Leyes de reciprocidad en $\mathbb{F}_q[X]$ y la resolución de congruencias de coeficientes polinomiales

Victor S. Albis[1]

Departamento de Matemáticas
Universidad Nacional de Colombia

José Rafael Huertas[2]

Universidad Distrital, Bogotá

En esta nota se presentan algunos resultados sobre las soluciones de algunos tipos de congruencias de coeficientes polinomiales usando las leyes de reciprocidad en $\mathbb{F}_q[X]$.

Palabras Claves: leyes de reciprocidad, número de soluciones de ecuaciones algebraicas sobre álgebras finitas.

In this note results about the solutions of some congruences with polynomial coefficients using the reciprocity laws in $\mathbb{F}_q[X]$ are proven.

Keywords: Reciprocity laws, number of solutions of algebraic equations over finite algebras.

MSC: 11T55.

[1] vsalbisg@unal.edu.co
[2] jorahus@gmail.com

Introducción

Si K es un cuerpo conmutativo designaremos con $K[X]$ al dominio de los polinomios de coeficientes en K, en la indeterminada X. Ahora bien, existe una analogía entre las aritméticas de los anillos $\mathbb{Z}$ y $\mathbb{F}_q[X]$, donde $\mathbb{F}_q$ es un cuerpo finito de q elementos. En efecto, ambos son euclídeos y, por ende, factoriales, y las nociones de divisibilidad y sus propiedades básicas son esencialmente las mismas. Por esto algunos autores llegan a decir que $\mathbb{Z}$ *y* $\mathbb{F}_{\mathrm{q}}[\mathrm{X}]$ *son dos mundos paralelos*. Es, pues, natural que se estudien en $\mathbb{F}_q[X]$ problemas aritméticos análogos a los estudiados en $\mathbb{Z}$. En particular, *la ley de la reciprocidad cuadrática* no podía escapar a este paralelismo. Por eso vale la pena distinguir estos dos mundos: el primero lo apelaremos el *mundo racional* y al segundo el *mundo polinomial*.

El propósito de esta nota es presentar algunos resultados sobre las soluciones de algunos tipos de congruencias de coeficientes polinomiales usando las leyes de reciprocidad en $\mathbb{F}_q[X]$.

En contraste con el número de demostraciones de la ley de la reciprocidad cuadrática en $\mathbb{Z}$ (de la cual existían hasta hace poco por lo menos 152 demostraciones, 8 de las cuales debidas a Gauss), la historia de las demostraciones de las leyes de reciprocidad en $\mathbb{F}_q[X]$ es muy corta. En efecto, el caso particular $q = p$, primo impar, y $d = 2$, como extensión directa de la clásica ley de reciprocidad cuadrática, lo demostró Dedekind [5] en el año `1857`. El caso $q = p^r$, donde p es un primo arbitrario, y $d = q - 1$ fue demostrado en `1928` por Schmidt [13] y por Carlitz [2, 3] en `1932` y `1933`. En este último trabajo Carlitz indica que su demostración se puede extender al caso general. Ore la demuestra en el caso general en `1934` e indica algunas posibles generalizaciones en un extenso artículo [12]. Finalmente, en `1949` Hasse [7, páginas 100–103] da una demostración donde se requiere un conocimiento previo de resultados básicos de la teoría de cuerpos.

Con el fin de facilitar la lectura, en la sección 1 recordamos, sin demostraciones, algunos resultados previos sobre la estructura y propiedades de los anillos $\mathbb{F}_q[X]/(h(X))$.

En la sección 2 introducimos los análogos del símbolo de Legendre en $\mathbb{F}_q[X]$ y enunciamos y demostramos, siguiendo los lineamientos de Hasse, el teorema que contiene la que podríamos llamar *la versión polinomial de las leyes de reciprocidad*. Y, finalmente, en la sección 3 aplicamos lo anterior para resolver congruencias en $\mathbb{F}_q[X]$ análogas a congruencias clásicas en $\mathbb{Z}$, en el mismo espíritu de la teoría de números.

