - 2(1,2) - (0,2) - (1,2) = -1/2\, f - 1$$

$$3(1,2) = (0,0) + 1/2\, f + 1$$

$$L_1 - 2L_2 - 2L_3 : (0,0) + (0,1) + (0,2) + (0,3) - 2(0,1) - 2(0,3) - 4(1,2) - 2(0,2) - 2(1,2) = -2f - 1$$

$$(0,0) - (0,1) - (0,2) - (0,3) - 6(1,2) = -2f - 1$$

$$R(1,1) = (0,0) - (0,1) + (0,2) - (0,3) - (2,0) + (2,1) - (2,2) + (2,3) + 2\beta\left[(1,0) - (1,1) + (1,2) - (1,3)\right]$$

$$= (0,0) - (0,1) - (0,2) - (0,2) + 2(1,2) + 2\beta\left[(1,0) - (0,3)\right]$$

$$R(1,1) = -x + 2\beta y, \quad x = 2f + 1 - 8(1,2), \quad y = (0,1) - (0,3) \tag{41}$$

$$R(-1,-1) = -x - 2\beta y$$

y por (30)

$$R(1,1)\, R(-1,-1) = p$$

$$\therefore \quad p = x^2 + 4y^2, \qquad x \equiv 1 \pmod 4 \qquad (42)$$

Aquí, x solo tiene un valor, que está determinado por la congruencia de la derecha de (42), pero y puede tener dos valores, que dependen del cambio de la raíz primitiva g.

Ahora tenemos:

$$2(0,0) = -f - 2 + 2(0,0) + f + 2$$

$$2(0,0) = -f - 2 + 6(1,2)$$

$$16(0,0) = -8f - 16 + 48(1,2) = 4f + 1 - 12f - 15 + 48(1,2)$$

$$16(0,0) = p - 11 - 12f - 4 + 48(1,2) = p - 11 - 6(2f + 1 - 8(1,2))$$

$$16(0,0) = p - 11 - 6x$$

Por L_2 tenemos

$$(0,1) + (0,3) + 2(1,2) = f$$

$$(0,1) = f - 2(1,2) - (0,3)$$

$$= 2\,(1/2\,f - (1,2)) - (0,3)$$

$$= 2(0,2) - (0,3)$$

$$2(0,1) = 2(0,2) + (0,1) - (0,3)$$

$$16(0,1) = 16(0,2) + 8((0,1) - (0,3))$$

$$16(0,1) = h + 8y, \qquad h = 16(0,2)$$

$$(0,3) = f - 2(1,2) - (0,1)$$

$2(0,3) = 2(0,2) - (0,1) + (0,3) = 2(0,2) - ((0,1) - (0,3))$

$16(0,3) = 16(0,2) - 8((0,1) - (0,3))$

$16(0,3) = h - 8y$

$16(1,2) = 16(1,2) + 4f + 2 - 4f - 2 = p + 1 - 2(2f + 2 - 8(1,2))$

$16(1,2) = p + 1 - 2x$

Por L_3 tenemos:

$(0,2) = 1/2\,f - (1,2)$

$16(0,2) = 8f - 16(1,2) + 4f + 2 + 4f - 2 = 4f - 2 + 2(2f + 1 - 8(1,2))$

$16(0,2) = p - 3 + 2x$

$\therefore\ h = p - 3 + 2x$

Por lo tanto tenemos:

$$\begin{aligned} 16(0,0) &= p - 11 - 6x \\ 16(0,1) &= p - 3 + 2x + 8y \\ 16(0,2) &= p - 3 + 2x \qquad (43) \\ 16(0,3) &= p - 3 + 2x - 8y \\ 16(1,2) &= p + 1 - 2x \end{aligned}$$

Para f impar:

Por (17) tenemos:

$$(k,h) = (h + 1/2\,e,\ k + 1/2\,e), \qquad (k,h) = (e - k,\ h - k)$$

$$\begin{aligned} (0,0) &= (2,2) = (2,0) \\ (0,1) &= (1,3) \\ (0,3) &= (1,2) \\ (1,0) &= (2,3) = (2,1) = (1,1) \end{aligned} \tag{44}$$

De (19) se obtienen las siguientes expresiones:

$$\begin{aligned} L_1' &: \quad (0,0) + (0,1) + (0,2) + (0,3) = f \\ L_2' &: \quad (0,1) + (0,3) + 2(1,0) = f \\ L_3' &: \quad (0,0) + (1,0) = 1/2(f - 1) \end{aligned} \tag{45}$$

$$R(1,1) = (0,0) - (0,1)\ \ (0,2) - (0,3) - (2,0) + (2,1) - (2,2) + (2,3)$$
$$+ 2\,\beta\,\big[\,(1,0) - (1,1) + (1,2) - (1,3)\big]$$

$$R(1,1) = -(0,0) - (0,1) + (0,2) - (0,3) + 2(1,0) + 2\,\beta\,\big[(0,3) - (0,1)\big]$$
$$-L_1' + 2\,L_2' + 2\,L_3' :$$

$$-(0,0) - (0,1) - (0,2) - (0,3) + 2(0,1) + 2(0,3) + 4(1,0) + 2(0,0) + 2(1,0) =$$
$$-f + 2f + f - 1$$

$$(0,0) + (0,1) - (0,2) + (0,3) + 6(1,0) = 2f - 1$$

$$(0,0) + (0,1) - (0,2) + (0,3) - 2(1,0) = 2f - 1 - 8(1,0)$$

$$R(1,1) = -x + 2\,\beta\,y, \qquad x = 2f - 1 - 8(1,0), \qquad y = (0,3) - (0,1) \tag{46}$$

Entonces (42) es válida, es decir:

$$p = x^2 + 4y^2, \quad x \equiv 1 \pmod 4$$

Todas las (i, j) están determinadas y están dadas en términos de p, x y y.

