CUBO 11, 37-47 (1995)
Novena Jornada de Matemática de la Zona Sur

Ciclotomía y Niveles Superiores

Mónica Canales

Resumen

Sea $p > 2$ primo y sea $d \geq 2$ entero tal que $d \mid p-1$. En este trabajo queremos establecer un método recurrente para encontrar los coeficientes de la ecuación de período, resolvente de la ecuación ciclotómica $X^p - 1 = 0$ para d, en términos de sumas de caracteres. Esto, motivados por su relación con el nivel d-ésimo de un cuerpo finito con p elementos, definido como

$$s_d(\mathbf{F}_p) = \min\left\{ s \,\middle|\, -1 = a_1^d + \ldots + a_s^d,\ a_i \in \mathbf{F}_p^* \right\}$$

1 Introducción

Sea $p > 2$ primo, $d \geq 1$ entero tal que $p - 1 = dc$ y sean ζ una raíz p-ésima primitiva de la unidad y ω un generador de $\mathbf{F}_p^*$, el grupo multiplicativo cíclico de los elementos no nulos del cuerpo finito con p elementos.

El método de Gauss para resolver la ecuación ciclotómica $X^p - 1 = 0$, introduce los conceptos de *períodos* y *ecuación de período*.

Las $p-1$ raíces del polinomio ciclotómico irreductible

$$1 + X + X^2 + \ldots + X^{p-1} = 0$$

dadas por $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, i.e., $\zeta, \zeta^{\omega}, \ldots, \zeta^{\omega^{p-2}}$, se pueden agrupar en d *períodos* de c términos, definidos por

$$\eta_i = \zeta^{\omega^i} + \zeta^{\omega^{i+1}} + \zeta^{\omega^{2i+1}} + \ldots + \zeta^{\omega^{(e-1)i+e-1}},\ 0 \leq i \leq d-1$$

que satisfacen a su vez un polinomio irreducible sobre $\mathbf{Z}[X]$

$$P_d(X) = \prod_{i=0}^{d-1} (X - \eta_i) \in \mathbf{Z}[X]$$

llamado *ecuación de período*.

El problema ciclotómico para $d \mid p-1$ se dice resuelto si se conocen los coeficientes de la ecuación de período. Este es un antiguo y difícil problema.

En nuestro estudio de niveles superiores de cuerpos finitos [1] se ha determinado el nivel d-ésimo de $\mathbf{F}_p$

$$s_d(\mathbf{F}_p) = \min\left\{ s \,|-1 = a_1^d + \ldots + a_s^d,\ a_i \in \mathbf{F}_p^* \right\}$$

en términos de los primeros coeficientes de $P_d(X)$, por lo que nuestro problema fundamental es ahora encontrar una manera de determinar explícitamente estos coeficientes.

2 Sobre la determinación de los coeficientes de la Ecuación de Período

Aquí establecemos un método recurrente para expresar los coeficientes de la ecuación de período en término de sumas de caracteres, ésto pues los períodos mismos son sumas de caracteres.

Recordemos que un carácter sobre $\mathbf{F}_p^*$ es una aplicación $\chi : \mathbf{F}_p^* \longrightarrow \mathbf{C} - \{0\}$ tal que $\chi(xy) = \chi(x)\chi(y)$, $\forall x, y \in \mathbf{F}_p^*$. En particular $\chi^{p-1}(x) = \chi(1) = 1$, $\forall x \in \mathbf{F}_p^*$.

Los caracteres sobre $\mathbf{F}_p^*$ forman un grupo isomorfo a $\mathbf{F}_p^*$ con la multiplicación natural $\chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$. Se tiene $\chi^{-1}(x) = \dfrac{1}{\chi(x)} = \overline{\chi}(x)$ y $\chi_0(x) = 1$, $\forall x \in \mathbf{F}_p^*$ es la unidad del grupo y se dice carácter principal.

Considerando $U = (\mathbf{F}_p^*)^d$ el subgrupo de las potencias d-ésimas en $\mathbf{F}_p^*$, se tiene

$$\eta_0 = \zeta + \zeta^{\omega^d} + \zeta^{\omega^{2d}} + \ldots + \zeta^{\omega^{(e-1)d}} = \tau_U(\chi_0)$$

donde

$$\tau_H(\chi) = \sum_{x \in H} \chi(x)\zeta^x$$

es la suma de Gauss asociada al carácter χ sobre $H \leq \mathbf{F}_p^*$.