1 Algunos resultados preliminares

Para la comprensión de lo que sigue suponemos un conocimiento elemental de las nociones básicas de la teoría de anillos y de la teoría de cuerpos:

ideales, homomorfismos, anillos cocientes, teoremas de isomorfía, teorema chino de los restos, polinomios sobre un anillo, derivada de un polinomio, raíces de polinomios, raíces simples de un polinomio, extensiones algebraicas de cuerpos, cuerpos de descomposición, clausura algebraica de un cuerpo, para citar algunas; véanse, por ejemplo, [6, 8, 9, 11].

Escribiremos $A^\times$ para denotar al grupo multiplicativo de los elementos invertibles de un anillo A. En particular, si $A = K$ es un cuerpo, tenemos $K^\times = K \setminus \{0\}$, y si $K = \mathbb{F}_q$ es un cuerpo finito el grupo multiplicativo $K^\times$ tiene $q-1$ elementos y es, además, cíclico [6, pg. 361].

Al conjunto de los polinomios unitarios (mónicos) de coeficientes en $\mathbb{F}_q$ lo designamos con $M(q;X)$, mientras que al conjunto de los polinomios irreducibles y unitarios de coeficientes en $\mathbb{F}_q$ lo designamos con $P(q;X)$. Es claro que todo polinomio de $\mathbb{F}_q[X]$ tiene un único representante en $M(q;X)$ por la relación de equivalencia definida como sigue: $f(x) \sim g(X)$ si existe $a \in \mathbb{F}_q^\times$ tal que $f(x) = a\, g(X)$. En particular, todo polinomio irreducible tiene un único representante en $P(q;X)$. Por otra parte, si $f(x) \sim g(X)$ es fácil ver que $f(X)$ y $g(X)$ generan el mismo ideal: $(f(X)) = (g(X))$. Por estas razones, supondremos, salvo mención expresa contraria, que todos los polinomios de $\mathbb{F}_q[X]$ en consideración pertenecen a $M(q;X)$.

En [6, pgs. 362–365], se encuentran demostrados los resultados contenidos en las siguientes dos proposiciones.

Proposición 1.1. *Sean $\mathbb{F}_q$ y $X^q - X \in \mathbb{F}_p[X]$. Entonces*

(a) *$\alpha^q - \alpha = 0$ para todo $\alpha \in \mathbb{F}_q$;*

(b) *todas las raíces de $X^q - X$ son simples;*

(c) *el conjunto de las raíces de $X^q - X$ es precisamente $\mathbb{F}_q$;*

(d) *$\mathbb{F}_q$ es el cuerpo de descomposición de $X^q - X$ sobre $\mathbb{F}_p$.* ☑

Proposición 1.2. *Sean $\mathbb{F}_q$ un cuerpo finito y $n \geq 1$ un entero. Entonces subsisten las siguientes propiedades*

(a) *en una clausura algebraica Ω de $\mathbb{F}_q$ existe una y sólo una extensión K de $\mathbb{F}_q$ de grado n;*

(b) *$K = \mathbb{F}_q[X]/(p(X))$ donde $p(X) \in P(q;X)$ es de grado n;*

(c) *$K = \mathbb{F}_q(\alpha)$, donde α es la clase de X módulo $p(X)$. Los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, conforman una base de K sobre $\mathbb{F}_q$;*

(d) *K es isomorfo a $\mathbb{F}_{q^n}$ y tiene por lo tanto q^n elementos;*

(e) $p(X) = (X-\alpha)(X-\alpha^q)\cdots(X-\alpha^{q^{n-1}})$. ☑

Ahora bien, si $a(X) \in \mathbb{F}_q[X]$, su clase módulo $p(X)$ se puede escribir en términos de la base 1, α, α^2, $\ldots$, α^{n-1} en la forma

$$a(\alpha) = \beta_0 + \beta_1\alpha + \cdots + \beta_{n-1}\alpha^{n-1}\,,$$

donde cada $\beta_i \in \mathbb{F}_q$. Usando que $\beta^q = \beta$ para todo $\beta \in \mathbb{F}_q$ y que

$$(a + b + \cdots + z)^q = a^q + b^q + \cdots + z^q\,,$$

podemos escribir para $a(X) \in \mathbb{F}_q[X]$

$$a(\alpha)^{q^i} = a(\alpha^{q^i})\,, \tag{1}$$

con $i = 0, 1, \cdots$.