$$(0,2) = f - (0,3) - (0,0) - (0,1)$$

$$(0,2) = f - f + 2(1,0) - (0,0)$$

$$= 2(1,0) - (0,0) = 3(1,0) - (1,0) - (0,0) = 3(1,0) - 1/2(f - 1)$$

$$16(0,2) = 48(1,0) - 8f + 8 = 4f + 2 - 12f + 6 + 48(1,0)$$

$$= p + 1 - 6(2f - 1 - 8(1,0))$$

$$16(0,2) = p + 1 - 6x$$

$$2(0,0) = f - 1 - 2(1,0)$$

$$16(0,0) = 8f - 8 - 16(1,0) = 2(2f - 1 - 8(1,0)) + 4f - 6 = 2x + p - 7$$

$$16(0,0) = p - 7 + 2x$$

$$2(1,0) = f - 1 - 2(0,0)$$

$$16(1,0) = 8f - 8 - 16(0,0) = 8f - 8 - (p - 7 + 2x)$$

$$= 2(p - 5) - p + 7 - 2x$$

$$= p - 3 - 2x$$

$$16(1,0) = p - 3 - 2x$$

$$(0,1) = f - (0,3) - 2(1,0)$$

$$2(0,1) = f - (0,3) + (0,1) - 2(1,0)$$

$$16(0,1) = 8f - 8y - 16(1,0) = 2p - 2 - p + 3 + 2x - 8y$$

$$16(0,1) = p + 1 + 2x - 8y$$

$$2(0,3) = f - (0,1) + (0,3) - 2(1,0)$$

$$16(0,3) = 8f - 16(1,0) + 8y$$

$$16(0,3) = 8f - 16(1,0) + 8y$$

$$16(0,3) = p + 1 + 2x + 8y$$

$$\begin{aligned} 16(0,0) &= p - 7 + 2x \\ 16(0,1) &= p + 1 + 2x - 8y \qquad (47) \\ 16(0,2) &= p + 1 - 6x \\ 16(0,3) &= p + 1 + 2x + 8y \end{aligned}$$

CAPITULO V

Caso e = 5

$p = 5f+1$ y f par.

Por (16) se tiene:

$$(k,h) = (h,k) \quad y \quad (e-k,\ h-k) = (k,h)$$

$$\begin{aligned}
&(0,1) = (1,0) = (4,4)\\
&(0,2) = (2,0) = (3,3)\\
&(0,3) = (2,2) = (3,0)\\
&(0,4) = (1,1) = (4,0)\\
&(1,2) = (2,1) = (1,4) = (3,4) = (4,3) = (4,1)\\
&(1,3) = (2,3) = (2,4) = (3,2) = (3,1) = (4,2)
\end{aligned} \tag{48}$$

Entonces las 25 (i, j) se reducen a:

$$(0,0),\ (0,1),\ (0,2),\ (0,3),\ (0,4),\ (1,2),\ (1,3)$$

De (19) tenemos:

$$\begin{aligned}
&(0,0)+(0,1)+(0,2)+(0,3)+(0,4) = f-1\\
&(0,1)+(0,4)+2(1,2)+(1,3) = f\\
&(0,2)+(0,3)+(1,2)+2(1,3) = f
\end{aligned} \tag{49}$$

Si β es una raiz quinta primitiva de la unidad entonces

(50) $\qquad \beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$

Por (29) se tiene

$$R(i,1) = \sum_{j=1}^{2} 2\beta^j \sum_{h=0}^{4} \beta^{-2h}(j,h) + \sum_{h=0}^{4} \beta^{-2h}(0,h)$$

$$R(1,1) = 2\beta\left[(1,0) + \beta^{-2}(1,1) + \beta^{-4}(1,2) + \beta^{-6}(1,3) + \beta^{-8}(1,4)\right]$$
$$+2\beta^2\left[(2,0) + \beta^{-2}(2,1) + \beta^{-4}(2,2) + \beta^{-6}(2,3) + \beta^{-8}(2,4)\right]$$
$$+(0,0) + \beta^{-2}(0,1) + \beta^{-4}(0,2) + \beta^{-6}(0,3) + \beta^{-8}(0,4)$$
$$= 2\beta(1,0) + 2\beta^4(1,1) + 2\beta^2(1,2) - 2(1,3)(\beta + \beta^2 + \beta^3 + \beta^4)$$
$$2\beta^3(1,4) + 2\beta^2(2,4) - 2(2,1)(\beta + \beta^2 + \beta^3 + \beta^4) +$$
$$2\beta^3(2,2) + 2\beta(2,3) + 2\beta^4(2,4) - (0,0)(\beta + \beta^2 + \beta^3 + \beta^4)$$
$$+\beta^3(0,1) + \beta(0,2) + \beta^4(0,3) + \beta^2(0,4)$$

$$R(1,1) = a_1\beta + a_2\beta^2 + a_3\beta^3 + a_4\beta^4$$

$$a_1 = (0,2) - (0,0) + 2(0,1) - 2(1,2)$$

$$a_2 = (0,4) - (0,0) + 2(0,2) - 2(1,3) \qquad (51)$$

$$a_3 = (0,1) - (0,0) + 2(0,3) - 2(1,3)$$

$$a_4 = (0,3) - (0,0) + 2(0,4) - 2(1,2)$$

$$R(-1,-1) = a_4\beta + a_3\beta^2 + a_2\beta^3 + a_1\beta^4$$

Por (30) tnemeos:

$$p = R(1,1)\ R(-1,-1)$$

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2 + (\beta + \beta^4)B + (\beta^2 + \beta^3)C$$