De este modo encontramos, por propiedades de extensión de caracteres y sumas de Gauss que

$$\eta_0 = \frac{1}{d} \sum_{\chi | \chi^d = \chi_0} \tau(\chi) \qquad \text{donde} \qquad \tau(\chi) = \sum_{x \in \mathbf{F}_p^*} \chi(x)\zeta^x$$

y en general

$$\eta_i = \frac{1}{d} \sum_{\chi | \chi^d = \chi_0} \overline{\chi}(\omega^i)\tau(\chi) \quad , \qquad 0 \leq i \leq d-1$$

los d conjugados de η_0 en $Q(\zeta)$ por $Gal(\mathbf{Q}(\eta_0)/\mathbf{Q}) \cong \mathbf{F}_p^* / U = \langle \omega (\mathrm{mod}\, U) \rangle$.

Luego, considerando los coeficientes de $P(x) = x^d + \alpha_1 x^{d-1} + \alpha_2 x^{d-2} + \ldots + \alpha_d$ como las funciones simétricas en los períodos, resulta

$$\alpha_1 = -\sum_{i=0}^{d-1} \eta_i = -\sum_{x \in \mathbf{F}_p^*} \zeta^x = -(-1) = 1$$

$$\alpha_2 = \sum_{a_1 < a_2} \left(\frac{1}{d} \sum_{\chi_1^d = \chi_0} \overline{\chi}_1(a_1)\tau(\chi_1) \right) \left(\frac{1}{d} \sum_{\chi_2^d = \chi_0} \overline{\chi}_2(a_2)\tau(\chi_2) \right)$$

donde denotamos $a < b$ si $a \equiv \omega^i (\mathrm{mod}\, U)$, $b \equiv \omega^j (\mathrm{mod}\, U)$ y $0 \leq i < j \leq d-1$.

Y en general

$$\alpha_n = \frac{(-1)^n}{d^n} \sum_{\chi_1^d = \ldots = \chi_n^d = \chi_0} \left(\sum_{a_1 < \ldots < a_n} \overline{\chi}_1(a_1) \ldots \overline{\chi}_n(a_n) \right) \tau(\chi_1) \ldots \tau(\chi_n).$$

Ahora debemos explicitar estas sumas. En

$$\alpha_2 = \frac{1}{d^2} \sum_{\chi_1^d = \chi_2^d = \chi_0} \left(\sum_{a_1 < a_2} \overline{\chi}_1(a_1)\overline{\chi}_2(a_2) \right) \tau(\chi_1)\tau(\chi_2)$$

observamos que $\tau(\chi_1)\tau(\chi_2)$ conmutan y que claramente

$$\sum_{\chi_1, \chi_2} \sum_{a_1 < a_2} \overline{\chi}_1(a_1)\overline{\chi}_2(a_2) = \sum_{\chi_1, \chi_2} \sum_{a_1 > a_2} \overline{\chi}_1(a_1)\overline{\chi}_2(a_2)$$

luego

$$\sum_{\chi_1,\chi_2}\sum_{a_1,a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2) = 2\sum_{\chi_1,\chi_2}\sum_{a_1<a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2)+\sum_{\chi_1,\chi_2}\sum_{a_1=a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2)$$

de lo que resulta

$$\alpha_2 = \frac{1}{d^2}\sum_{\chi_1^d=\chi_2^d=\chi_0}\left(\frac{1}{2}\sum_{a_1,a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2)-\frac{1}{2}\sum_{a_1=a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2)\right)\tau(\chi_1)\tau(\chi_2).$$

Es decir, hemos conseguido expresar la suma interior en α_2, en términos de las sumas libres $\sum_{a_1,a_2}\overline{\chi}_1(a_1)\overline{\chi}_2(a_2)$ y $\sum_{a_1}\overline{\chi}_1\overline{\chi}_2(a_1)$, las cuales pueden calcularse pues por propiedades de sumas de caracteres se tiene

$$\sum_{x\in\mathbf{F}_p}\chi(x) = \begin{cases} p-1 & \text{si} \quad \chi=\chi_0 \\ 0 & \text{si} \quad \chi\neq\chi_0 \end{cases}$$

y si χ es un carácter de orden d, cuyas potencias inducen todos los caracteres con la propiedad $\chi^d=\chi_0$, entonces

$$\sum_{i=0}^{d-1}\chi^i(-1) = \begin{cases} -1 & \text{si} \quad 2d\nmid p-1 \\ d-1 & \text{si} \quad 2d\mid p-1. \end{cases}$$