También, para expresar que dos polinomios $a(X)$ y $b(X) \in \mathbb{F}_q[X]$ están en la misma clase módulo el ideal $(h(X))$ escribimos $a(X) \equiv b(X)(\mathrm{mod}\, h(X))$. De modo que si $f(t) \in \mathbb{F}_q[X][t]$, resolver la congruencia $f(t) \equiv 0(\mathrm{mod}\, h(X))$ equivale a resolver la ecuación polinomial $\overline{f}(t) = 0$ donde $\overline{f}(t)$ es el polinomio en $\mathbb{F}_q[X]/(h(X))[t]$ cuyos coeficientes son las clases módulo $(h(X))$ de los coeficientes de $f(t)$.

Si definimos a

$$\Phi(h(X)) = \mathrm{card}\,[\mathbb{F}_q[X]/(h(X))]^\times\,,$$

como el análogo de la *función indicatriz* de Euler en $\mathbb{Z}$, a saber,

$$\varphi(m) = \mathrm{card}(\mathbb{Z}/m\mathbb{Z})^\times \qquad (m > 0)\,.$$

Podemos verificar que en este caso se tiene una *función multiplicativa* Φ definida sobre el monoide $M(q; X)$. Es decir, una función que cumple $\Phi(h(X)g(X)) = \Phi(h(X))\Phi(g(X))$ si m.c.d. $(h(X), g(X)) = 1$. Por otra parte,

$$\mathrm{N}(h(X)) = \mathrm{card}\,[\mathbb{F}_q[X]/(h(X))]\,,$$

se llama la *norma* del polinomio $h(X)$ o si se quiere la norma del ideal $(h(X))$.

Análogamente al caso de los números enteros, un conjunto $r_1(X), \cdots, r_m(X)$ de polinomios en $M(q; X)$ se dice un *sistema completo de restos*

módulo el polinomio $h(X)$ si dado un polinomio $g(X) \in \mathbb{F}_q[X]$ existe un $r_i(X)$ tal que $g(x) \equiv r_i(X) (\mathrm{mod}\, h(X))$.

La estructura del anillo $\mathbb{F}_q[X]/(p(X)^v)$ se encuentra en las siguientes proposiciones [1, 15].

Proposición 1.3. *Sea*

$$p(X) = \pi_0 + \pi_1 X + \cdots + \pi_{m-1} X^{m-1} + X^m \in P(q; X)\,.$$

Si x *designa a la clase de equivalencia de* X *módulo* $(p(X)^v)$*, entonces*

(a) $\mathbb{F}_q[X]/(p(X)^v)$ *es una* $\mathbb{F}_q$*–álgebra de dimensión* $v\,m$ *y* $q^{v\,m}$ *elementos;*

(b) $1, x, \cdots, x^{v\,m-1}$ *es una* $\mathbb{F}_q$*–base de esta álgebra;*

(c) *si* $\theta(a(X)) = \theta(\sum_{k=0}^{s} \alpha_k X^k) := \sum_{k=0}^{s} \alpha_k x^k)$*, entonces* $\theta(p(X)) := z_v$ *cumple las condiciones* $z_v^v = 0, z_v^k \neq 0$ *si* $0 \leq k < v$*;*

(d) *los polinomios unitarios de* $\mathbb{F}_q[X]$ *de grado estrictamente menor que* $v\,m$ *forman un sistema completo de restos módulo* $(p(X)^v)$*;*

(e) *el álgebra* $\mathbb{F}_q[X]/(p(X)^v)$ *contiene un cuerpo* L *isomorfo al cuerpo* $\mathbb{F}_q[X]/(p(X))$ *con el cual lo identificamos;*

(f) *la* L*–dimensión de*

$$\mathbb{F}_q[X]/(p(X)^v) = \{\lambda_0 + \lambda_1 z_v + \cdots + \lambda_{v-1}^{v-1}\,;\, \lambda_i \in L\}\,,$$

es v*, una de cuyas bases (llamada canónica) es precisamente* $1, z_v, \ldots, z_v^{v-1}$. ☑

Proposición 1.4. *El grupo de las unidades de* $\mathbb{F}_q[X]/(p(X)^v)$ *está dado por*

$$L_v^{\times} = L^{\times} \times \{1 + \lambda_1 z_v + \cdots + \lambda_{v-1} z_v^{v-1}\,;\, \lambda_i \in L\}\,.$$

Este grupo tienen orden $\Phi(p(X)^v) = (q^m - 1)q^{m(v-1)}$. ☑

Todo polinomio $g(X) \in \mathbb{F}_q[X]$ tal que $\theta(g(X)) = g(x)$ genere a $L^{\times}$ se dice una *raíz primitiva módulo* $p(X)$. Esto equivale a decir que dado $a(X) \in \mathbb{F}_q[X]$ existe un entero b tal que $a(X) \equiv g(X)^b (\mathrm{mod}\, p(X))$.