Donde $B = a_1a_2 + a_2a_3 + a_3a_4$, $C = a_1a_3 + a_2a_4 + a_1a_4$

Reemplazando $\beta + \beta^4$ por $-1 - \beta^2 - \beta^3$ y haciendo notar que (50) es irreducible, se tiene:

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2 - B - (\beta^2 + \beta^3)(B - C)$$

y $\quad (\beta^2 + \beta^3)(B - C) = 0$

$$\Rightarrow \quad B = C$$

$$\therefore \quad p = a_1^2 + a_2^2 + a_3^2 + a_4^2 - B \ , \quad B = C \qquad (52)$$

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2 - 1/2\,(B + C)$$

$$16p = 16(a_1^2 + a_2^2 + a_3^2 + a_4^2) - 8(B + C)$$

$$16p = x^2 + 5(a_1 - a_2 - a_3 + a_4)^2 + 10F^2 + 10G^2$$

(53)

donde $x = a_1 + a_2 + a_3 + a_4$, $\quad F = a_2 - a_3$, $\quad G = a_1 - a_4$

$$x = (0,0) - (0,2) + 2(1,2) - 2(0,1) + (0,0) - (0,4) + 2(1,3) - 2(0,2)$$
$$+ (0,0) - (0,1) + 2(1,3) - 2(0,3) + (0,0) - (0,3) + 2(1,2) - 2(0,4)$$

$$x = -3(0,1) - 3(0,2) - 3(0,3) - 3(0,4) + 4(0,0) + 4(1,2) + 4(1,3)$$

$$x = -3f + 3 + 7(0,0) + 4(1,2) + 4(1,3)$$

$$7(0,0) = -7f - 7 + 21(1,2) + 21(1,3)$$

$$x = -10f - 4 + 25(1,2) + 25(1,3)$$

$$a_1 - a_2 - a_3 + a_4 = (0,2) - (0,0) + 2(0,1) - 2(1,2) - (0,4) + (0,0) - 2(0,2)$$
$$+ 2(1,3) - (0,1) + (0,0) - 2(0,3) + 2(1,3) + (0,3) - (0,0)$$
$$+ 2(0,4) - 2(1,2)$$

$$= -(0,2) - (0,3) + (0,4) + (0,1) - 4(1,2) + 4(1,3)$$

$$= -f + (1,2) + 2(1,3) + f - 2(1,2) - (1,3) - 4(1,2) + 4(1,3)$$

$$= -5(1,2) + 5(1,3)$$

$$a_1 - a_2 - a_3 + a_4 = 5\left[(1,3) - (1,2)\right]$$

$$F = (0,4) - (0,0) + 2(0,2) - 2(1,3) - (0,1) + (0,0) - 2(0,3) + 2(1,3)$$

$$F = 2\left[(0,2) - (0,3)\right] - \left[(0,1) - (0,4)\right]$$

(54) $\quad x = 25\left[(1,2) + (1,3)\right] - 10f - 4, \quad a_1 - a_2 - a_3 + a_4 = 5w,$

$$w = (1,3) - (1,2)$$

$$F = 2u - v, \quad G = u + 2v, \quad u = (0,2) - (0,3), \quad v = (0,1) - (0,4)$$

Entonces se tiene:

(55) $\quad 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \quad$ y $\quad x \equiv 1 \pmod 5.$

Sea $D = G^2 + 4FG - F^2$

$$D = (a_1 - a_4)^2 + 4(a_2 - a_3)(a_1 - a_4) - (a_2 - a_3)^2$$

$$= a_1^2 - a_2^2 - a_3^2 + a_4^2 + 2(a_1 a_2 + a_2 a_3 + a_3 a_4) - 2(a_1 a_3 + a_2 a_4 + a_1 a_4)$$

$$+ 2a_1 a_2 + 2a_3 a_4 - 2a_1 a_3 - 2a_2 a_4$$

$$= (a_1 + a_4)^2 - (a_2 + a_3)^2$$

$$D = (a_1 + a_4)^2 - (a_2 + a_3)^2$$

$$-5xw = (a_1 + a_2 + a_3 + a_4)(a_1 - a_2 - a_3 + a_4)$$

$$= a_1^2 + 2a_1a_4 + a_4^2 - a_2^2 - 2a_2a_3 - a_3^2$$

$$-5xw = (a_1+a_4)^2 - (a_2+a_3)^2$$

$$\therefore \quad D = -5xw$$

$$-25xw = 5D = (2F+G)^2 + 4(2F+G)(-F+2G) - (-F+2G)^2$$

$$= 25(u^2 + 4uv - v^2)$$

$$\therefore \quad xw = v^2 - 4uv - u^2 \qquad (56)$$

Por (49) y el valor de x se tiene

$$(0,1)+(0,2)+(0,3)+(0,4)+3(1,2)+3(1,3) = 2f$$

$$x \qquad f - 1 - (0,0) + 3(1,2) + 3(1,3) = 2f$$

$$(0,0) - 3(1,2) - 3(1,3) + f + 1 = 0$$

$$15(0,0) = 3\left[25(1,2) + 25(1,3)\right] - 25f - 25$$

$$25(0,0) = 3(x + 10f + 4) - 25f - 25$$

$$25(0,0) = 3x + 30f + 12 - 15f - 25$$

$$(57) \qquad 25(0,0) = p - 14 + 3x$$

Teorema: La congruencia

$$(58) \qquad x^5 + y^5 \equiv 1 \pmod{p = 5f+1}$$

tiene $p - 4 + 3x$ soluciones.

Demostración:

Por el corolario del teorema 1, capítulo I, (58) tiene

$25(0,0) = p - 14 + 3x$ soluciones primas a p.

Además tiene 5 soluciones con $x \equiv 0$ y 5 soluciones con $y \equiv 0$

$\therefore$ (58) tiene $p - 4 + 3x$ soluciones.