Luego

$$\begin{aligned}\alpha_2 &= \frac{1}{d^2}\sum_{\chi_1^d=\chi_2^d=\chi_0}\left(\frac{1}{2}\sum_{a_1}\overline{\chi}_1(a_1)\sum_{a_2}\overline{\chi}_2(a_2)-\frac{1}{2}\sum_{a}\overline{\chi}_1\overline{\chi}_2(a)\right)\tau(\chi_1)\tau(\chi_2)\\ &= \frac{1}{d^2}\sum_{i,j=0}^{d-1}\left(\frac{1}{2}\sum_{a_1}\overline{\chi}^i(a_1)\sum_{a_2}\overline{\chi}^j(a_2)-\frac{1}{2}\sum_{a}\overline{\chi}^{i+j}(a)\right)\tau(\chi^i)\tau(\chi^j)\\ &= \frac{1}{d^2}\left(\frac{1}{2}(d^2-d)\tau(\chi_0)^2-\frac{d}{2}\sum_{i=1}^{d-1}\tau(\chi^i)\tau(\overline{\chi}^i)\right)\end{aligned}$$

De

$$\tau(\chi_0)=\sum_{x\in\mathbf{F}_p}\zeta^x=-1$$

y

$$\tau(\chi^i)\tau(\overline{\chi}^i)=\chi^i(-1)p,\ 0<i\leq d-1$$

resulta

$$\alpha_2 = \frac{1}{d^2}\left(\frac{d^2-d}{2} - \frac{d}{2}p\sum_{i=1}^{d-1}\chi^i(-1)\right)$$

i. e.

$$\alpha_2 = \begin{cases} \dfrac{p+(d-1)}{2d} & \text{si} \quad 2d \nmid p-1 \\ \dfrac{(d-1)(1-p)}{2d} & \text{si} \quad 2d \mid p-1. \end{cases}$$

Así hemos encontrado explícitamente el coeficiente α_2 en términos de p y d.

Análogamente es posible expresar la suma interior en α_n en términos de las sumas libres $\sum_{a_1,\ldots,a_n} \overline{\chi}_1(a_1)\cdots\overline{\chi}_n(a_n), \ldots, \sum_{a_i} \overline{\chi}_1\cdots\overline{\chi}_n(a_i)$.

Primero introduciremos algunas notaciones: Sean

$$\sum_{a_1,\ldots,a_{n-1}} := \sum_{\chi_1,\ldots,\chi_n} \sum_{a_1,\ldots,a_{n-1}=\ldots=a_n} \overline{\chi}_1(a_1)\cdots\overline{\chi}_n(a_n)$$

$$\sum_{a_1<\ldots<a_{n-1}} = \sum_{\chi_1,\ldots,\chi_n} \sum_{a_1<\ldots<a_{n-1}=\ldots=a_n} \overline{\chi}_1(a_1)\cdots\overline{\chi}_n(a_n)$$

$$\sigma_i^{(n-k)} := i + (i+1) + \ldots + (n-k)$$

$$\begin{aligned} \sigma_i^{(n-k)^2} &:= i\sigma_i^{(n-k)} + (i+1)\sigma_{i+1}^{(n-k)} + \ldots + (n-k)^2 \\ &= i^2 + i(i+1) + \ldots + i(n-k) \\ &\quad\ (i+1)^2 + \ldots + (i+1)(n-k) \\ &\quad\ \ddots \quad \vdots \\ &\quad\ (n-k)^2 \end{aligned}$$

$$\sigma_i^{(n-k)^3} := i\sigma_i^{(n-k)^3} + (i+1)\sigma_{i+1}^{(n-k)^3} + \ldots + (n-k)^3$$

$$\vdots$$

donde $n \geq 2$, $0 \leq k \leq n-1$ y $\sigma_i^{(n-k)^s}$ definido si $2 \leq i \leq n-k$.

Entonces se obtiene el siguiente resultado.

$$
\begin{aligned}
n!\sum_{a_1,\dots,a_n} = & \sum_{a_1<\dots<a_n} + (n-1)!\left[1+\sigma_2^{(n-1)}\right]\sum_{a_1<\dots<a_{n-1}} \\
& + \dots \\
& + \left[1+\sigma_2^{(n-k)}+\sigma_2^{(n-k)^2}+\dots+\sigma_2^{(n-k)^k}\right](n-k)!\sum_{a_1<\dots<a_{n-k}} \\
& + \dots \\
& + \left[1+2+2^2+\dots+2^{n-2}\right]2!\sum_{a_1<a_2} \\
& + \sum_{a_1}
\end{aligned}
$$

de lo que se sigue el resultado. ■

Con este resultado se obtiene recurrentemente la suma interior de α_n en función de las sumas libres $\sum_{a_1}, \sum_{a_1,a_2}, \dots, \sum_{a_1,\dots,a_n}$.