Utilizando los anteriores resultados y la versión polinomial del teorema chino de los restos, es posible calcular efectivamente $\mathrm{N}(h(X))$ y $\Phi(h(X))$ para todo $h(X) \in \mathbb{F}_q[X]$.

Por otra parte, es posible demostrar que la clase de $a(X) \in \mathbb{F}_q[X]$ es invertible módulo $h(X)$ si y sólo si $\mathrm{m.\,c.\,d.}(a(X), h(X)) = 1$ (la demostración sigue el modelo de la demostración del resultado análogo en $\mathbb{Z}$). Podemos, pues, escribir la siguiente proposición.

Proposición 1.5. *Si $h(X) \in M(q; X)$ y $p(X) \in P(q; X)$, entonces*

(a) Generalización del teorema de Euler. $a(X)^{\Phi(h(X))} \equiv 1 (\mathrm{mod}\, h(X))$ *si* $\mathrm{m.\,c.\,d.}(a(X), h(X)) = 1$*;*

(b) Generalización del pequeño teorema de Fermat.

$$a(X)^{q^d - 1} \equiv 1 (\mathrm{mod}\, p(X))\,,$$

si $p(X) \nmid a(X)$. ☑

Finalizamos esta sección con dos definiciones y una proposición, las cuales usaremos luego.

Sea L/K una extensión de cuerpos finitos de grado $[L : K] = n$. Entonces si $|K| = p^m$, tenemos $|L| = p^{mn}$. Si $\alpha \in L$ definimos la *traza* de α sobre K por la relación

$$\mathrm{tr}_{L/K}(\alpha) := \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \in K\,.$$

La traza $\mathrm{tr}_{L/K} : L \to K$ es una aplicación K–lineal. También definimos la *norma* de α sobre K por la relación

$$\mathrm{n}_{L/K}(\alpha) := \alpha\alpha^q \cdots \alpha^{q^{n-1}} \in K\,.$$

Estas definiciones contienen el hecho de que tanto $\mathrm{tr}_{L/K}(\alpha)$ como $\mathrm{n}_{L/K}(\alpha)$ son elementos de K (para estos hechos, véanse, por ejemplo, [1, 10]).

Para finalizar es sección enunciamos sin demostración la siguiente proposición [14].

Proposición 1.6. *Sea $L/\mathbb{F}_q$ una extensión de grado n y $\alpha \in L$. Entonces el polinomio $X^q - X - \alpha \in L[X]$ tiene una solución en L si y sólo si* $\mathrm{tr}_{L/\mathbb{F}_q}(\alpha) = 0$. ☑

2 Versión polinomial del símbolo de Legendre

La exposición que sigue la hemos tomado esencialmente de [7, pgs. 100–103]. Empezamos con la siguiente proposición que generaliza el *criterio de Euler* del caso racional.

Proposición 2.1. *Sea d un entero positivo. Si $q \equiv 1 (\mathrm{mod}\, d)$, entonces la sucesión*

$$1 \to (\mathbb{F}_{q^r}^{\times})^{(d)} \to \mathbb{F}_{q^r}^{\times} \stackrel{w}{\to} \boldsymbol{\mu}_d \to 1\,,$$

donde $(\mathbb{F}_{q^r}^{\times})^{(d)} = \{\alpha^d\,;\, \alpha \in \mathbb{F}_{q^r}^{\times}\}$, $\boldsymbol{\mu}_d$ es el grupo multiplicativo de las raíces d–ésimas de la unidad contenidas en $\mathbb{F}_{\mathrm{q}}$ y $w(\alpha) = \alpha^{(q^r-1)d}$, es exacta.