Por (53) y de la definición de w en (54), obtenemos:

$$4a_1 = 4a_1 - a_2 + a_4 + a_2 + a_3 + a_4 - 2a_4$$
$$= a_1 - a_2 - a_3 + a_4 + a_1 + a_2 + a_3 + a_4 + 2a_1 - 2a_4$$
$$= 5w - x + 2G$$
$$4a_1 = 5w - x + 2G$$

$$4a_2 = 4a_4 \quad a_1 - a_2 - a_3 + a_1 + a_2 + a_3 - 2a_1$$
$$= a_1 - a_2 - a_3 + a_4 + a_1 + a_2 + a_3 + a_4 + 2a_4 - 2a_1$$
$$= 5w - x - 2G$$
$$4a_2 = 5w - x - 2G$$

Análogamente obtenemos

$$4a_2 = -5w - x + 2F$$
$$4a_3 = -5w - x - 2F$$

Entonces

$$\begin{aligned} 4a_1 &= 5w - x + 2G \\ 4a_2 &= 5w - x - 2G \\ 4a_3 &= -5w - x + 2F \\ 4a_4 &= -5w - x - 2F \end{aligned} \qquad (59)$$

Teorema: Hay exactamente 8 soluciones enteras simultáneas de (55) y (56). Si (x, u, v, w) es una solución también (x, -u, -v, w) y $(x, \pm v, \mp u, -w)$ son soluciones, Las 4 restantes se obtienen de estas 4 cambiando todos los signos.

Demostración

Puesto que 5 es un residuo cuadrático de un primo $p = 5f + 1$, entonces la congruencia

$$s^2 \equiv 5 \pmod{p}$$

tiene solución.

Esto lo afirmamos por el siguiente teorema:

Cada $p \neq q$ (p y q primos) puede ser únicamente representado en la forma $p = 4qk \pm a$ donde $0 < a < 4q$ y $a \equiv 1 \pmod 4$. Para cada primo impar fijo q, las soluciones de la ecuación $(q/p) = 1$ son exactamente los primos $p \neq q$ tal que la correspondiente a es un residuo cuadrático de q, es decir, $(q/p) = (a/q)$. Los números a tales que $0 < a < 4q$, $a \equiv 1 \pmod 4$ y $(a/q) = 1$ están dados por los mínimos residuos positivos (mod. 4q) de los números $1^2, 3^2, \ldots, (q-2)^2$.

En este caso $q = 5$ y queremos ver que para un primo p de la forma $p = 5f+1$, 5 es un residuo cuadrático de p.

Entonces 5 es un residuo cuadrático de primos de la forma $20k \pm 1$, $20k \pm 9$.

Vamos a ver que p es de alguna de éstas formas.

Sabemos que f es par, $f = 2f'$

$$p = 5(2f')+1 = 10f'+1$$

i) Supongamos que $f' = 2f''$

$$p = 10(2f'')+1 = 20f''+1$$

ii) Si $f' = 2f''$ 1

$$p = 10(2f''+1)+1 = 20f''+11 = 20(f''+1) - 9$$

$\therefore$ $p = 5f+1$ es de la forma $20k+1$ ó de la forma $20k+9$

$\therefore$ 5 es un residuo cuadrático de $p = 5f+1$

y por lo tanto $s^2 \equiv 5 \pmod{p}$ tiene dos soluciones.

De (55) tenemos:

(55') $$50(u^2+v^2) \equiv -x^2 - 125w^2 \pmod{p}$$

En (56) despejado $v^2 - u^2$ y elevando al cuadrado:

$$(v^2 - u^2)^2 = (xw+4uv)^2$$

$$v^4+u^4 = (xw+4uv)^2+2u^2v^2$$

$$2500(v^4+u^4) = 2500(xw+4uv)^2+5000u^2v^2$$

En (55') elevando al cuadrado obtenemos

$$2500(u^4+v^4)\equiv(x^2+125w^2)^2-2500u^2v^2$$

$$\therefore\quad (x^2+125w^2)^2-5000u^2v^2\equiv 2500(xw+4uv)^2+5000u^2v^2$$

$$(x^2+125w^2)^2\equiv 2500(xw+4uv)^2+10000u^2v^2$$

$$(x^2-125w^2)^2\equiv 2500x^2w^2+20000xwuv+40000u^2v^2-500x^2w^2+10000u^2v^2$$

$$(x^2-125w^2)^2\equiv 2000x^2w^2+20000xwuv+50000u^2v^2$$

y multiplicando por $s^2\equiv 5 \pmod{p}$

$$s^2(x^2-125w^2)^2\equiv 10000x^2w^2+100000xwuv+250000u^2v^2$$

$$s^2(x^2-125w^2)^2\equiv 10000(xw+5uv)^2$$

Para una s adecuada

$$s(x^2-125w^2)\equiv 100(xw+5uv) \tag{60}$$

Ahora, multiplicando (55') por 50, (60) por 10 y sumando

$$2500(u^2+v^2)+1000xw+5000uv\equiv -50(x^2+125w^2)+10s(x^2-125w^2)$$

$$2500(u+v)^2\equiv -1000xw-50(50(x^2+125w^2)+10s(x^2-125w^2) \tag{61}$$

Sea r un entero tal que $\operatorname{ord}_p r = 5$. Este existe ya que si g es una raiz primitiva de p, entonces $g^{p-1}\equiv 1 \pmod{p}$