Por ejemplo obtenemos:

$$
\begin{aligned}
3!\sum_{a_1<a_2<a_3} &= \sum_{a_1,a_2,a_3} -3\sum_{a_1,a_2} +2\sum_{a_1} \\
4!\sum_{a_1<\dots<a_4} &= \sum_{a_1,\dots,a_4} -6\sum_{a_1,a_2,a_3} +11\sum_{a_1,a_2} -6\sum_{a_1} \\
5!\sum_{a_1<\dots<a_5} &= \sum_{a_1,\dots,a_5} -10\sum_{a_1,\dots,a_4} +35\sum_{a_1,a_2,a_3} -50\sum_{a_1,a_2} +24\sum_{a_1} \\
&\vdots
\end{aligned}
$$

Ahora bien, con este resultado obtenemos

$$
\begin{aligned}
\alpha_3 &= \frac{(-1)^3}{d^3}\sum_{i,j,k=0}^{d-1}\left[\frac{1}{3!}\sum_{a_1}\overline{\chi}^i(a_1)\sum_{a_2}\overline{\chi}^j(a_2)\sum_{a_3}\overline{\chi}^k(a_3)\right. \\
&\quad -\frac{3}{3!}\sum_{a_1}\overline{\chi}^i(a_1)\sum_{a_2}\overline{\chi}^{j+k}(a_2) \\
&\quad \left.+\frac{2}{3!}\sum_{a_1}\overline{\chi}^{i+j+k}(a_1)\right]\tau(\chi^i)\tau(\chi^j)\tau(\chi^k) \\
&= -\frac{1}{d^3}\left(\frac{(d^3-3d^2+2d)}{6}\tau(\chi_0)^3\right. \\
&\quad \left.+\frac{(-3d^2+2d)}{6}\tau(\chi_0)\sum_{j=1}^{d-1}\tau(\chi^j)\tau(\overline{\chi}^j)+\frac{(2d)}{6}\sum\nolimits_3\right)
\end{aligned}
$$

donde

$$\sum_3 = \sum_{\substack{i,j,k=1 \\ i+j+k \equiv 0(d)}}^{d-1} \tau(\chi^i)\tau(\chi^j)\tau(\chi^k)$$

como en esta última sumatoria χ^i, χ^j y $\chi^{i+j} \neq \chi_0$, se tiene la siguiente relación entre sumas de caracteres. Si

$$\pi(\chi^i, \chi^j) = \sum_{x \in \mathbf{F}_p} \chi^i(x)\chi^j(1-x)$$

es la suma de Jacobi asociada a χ^i y χ^j.Entonces

$$\pi(\chi^i, \chi^j) = \frac{\tau(\chi^i)\tau(\chi^j)}{\tau(\chi^{i+j})}$$

de donde se obtiene

$$\sum_3 = \sum_{\substack{i,j=1 \\ i+j \not\equiv 0(d)}}^{d-1} \pi(\chi^i, \chi^j)\tau(\chi^{i+j})\tau(\overline{\chi}^{i+j}) = p\alpha_3^*$$

con

$$\alpha_3^* = \sum_{\substack{i,j=1 \\ i+j \not\equiv 0(d)}}^{d-1} \chi^{i+j}(-1)\pi(\chi^i, \chi^j)$$

Luego

$$\alpha_3 = \frac{1}{6d^2}\left((d^2 - 3d + 2) + (3d-6)p - 2\alpha_3^* p\right)$$

Similarmente se obtiene α_{n+1} en términos de la sumatoria

$$\sum_{n+1} = \sum_{\substack{i_1,\ldots,i_n=1 \\ i_1+\ldots+i_n \not\equiv 0(d)}}^{d-1} \tau(\chi^{i_1})\ldots\tau(\chi^{i_n})\tau(\overline{\chi}^{i_1+\ldots+i_n})$$

Estas sumas son en sí mismas un problema no trivial. Hasta ahora hemos encontrado por este método las ecuaciones de período para $d = 4, 6$ y 8.