Demostración. Claramente ω es un homomorfismo de grupos con valores en $\boldsymbol{\mu}_d$, pues $w(\alpha)^d = 1$. Sea Ω una clausura algebraica de $\mathbb{F}_{q^r}$. Dado $\alpha \in \mathbb{F}_{q^r}^{\times}$, existe $\beta \in \Omega$ tal que $\beta^d = \alpha$. Ahora bien, $\alpha \in \ker w$ $\Leftrightarrow$ $\alpha^{(q^r-1)/d} = 1 = \beta^{q^r-1} \Leftrightarrow \beta \in (\mathbb{F}_{q^r}^{\times})^{(d)}$. Es decir, $(\mathbb{F}_{q^r}^{\times})^{(d)} = \ker w$. Finalmente, dado $\alpha \in \boldsymbol{\mu}_d$ existe $\beta \in \Omega$ tal que $\beta^{(q^r-1)/d} = \alpha$. Como $\alpha^d = \beta^{q^r-1} = 1$, vemos que $\beta \in \mathbb{F}_{q^r}^{\times}$, es decir, existe $\beta \in \mathbb{F}_{q^r}^{\times}$ tal que $w(\beta) = \alpha$. ☑

La función w se extiende a todo $\mathbb{F}_{q^r}$ haciendo $w(0) = 0$.

Veamos por qué hemos dicho que esta proposición generaliza el criterio de Euler. Si tomamos $p(X) \in P(q; X)$, de grado r, entonces $L = \mathbb{F}_{q^r} = \mathbb{F}_q[X]/(p(X))$. Si $d \mid q-1$, y escribimos $w_{P(X)}$ en la anterior sucesión exacta en vez de w, definimos

$$(- \mid p(X))_d := w_{P(X)}\,,$$

como el *d–símbolo de Legendre*. Podemos entonces escribir el criterio de Euler como

$$(a(X) \mid p(X))_d \equiv \begin{cases} a(X)^{(N(p(X))-1)/d} (\mathrm{mod}\, p(X)) & \text{si} \quad p(X) \nmid a(X)\,, \\ 0\,(\mathrm{mod}\, p(X)) & \text{si} \quad p(X) \mid a(X)\,. \end{cases}$$

Como $(- \mid p(X))_d$ es un homomorfismo, resulta que

(i) $(a(X)b(X) \mid p(X))_d = (a(X) \mid p(X))_d (b(X) \mid p(X))_d$;

(ii) $(1 \mid p(X))_d = 1$;

(iii) si $\alpha \in \mathbb{F}_q[X]^\times = {\mathbb{F}_q}^\times$, entonces $(\alpha \mid p(X)) = \alpha^{N(p(X))-1)/d} \in \boldsymbol{\mu}_d$, puesto que $p(X) \nmid \alpha$. Aquí $\boldsymbol{\mu}_d$ designa al grupo de las raíces d–ésimas de la unidad contenidas en ${\mathbb{F}_q}^\times$.

El resultado (iii) corresponde a una única *ley suplementaria de reciprocidad* como análoga a las leyes suplementarias de la reciprocidad cuadrática en $\mathbb{Z}$.

Tenemos el siguiente *teorema de reciprocidad* para el d–símbolo de Legendre.

Proposición 2.2. *Sean $p(X), g(X) \in P(q;X)$, de grados r y t, respectivamente. Si $d \mid q-1$, entonces*

$$\big(g(X) \mid p(X)\big)_d = (-1)^{rt(q-1)/d}\big(p(X) \mid g(X)\big)_d\,.$$

En particular, si $p = 2$ tenemos

$$\big(g(X) \mid p(X)\big)_d = (-1)^{rt}\big(p(X) \mid g(X)\big)_d\,.$$

Demostración. Sea Ω una clausura algebraica de $\mathbb{F}_q$, en la cual

$$p(X) = (X-\alpha)(X-\alpha^q)\cdots(X-\alpha^{q^{r-1}})\,,$$

y sea $L = \mathbb{F}_q(\alpha) = \mathbb{F}_q[X]/(p(X)) \subset \Omega$. En $L[X]$ podemos definir el símbolo de Legendre

$$\big(a(X) \mid (X-\alpha)\big)'_d \equiv a(X)^{[N(X-\alpha)-1]/d} (\mathrm{mod}\, X-\alpha)\,.$$

Como $N(X-\alpha) = q^r$ en L, vemos que

$$\big(a(X) \mid (X-\alpha)\big)'_d \equiv a(X)^{(q^r-1)/d} (\mathrm{mod}\, X-\alpha)\,.$$