$$g^{5f} = (g^f)^5\equiv 1 \pmod{p}.$$

$$\sum_{i=1}^{4} r^i\equiv -1 \pmod{p}$$

Sea $a = r^4 - r, \quad b = r^3 - r^2$

$$a^2 + b^2 = (r^4 - r)^2 + (r^3 - r^2)^2 \equiv r^3 - 2 + r^2 + r - 2 + r^4$$

$$\equiv r + r^2 + r^3 + r^4 - 4 \equiv -5$$

$$a^2 + b^2 \equiv -5 \pmod{p}$$

$$a^2 - b^2 \equiv r^3 - 2 + r^2 - r + 2 - r^4 \equiv -r^4 + r^3 + r^2 - r = s$$

$$a^2 - b^2 \equiv s \pmod{p}, \quad s = -r^4 + r^3 + r^2 - r$$

$$s^2 = (-r^4 + r^3 + r^2 - r)^2 \equiv (-1 - 2r^4 - 2r^2)^2 \equiv 1 + 4r^4 + 4r + 4r^3 + 8 + 4r^2$$

$$9 + 4(r + r^2 + r^3 + r^4) \equiv 5$$

$$s^2 \equiv 5 \pmod{p}$$

$$ab = (r^4 - r)(r^3 - r^2) = r^2 - r - r^4 + r^3 = s$$

$$ab \equiv s \pmod{p}$$

Definimos $m = -2a - 4b, \quad t = 4a - 2b$

$$m^2 = (2a \quad 4b)^2 = 4a^2 + 16ab + 16b^2 \equiv 10(a^2 + b^2) + 16s - 6(a^2 - b^2)$$

$$\equiv -50 + 16S - 6S = -50 + 10S$$

$$m^2 \equiv 10S - 50$$

$$t^2 = (4a - 2b)^2 = 16a^2 - 16ab + 4b^2 \equiv 10(a^2 + b^2) - 16S + 6(a^2 - b^2)$$

$$-50 - 16S + 6S = -10S - 50$$

$$t^2 \equiv -10S - 50$$

$$mt = -(2a+4b)(4a-2b) = -8a^2 - 12ab + 8b^2 \equiv -8(a^2 - b^2) - 12ab$$

$$\equiv -8S - 12S = -20S$$

$$mt \equiv -20S$$

Hemos obtenido

(62) $\quad m^2 \equiv 10S - 50, \quad t^2 \equiv -10S - 50, \quad mt \equiv -20S \pmod{p}$

(61) Se puede escribir de la siguiente manera:

$$[50(u+v)]^2 \equiv (mx + 5Stw)^2 \pmod{p}$$

$\therefore$ (61) es el cuadrado de

(63) $-50(u+v) \equiv mx + 5Stw \pmod{p}$

ó de la congruencia que resulta de ésta, cambiando los signos de u y v.

Este cambio debemos tomarlo con cuidado en el teorema.

Sea $\quad sk = t + m, \quad 2L = t - m$

Entonces (63) es la suma de

(64) $\quad 50u \equiv kx + 5sLw \quad$ y $\quad 50v \equiv -Lx + 5skw$

El producto de (64) concuerda con (60) porque:

$$1500uv \equiv (kx + 5sLw)(-Lx + 5skw)$$

$$\equiv -kLx^2 + 5sxw(k^2 - L^2 + 25s^2 kLw$$

pero $\quad kL \equiv -5s \quad$ y $\quad k^2 - L^2 \equiv -20s$

Entonces

$$2500uv \equiv 5sx^2 + 5sxw(-20s) + 125(-5S)w^2$$

$$\equiv 5s(x^2 - 125w^2) - 100s^2xw$$

$$5s(x^2 - 125w^2) \equiv 2500uv + 500xw$$

$$\therefore \quad s(x^2 - 125w^2) \equiv 100(xw + 5uv) \pmod{p}$$

La ambigüedad en la determinación de u y v es eliminada como sigue:

Reemplazemos r por r^2 y w por $-w$, entonces:

$$a_1 = (r^2)^4 - r^2 = r^3 - r^2 = b$$

$$b_1 = (r^2)^3 - (r^2)^2 = r - r^4 = -a$$

$$a_1^2 + b_1^2 \equiv -50, \quad a_1^2 - b_1^2 \equiv -s, \quad a_1 b_1 \equiv -s$$

$$m_1 = -2a_1 - 4b_1 = -2b + 4a = t$$

$$t_1 = 4a_1 - 2b_1 = 4b + 2a = -m$$

$$m_1 = t, \quad t_1 = -m$$

$$m_1 t_1 = -mt$$

$$50(u + v) \equiv -t_1 x + 5s m_1 w \pmod{p}$$

$$2k_1 = t_1 + m_1 = -m + t = 2L$$

$$2L_1 = t_1 - m_1 = -(m + t) = -2k$$

$$50u \equiv -Lx + 5sk_1 w, \quad 50v \equiv -k_1 x - 5sL_1 w$$

Entonces k, L, s, u, v corresponden a $L, -k, -s, -v, u$ respectivamente. De aquí, (64) se sigue para la solución dada o para la nueva so-

lución $(x_1, -v, u, -w)$ de (55) y (56).

Sean (x, u, v, w) y (x_1, u_1, v_1, w_1) soluciones cualesquiera de (55), (56). y (64)

Evidentemente

$$x x_1 + 50 u u_1 + 50 v v_1 + 125 w w_1 \equiv 0 \pmod{p}$$

Sea $A = | x x_1 + 50 u u_1 + 50 v v_1 + 125 w w_1 |$

Por (55) se tiene

$$(16p)^2 = (x^2 + 50u^2 + 50v^2 + 125w^2)(x_1^2 + 50u_1^2 + 50v_1^2 + 125w_1^2)$$

$$(16p)^2 = A^2 + 50(x u_1 - x_1 u)^2 + 50(x v - x_1 v)^2 + 125(x w_1 - x_1 w)^2$$
$$+ 2500(u v_1 - u_1 v)^2 + 6250(u w_1 - u_1 w)^2 + 6250(u w_1 - u_1 w)^2$$
$$+ 6250(u w_1 - v_1 w)^2$$