Cabe destacar que se obtuvo cada vez los coeficientes α_n en término de parámetros que aparecen en la representación de p, o múltiplos de p, por formas cuadráticas binarias. Mismos parámetros, necesarios y suficientes, que encuentra Dickson en [2].

A continuación presentamos $P_d(x), d = 4, 6$ como ejemplos para $d \mid p-1$, $2d \nmid p-1$:

Teorema 2.2 *Sea p primo tal que $p \equiv 1(4)$, $p \not\equiv 1(8)$. Sea $P_4(X)$ la ecuación de período asociada, entonces*

$$P_4(X) = X^4 + X^3 + \alpha_2 X^2 + \alpha_3 X + \alpha_4$$

donde

$$\alpha_2 = \frac{3+p}{8}$$
$$\alpha_3 = \frac{1+(1+2a)p}{16}$$
$$\alpha_4 = \frac{1+2(1+2a(2-a))p+9p^2}{256}$$

y $a \in \mathbf{Z}$ corresponde a la representación única de p como suma de dos cuadrados

$$p = a^2 + b^2 \qquad \text{con } a \equiv 1(4),\ b \equiv 0(2).$$

Teorema 2.3 *Sea p primo tal que $p \equiv 1(6)$, $p \not\equiv 1(4)$. Sea $P_6(X)$ la ecuación de período asociada, entonces*

$$P_6(X) = X^6 + X^5 + \alpha_2 X^4 + \alpha_3 X^3 + \alpha_4 X^2 + \alpha_5 X + \alpha_6$$

donde

$$\alpha_2 = \frac{5+p}{12}$$
$$\alpha_3 = \frac{1}{3\cdot 6^2}\left[10 + (6(R+1) + 3R' - a)\,p\right]$$
$$\alpha_4 = \frac{1}{2\cdot 6^3}\left[5 + \left(3(R+2)^2 + 2(3R'-a) - 2a^2 - 6\right)p + (6t+5)p^2\right]$$
$$\alpha_5 = \frac{1}{6^4}\left[1 + \left((R+2)(3(R+1)-a^2) - (3(R+1-R') + a + 1)\right)p \right.$$
$$\left. + ((R+2)(3t+1) + 3(R+1-R') + a)\,p^2\right]$$
$$\alpha_6 = \frac{1}{6^6}\left[(3(R+1-R')p + ap - 1)^2 + \left((3t+1)p + 3(R+1) - a^2\right)^2 p\right]$$

y

$$a = 2\,\mathrm{Re}\,\pi$$

$$R = 2\,\mathrm{Re}\,\overline{\chi}(2)\pi = \begin{cases} a & si \quad \chi(2)=1 \\ \dfrac{-a+9b}{2} & si \quad \chi(2)=\rho \\ \dfrac{-a-9b}{2} & si \quad \chi(2)=\overline{\rho} \end{cases}$$

$$R' = 2\,\mathrm{Re}\,\chi(2)\pi = \begin{cases} a & si \quad \chi(2)=1 \\ \dfrac{-a-9b}{2} & si \quad \chi(2)=\rho \\ \dfrac{-a+9b}{2} & si \quad \chi(2)=\overline{\rho} \end{cases}$$

$$t = 2\,\mathrm{Re}\,\chi(2) = \begin{cases} 2 & si \quad \chi(2)=1 \\ -1 & si \quad \chi(2)\neq 1 \end{cases}$$

donde $\rho = \dfrac{-1+i\sqrt{3}}{2}$, χ *es el carácter cúbico definido por* $\chi(\omega)=\rho$ *con* ψ *el carácter y*

$$\pi = \chi(2)\pi(\chi,\psi) = \frac{a+3b\sqrt{-3}}{2}, \text{ con } a \equiv 1(3).$$

Referencias

[1] Canales M. *Higher Levels of Finite Fields*, Tesis doctoral, Facultad de Ciencias, Universidad de Chile, **(1995)**.

[2] Dickson L.E. *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., **57 391-424 (1935)**.

[3] Dickson L.E. *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., **57 463-474 (1935)**.

[4] Dickson L.E. *Cyclotomy and trinomial congruences. Trans.*, Amer. Math. Soc., **37 363-380 (1935)**.

[5] Hasse H. *Vorlesungen über Zahlentheorie*, Springer, **(1964)**.

[6] Ireland K., Rosen M. *A classical introduction to modern number theory*, Springer, **(1990)**.

Dirección del autor:

Instituto de Matemáticas
Facultad de Ciencias. Universidad Austral
Casilla 567, Valdivia
mcanales@valdivia.uca.uach.cl