Pero

$$\big(a(X) \mid p(X)\big)_d \equiv a(X)^{(q^r-1)/d} (\mathrm{mod}\, p(X))\,,$$

implica que

$$\big(a(X) \mid p(X)\big)_d \equiv a(X)^{(q^r-1)/d} (\mathrm{mod}(X-\alpha)\,.$$

Luego

$$\big(a(X) \mid (X-\alpha)\big)'_d = \big(a(X) \mid p(X)\big)_d\,.$$

Por otra parte, si $a(X) \in \mathbb{F}_{\mathrm{q}}[\mathrm{X}]$, designemos con $a(\alpha)$ su clase módulo $p(X)$, de modo que $a(\alpha) \in L$. Pero $a(\alpha) = a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}$, $a_j \in \mathbb{F}_{\mathrm{q}}$, de modo que $a(\alpha)^{q^i} = a_0 + a_1\alpha^{q^i} + \cdots + a_{r-1}\alpha^{q^i(r-1)}$, pues $a_j^{q^i} = a_j$ ya que $a_j \in \mathbb{F}_{\mathrm{q}}$. Por lo tanto, en L

$$\begin{aligned}\big(a(X) \mid (X-\alpha)\big)'_d &= a(\alpha)^{(q^r-1)/d} = a(\alpha)^{[(q^r-1)/(q-1)][(q-1)/d]} \\ &= a(\alpha)^{(1+q+\cdots+q^{r-1})(q-1)/d} \\ &= \Big[a(\alpha)\, a(\alpha^q) \cdots a(\alpha^{q^{r-1}})\Big]^{(q-1)/d}\,.\end{aligned}$$

De aquí resulta que en L

$$\big(a(X) \mid p(X)\big)_d = \Big[a(\alpha)\, a(\alpha^q) \cdots a(\alpha^{q^{r-1}})\Big]^{(q-1)/d}\,, \tag{2}$$

donde α, α^q, $\ldots$, $\alpha^{q^{r-1}}$ son las raíces de $p(X)$. Pero

$$a(\alpha)\, a(\alpha^q) \cdots a(\alpha^{q^{r-1}}) = a(\alpha)\, a(\alpha)^q \cdots a(\alpha)^{q^{r-1}} = \mathrm{n}_{L/\,\mathbb{F}_{\mathrm{q}}}(a(\alpha)) \in \mathbb{F}_{\mathrm{q}}\,.$$

Luego (8) es válida en $\mathbb{F}_{\mathrm{q}}$. Sea ahora

$$g(X) = (X-\beta)(X-\beta^q)\cdots(X-\beta^{q^{t-1}})\,,$$

la descomposición de $g(X)$ en $\Omega[X]$, si $g(X) \in P(q;X)$. Entonces

$$\begin{aligned}\big(g(X) \mid p(X)\big)_d &= \prod_{i=0}^{r-1} g(\alpha^{q^i})^{(q-1)/d} = \prod_{i=0}^{r-1}\prod_{j=0}^{t-1} (\alpha^{q^i} - \beta^{q^j})^{(q-1)/d} \\ &= (-1)^{rt(q-1)/d}\big(p(X) \mid g(X)\big)_d\,. \qquad \boxtimes\end{aligned}$$

La demostración anterior es distinta a la dada en [2] por Carlitz.

En particular, si tomamos $d = 2$ y $q = p$ un primo impar, obtenemos el resultado de reciprocidad cuadrática demostrado por Dedekind en 1857 [5], a saber,

$$\big(g(X) \mid p(X)\big)_2 = (-1)^{rt(p-1)/2}\big(p(X) \mid g(X)\big)_2 .$$

El caso $d = q - 1$

$$\big(g(X) \mid p(X)\big)_{q-1} = (-1)^{rt}\big(p(X) \mid g(X)\big)_{q-1} ,$$

fue demostrado en 1928 por Schmidt [13] y por Carlitz en 1932 y 1933 [2, 3].