$\therefore \quad A \leq 16p$

$(16p)^2 \equiv A^2 \pmod{25}$

$\Rightarrow \quad 6p^2 \equiv A^2 \pmod{25}$

Por (55), $x \equiv w, \quad x_1 \equiv w_1 \pmod{2}$

$\Rightarrow$ A es par y por lo tanto A es de la forma $A = 2np$

$4n^2 p^2 \equiv A^2 \Rightarrow 4n^2 \equiv 6 \pmod{25}$

$2n \equiv \pm 16, \quad n = 5j \pm 1 \quad$ y $\quad j \equiv \pm 3 \pmod{5}$

$\therefore \quad A = 16p$

$$x u_1 - x_1 u = 0, \ldots, v w_1 - v_1 w = 0$$

$$(55) \Rightarrow x^2 \equiv x_1^2 \equiv 1 \pmod 5, \quad x \neq 0 \neq x_1$$

$$\frac{u}{x} = \frac{u_1}{x_1}, \quad \frac{v}{x} = \frac{v_1}{x_1}, \quad \frac{w}{x} = \frac{w_1}{x_1}$$

$\therefore \quad x^2 = x_1^2$ porque

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2$$

$$\frac{16p}{x^2} = 1 + 50\frac{u^2}{x^2} + 50\frac{v^2}{x^2} + 125\frac{w^2}{x^2}$$

$$\frac{16p}{x^2} = 1 + 50\frac{u_1^2}{x_1^2} + 50\frac{v_1^2}{x_1^2} + 125\frac{w_1^2}{x_1^2}$$

$$\therefore \quad \frac{x_1^2}{x^2} 16p = x_1^2 + 50u_1^2 + 50v_1^2 + 125w_1^2 = 16p$$

$$\therefore \quad x_1^2 = x^2$$

y por lo tanto

$$u^2 = u_1^2, \quad v^2 = v_1^2, \quad w^2 = w_1^2,$$

Esto prueba el teorema 8.

Ahora, escojamos una de las 8 soluciones de (55) y (56) Entonces las tres ecuaciones lineales (49) y las cuatro ecuaciones lineales en (54) cuyos miembros de la izquierda son x, w, u, y v determinan únicamente (o,h), $h = 0, 1, \ldots, 4$, $(1,2)$ y $(1,3)$ y por lo tanto quedan únicamente determinadas las 25 constantes ciclotómicas. Esto resuelve el problema ciclotómico para $e = 5$.

CAPITULO VI

Subdivisión de Períodos y Teorema de Jacobi

Subdivisión de Períodos

Sea d cualquier divisor de e y $E = e/d$

Entonces $p - 1 = ef = dEf$

$$\frac{p-1}{E} = df$$

Reemplazando e y f por E y df respectivamente (en (1), vemos que los E períodos son:

$$Y_k = \sum_{t=0}^{df-1} R^{g^{Et+k}} \qquad (k = 0, 1, \ldots, E-1)$$

Los valores $j, d+j, \ldots, (f-1)d+j$ de t dan los términos de η_{k+jE} en (1) porque

$$R^{g^{Ej+k}}, R^{g^{E(d+j)+k}}, \ldots, R^{g^{E((f-1)d+j)+k}} = R^{g^{(Ej+k)}},$$

$$R^{g^{E+(EJ+k)}}, \ldots, R^{g^{(f-1)e+(Ej+k)}}$$

y estos son precisamente los términos de η_{k+jE}

Entonces se tiene

$$Y_k = \sum_{j=0}^{d-1} \eta_{k+jE}$$

Tome $d = 2$. Entonces $e = 2E$ y

$$Y_k = \sum_{j=0}^{1} \eta_{k+jE} = \eta_k + \eta_{k+E}$$

$$Y_o Y_k = (\eta_o + \eta_E)(\eta_k + \eta_{k+E})$$

$$\eta_o \eta_k = \sum_{h=0}^{E-1} (k, h)\eta_h + fs_k + \sum_{H=0}^{E-1} (k, E+H)\eta_{E+H}$$

de aquí podemos obtener $\eta_o \eta_{k+E}$ reemplazando k por $k+E$

$$\eta_o \eta_{k+E} = \sum_{h=0}^{E-1} (k+E, h)\eta_h + \sum_{H=0}^{E-1} (k+E, E+H)\eta_{E+H} + fs_{k+E}$$

Similarmente, por (7) tnemos

$$\eta_E \eta_{E+k} = fs_k + \sum_{h=0}^{e-1} (k, h)\eta_{E+h} = fs_k + \sum_{h=0}^{E-1} (k, h)\eta_{E+h}$$

$$+ \sum_{H=0}^{E-1} (k, E+H)\eta_H$$

Reemplazando m por k y k por E - k en (7), obtenemos:

$$\eta_k \eta_E = fs_{E-k} + \sum_{h=0}^{e-1} (E-k,\ h)\eta_{k+h}$$

$$= fs_{E-k} + \sum_{h=E-k}^{2E-1-k} (E-k,\ h)\eta_{k+h} + \sum_{h=0}^{E-1-k} + \sum_{h=2E-k}^{2E-1}$$

En la primera suma tomemos $k+h = E+H$; obtenemos:

$$\sum_{H=0}^{E-1} (E-k,\ E+H-k)\eta_{E+H}$$

En las segunda y tercera sumas, tome $k+h = H$. En el último caso debemos quitar $2E$ de los índices de η.