En [2] Carlitz generaliza $\big(- \mid p(X)\big)_{q-1}$ a un *símbolo de Jacobi*. Si

$$f(X) = p_1(X) \cdots p_s(X) \in M(q\,; X) ,$$

es la descomposición de $f(X)$ en irreducibles $p_j(X) \in P(q; X)$ (cada uno de ellos aparece repetido según su multiplicidad), definimos el d–símbolo de Jacobi por la expresión

$$\left(\frac{a(X)}{f(X)}\right)_d := \left(\frac{a(X)}{p_1(X)}\right)_d \cdots \left(\frac{a(X)}{p_s(X)}\right)_d .$$

Ahora bien, si

$$g(X) = q_1(X) \cdots q_t(X) \in M(q\,; X) ,$$

es la descomposición canónica de $g(X)$, y hacemos $\alpha_i = \text{grado}(p_i(X))$ y $\beta_j = \text{grado}(q_j(X))$, vemos que

$$\begin{aligned}\left(\frac{g(X)}{f(X)}\right)_d &= \prod_{j=1}^{t}\prod_{i=1}^{s}\left(\frac{q_j(X)}{p_i(X)}\right)_d = \prod_{j=1}^{t}\prod_{i=1}^{s}(-1)^{\alpha_i\beta_j(q-1)/d}\left(\frac{p_i(X)}{q_j(X)}\right)_d \\ &= (-1)^{(\alpha_1+\cdots+\alpha_s)(\beta_1+\cdots+\beta_t)(q-1)/d}\left(\frac{f(X)}{g(X)}\right)_d .\end{aligned}$$

Como $\text{grado}(f(X)) = m = \sum_i \alpha_i$ y $\text{grado}(g(X)) = n = \sum_j \beta_j$, obtenemos

$$\left(\frac{g(X)}{f(X)}\right)_d = (-1)^{mn(q-1)/d} \left(\frac{f(X)}{g(X)}\right)_d ,$$

que podemos considerar como expresión de las leyes de reciprocidad para el d–símbolo de Jacobi.

3 Sobre la solubilidad de algunas congruencias

En esta sección utilizaremos lo expuesto anteriormente para dar condiciones necesarias y suficientes sobre la solubilidad de algunas congruencias en $\mathbb{F}_q[X]$. Los resultados son análogos de resultados conocidos en el caso de $\mathbb{Z}$.

Empezamos con la siguiente proposición.

Proposición 3.1. *Sean $p(X) \in P(q;X)$, de grado n, $a(X) \in \mathbb{F}_q[X]$, tales que* m.c.d.$(a(X), p(X)) = 1$. *Si $d \mid q-1$, entonces la congruencia*

$$t^d \equiv a(X) (\mathrm{mod}\, p(X)) ,$$

es soluble si y sólo si $\left(\frac{a(X)}{p(X)}\right)_d = 1$.

Demostración.

(⇒) Sea $t(X)$ una solución de la congruencia dada. Entonces $p(X) \nmid a(X)$, por hipótesis. Por el teorema de Fermat (Proposición 1.5, (b)), tenemos

$$a(X)^{(q^n-1)/d} \equiv (t(X)^d)^{(q^n-1)d} \equiv t(X)^{q^n-1} \equiv 1 (\mathrm{mod}\, p(X)) ,$$

lo cual muestra que $\left(\frac{a(X)}{p(X)}\right)_d = 1$.

(⇐) Recíprocamente, tomemos una raíz primitiva $g(X)$ módulo $p(X)$, de modo que

$$a(X) \equiv g(X)^b (\mathrm{mod}\, p(X)) , \quad b \quad \text{entero} .$$

Como, por hipótesis, $\left(\frac{a(X)}{p(X)}\right)_d = 1$, obtenemos

$$a(X)^{(q^n-1)/d} \equiv g(X)^{b(q^n-1)/d} \equiv 1(\mathrm{mod}\, p(X))\,.$$

Esto implica que $q^n - 1$ divide a $b(q^n - 1)/d$ (por el teorema de Lagrange para los grupos finitos) y, por lo tanto, $d \mid b$, es decir, $b = kd$ para algún entero k. Es claro ahora que $t(X) = g(X)^k$ es una solución de la congruencia dada. ☑

Proposición 3.2. *Sea $m \geq 1$ un entero, $p(X) \in P(q; X)$, de grado n y $d = \mathrm{m.c.d.}(m, q^n - 1)$. Entonces la congruencia $t^m \equiv a(X)(\mathrm{mod}\, p(X))$ tiene d soluciones si y sólo si $\left(\dfrac{a(X)}{p(X)}\right)_d = 1$.*

Demostración. Sea $g(X)$ una raíz primitiva módulo $p(X)$. Podemos escribir entonces $a(X) \equiv g(X)^b(\mathrm{mod}\, p(X))$ y $t(X) \equiv g(X)^y(\mathrm{mod}\, p(X))$.