Combinando tenemos:

$$\sum_{h=0}^{E-1-k} (E-k,\ h)\eta_{k+h}, \qquad \sum_{h=2E-k}^{2E-1} (e-k,\ h)\eta_{k+h}$$

$$k+h = H$$

Para $h = 0$ tenemos $H = k$ y para $h = E-1-k$, $H = E-1$

$$\therefore \qquad \sum_{H=k}^{E-1} (E-k,\ H-k)\eta_H$$

Para $h = 2E - k$ y $h = 2E - 1$ tenemos respectivamente

$$k + 2E - k = H \quad y \quad k + 2E - 1 = H$$

$$\sum_{H=2E}^{2E-Hk} (E - k,\ H - k)\eta_H = \sum_{H=0}^{-1+k} (E - k,\ H - k)\eta_H$$

y sumando

$$\sum_{H=k}^{E-1} (E - k,\ H - k)\eta_H + \sum_{H=0}^{k-1} (E - k,\ H - k)\eta_H =$$

$$\sum_{H=0}^{E-1} (E - k,\ H - k)\eta_H$$

$$\eta_k \eta_E = f_{s_{E-k}} + \sum_{H=0}^{E-1} (E - k,\ E\ H - k)\eta_{E+H}$$

$$+ \sum_{H=0}^{E-1} (E - k,\ H - k)\eta_H$$

Entonces

$$Y_o Y_k = 2f_{s_k} + f_{S_{k+E}} + f_{S_{E-k}} + \sum_{h=0}^{E-1} (k, h)\eta_h + \sum_{h=0}^{E-1} (k,\ E+h)\eta_{E+h}$$

$$\sum_{h=0}^{E-1} (k+E,\ h)\eta_h + \sum_{h=0}^{E-1} (k+E,\ E+h)\eta_{E+h}$$

$$\sum_{h=0}^{E-1} (k,h)\eta_{E+h} \sum_{h=0}^{E-1} (k,\ E+h)\eta_h \sum_{h=0}^{E-1} (E-k,\ E+h-k)\eta_{E+h}$$

$$\sum_{h=0}^{E-1} (E-k,\ h-k)\eta_h$$

$$= 2fs_k + fs_{k+E} + fs_{E-k}$$

$$+ \sum_{h=0}^{E-1} \left[(k,h)+(k+E,h)+(k,E+h)+(E-k,\ h-k)\right]\eta_h$$

$$\sum_{h=0}^{E-1} \left[(k,E+h)+(k+E,\ E+h)+(k,h)+(E-k,\ E+h-k)\right]\eta_{E+h}$$

Pero por (14) y (15) se tiene que

$$(e-k,\ h-k) = (k,\ h)$$

$(k+E,\ E+h) = (e-(k+E),\ E+h-(E+k)) = (e-k-e/2,\ h-k) =$

$(E-k,\ h-k)\ (E-k,\ E+h-k) = (e-(E-k),\ E+h-k-(E-k)) =$

$(E+k,\ h)$

$$Y_o Y_k = 2fs_k + fs_{k+E} + fs_{E-k}$$

$$+ \sum_{h=0}^{E-1} (k,h)+(k+E,h)+(k,E+h)+(E-k,\ h-k)\Big]\eta_h$$

$$\sum_{h=0}^{E-1} \left[(k,h)+(k+E,h)+(k,E+h)+(E-k,\ h-k)\right] \eta_{h+E}$$

$$\therefore \quad Y_o Y_k = 2fs_k + fs_{k+E} + fs_{E-k} + \sum_{h=0}^{E-1} (k,h)_E \left(\eta_h + \eta_{E+h}\right) =$$

$$Y_o Y_k = 2fs_k + fs_{k+E} + fs_{E-k} + \sum_{h=0}^{E-1} (k,h)_E Y_h$$

donde $(k,h)_E = (k,h)+(k+E,h)+(k,E+h)+(E-k,\ h-k)$

Por (14) y (15)

$$(0,0)_E = (0,0)+(E,0)+(0,E)+(E,0)$$

Si f es par.

$$(E,0) = (0,E)$$

$$\therefore \quad (0,0)_E = (0,0)+3(0,E) \quad \text{si f es par}$$

Si f es impar.

$$(k,h) = (h+E/2,\ k+e/2),\ (e-k,\ h-k) = (k,\ h)$$

$$(e/2,0) = (e/2,\ e) = (e/2,\ e/2) = (0,0)$$

$$(0,0)_E = (0,0)+2(e/2,0)+(0,\ e/2)$$

$$\therefore \quad (0,0)_E = 3(0,0)+(0,E) \quad \text{si f es impar.}$$

En (22) para $e = 2E$, $m = 2M$, tome $j = J+E$ en los términos con

$j = E_1, \ldots, 2E-1$

Tenemos:

$$F(\beta^{2M}) = \sum_{j=0}^{2E-1} \beta^{2Mj} \eta_j = \sum_{j=0}^{E-1} \beta^{2Mj} \eta_j + \sum_{j=E}^{2E-1} \beta^{2Mj} \eta_j$$

$$= \sum_{j=0}^{E-1} \beta^{2Mj} \eta_j + \sum_{j=0}^{E-1} \beta^{2M(j+E)} \eta_{j+E} =$$

$$= \sum_{j=0}^{E-1} \beta^{2Mj} \eta_j + \sum_{j=0}^{E-1} \beta^{2Mj} \eta_{j+E}$$

$$= \sum_{j=0}^{E-1} \beta^{2Mj} (\eta_j + \eta_{j+E}) = \sum_{j=0}^{E-1} \beta^{2Mj} Y_j$$

$$\therefore \quad F(\beta^{2M}) = \sum_{j=0}^{E-1} \beta^{2Mj} Y_j$$

Ahora, $B = \beta^2$ es una raiz E -ésima de la unidad.

Sea $\phi(B^m)$ la función obtenida de $F(\beta^m)$ en (22) al reemplazar e por E, β por B y η por Y.

Entonces $F(\beta^{2M}) = \phi(B^m)$

Aplicando (26) también para ϕ, obtenemos:

$$R(2r, 2s)_e = \left\{ R(r,s)_E \quad \text{con } \beta \text{ reemplazada por } \beta^2 \right\}$$

Teorema de Jacobi.- Si $g^m \equiv 2 \pmod{p}$, la función (23) tiene la propiedad siguiente:

$$F(-1)\, F(\alpha^2) = {}^{2m} F(\alpha)\, F(-\alpha) \tag{65}$$

Demostración

$$F(\alpha) = \sum_{i=0}^{p-2} \alpha^i R^{g^i}$$

$$F(-\alpha) = \sum_{j=0}^{p-2} (-\alpha)^j R^{g^j}$$

$$F(\alpha)\, F(-\alpha) = \sum_{i=0}^{p-2} \alpha^i R^{g^i} \sum_{j=0}^{p-2} (-\alpha)^j R^{g^j} = \sum_{i=0}^{p-2} \sum_{j=0}^{p-2} \alpha^i (-\alpha)^j R^{g^i} R^{g^j}$$

$$F(\alpha)\, F(-\alpha) = \sum_{i=0}^{p-2} \sum_{j=0}^{p-2} (-1)^j \alpha^{i+j} R^{g^i + g^j}$$

Para una i fija, el coeficiente de α^i en $F(\alpha)\, F(-\alpha)$ es:

$$\sum_{j=0}^{p-2} (-1)^j R^c, \quad \text{con} \quad c \equiv g^{i-j} + g^j \tag{66}$$

. . éste es el coeficiente de α^{2m+i} en el segundo miembro de (65).

Si i es impar, la suma (66) es cero, puesto que $j = J$ y $j = i - J$ dan lugar al mismo valor de c módulo p., mientras que uno

es impar y el otro es par.

Sea i par, $i = 2t$

$$F(\alpha^2) = \sum_{k=0}^{p-2} \alpha^{2k} R^{g^k}$$

El coeficiente de α^{2m+2t} en $F(-1)\,F(\alpha^2)$ es

$$F(-1)\,(R^{g^{m+t}} + R^{g^{m+t+\frac{1}{2}(p-1)}}) = F(-1)\,(R^{g^{m+t}} + R^{-g^{m+t}})$$

ó usando que $g^m \equiv 2 \pmod{p}$ el coeficiente es:

$$(67) \qquad \sum_{k=0}^{p-2} (-1)^k R^{g^k + 2g^t} + \sum_{k=0}^{p-2} (-1)^k R^{g^k - 2g^t}$$

1º/ Sea $J \not\equiv t \pmod{\tfrac{1}{2}(p-1)}$. Entonces J e $i - J$ son valores de j que son incongruentes modulo $(p-1)$ porque

si $J \equiv i - J$ entonces $2J \equiv i = 2t \pmod{(p-1)}$

$\Rightarrow J \equiv t \pmod{\tfrac{1}{2}(p-1)}$, lo cual no puede ser.

$\therefore$ J e $i - J$ son incongruentes (mod. $(p-1)$), dejando a la misma c en (66), y el coeficiente de R^c es $2(-1)^J$.

El término R^c aparece en la primera suma de (67) para

$$g^k \equiv g^{-J}(g^t - g^J)^2 \qquad \text{porque}$$

$$g^k \equiv g^{-J}(g^t - g^J)^2 = g^{2t-J} + g^J - 2g^t$$

$$g^k + 2g^t \equiv g^{i-J} + g^J$$

χ en la segunda suma aparece para $g^k \equiv g^{-J}(g^t + g^J)^2$.

En cada caso g^k y g^J son ambos residuos cuadráticos de p ó no lo son, de aquí $k \equiv J \pmod 2$.

Entonces el coeficiente de R^c en (67) es $2(-1)^J$

2°/ Sea $J \equiv t \pmod{\tfrac{1}{2}(p-1)}$.

$$2J \equiv 2t \pmod{(p-1)}$$

$$\Rightarrow g^{2J} \equiv g^{2t} \pmod p$$

$$g^J \equiv \pm g^t \pmod p$$

Tenemos $g^{2J} \equiv g^i$

$$g^J \equiv g^{i-J}$$

$$2g^J \equiv g^{i-J} + g^J \equiv c$$

$$\therefore c \equiv 2g^J \equiv \pm 2g^t$$

$$\therefore c \equiv \pm 2g^t \pmod p$$

Ahora, solo una de las dos sumas (67) nos da un término R^c, el segundo cuando $g^k \quad 4g^t$ y el primero cuando $g^k \quad -4g^t$.

En ambos casos $g^k \quad 4g^J \pmod p$, de aquí $k \quad J \pmod 2$.

Entonces $(-1)^J$ es el coeficiente de R^c en ambos (66) y (67).

Falta considerar exponentes c que no aparecen en (66).

Sea $z = g^j$

Entonces $\frac{g^{2t}}{z} + z \equiv c \pmod{p}$ no tiene raiz z.

$\therefore$ $c^2 - 4g^{2t}$ no es residuo cuadrático de p.

De aquí para una de las congruencias

$$c - 2g^t \equiv g^k, \quad c + 2g^t \equiv g^k \pmod{p}$$

la solución g^k es un residuo y para la otra no.

Entonces x^c aparece en una de las sumas (67) con el coeficiente $+1$ y en la otra con el coeficiente -1 y por lo tanto se anulan.

Hemos demostrado que (66) y (67) tiene los mismos coeficientes de R^c para cada c.

$\therefore$ Queda demostrado (65).

B I B L I O G R A F I A

1 L. E. Dickson — Ciclotomy, higher congruences and Waring's problem. Amer. J. Math. 57 (1935) 391-408

2 W. J. LeVeque — Topi .s in Number Theory Vol. I y II. Addison Wesley Publishing Company, Inc.

3 Ivan Niven y H. Zuckerman — An introduction to the Theory of Numbers. John Wiley & Sons, Inc.