($\Rightarrow$) Sea $t(X)$ una solución de la congruencia dada. Es claro que $p(X) \nmid t(X)$, luego, por el teorema de Fermat (proposición 1.5, (b)),

$$(t(X)^{m/d})^{q^n-1} \equiv 1(\mathrm{mod}\, p(X))\,.$$

Pero entonces

$$\begin{aligned} a(X)^{(q^n-1)/d} &\equiv (t(X)^m)^{(q^n-1)/d} \equiv (t(X)^{m/d})^{q^n-1} \\ &\equiv 1 \bmod p(X))\,, \end{aligned} \tag{3}$$

lo cual significa que $\left(\dfrac{a(X)}{p(X)}\right)_d = 1$.

($\Leftarrow$) Recíprocamente, la congruencia $t^m \equiv a(X)(\mathrm{mod}\, p(X))$ es equivalente a la congruencia $my \equiv b(\mathrm{mod}\, q^n - 1)$, la cual, por un teorema clásico de la teoría de números es soluble si y sólo si $d \mid b$, en cuyo caso hay exactamente d soluciones. Si ahora $\left(\dfrac{a(X)}{p(X)}\right)_d = 1$, tenemos

$$a(X)^{(q^n-1)/d} \equiv 1(\mathrm{mod}\, p(X))\,,$$

y entonces

$$a(X)^{(q^n-1)/d} \equiv (g(X)^b)^{(q^n-1)/d} \equiv g(X)^{b(q^n-1)/d}) \equiv 1(\mathrm{mod}\, p(X))\,.$$

Esto implica que q^n-1 divide a $b(q^n-1)/d$, lo cual fuerza a que $d \mid b$, lo cual, a su vez, es equivalente a la solubilidad de la congruencia propuesta. ☑

Consideremos ahora la congruencia

$$t^q - t \equiv a(X)(\mathrm{mod}\, p(X))\,, \tag{4}$$

donde $a(X) \in \mathbb{F}_q[X]$, $p(X) \in P(q;X)$ y grado$(p(X)) = n$. La siguiente proposición contiene una condición necesaria y suficiente para que esta congruencia sea soluble.

Proposición 3.3. *Sea* $L = \mathbb{F}_q[X]/p(X))$. *La congruencia* (3) *es soluble en* $\mathbb{F}_q[X]$ *si y sólo si* $\mathrm{tr}_{L/\mathbb{F}_q}(a(X)) \equiv 0(\mathrm{mod}\, p(X))$.

Demostración. Es una consecuencia inmediata de la proposición 1.6. ☑

Pero en [4] se encuentra la siguiente proposición.

Proposición 3.4. *Sean*

$$p(X) = c_0 + c_1X + \cdots + X^n \in P(q;X)\,,$$

y

$$p'(X) = c_1 + 2c_2X + \cdots + nX^{n-1}\,.$$

Si

$$p'(X)a(X) \equiv b_0 + b_1X + \cdots + b_{n-1}X^{n-1}(\mathrm{mod}\, p(X)) \quad b_i \in \mathbb{F}_q\,,$$

entonces $\mathrm{tr}_{L/\mathbb{F}_q}(a(X)) \equiv b_{n-1}(\mathrm{mod}\, p(X))$.

Combinando las dos anteriores proposiciones, encontramos otro criterio de solubilidad de la congruencia (3).

Proposición 3.5. *Si* grado$(p(X)) = n$, *la congruencia* (3) *es soluble si y sólo si* $p'(X)a(X)$ *es congruente módulo* $p(X)$ *a un polinomio de grado estrictamente menor que* $n-1$. ☑

Bibliografía

[1] V. S. Albis, *Lecciones sobre la aritmética de polinomios* (Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, 1999).

[2] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Am. J. Math. **54**, 39 (1932).

[3] L. Carlitz, *On a theorem of higher reciprocity*, Bull. Am. Math. Soc. **39**, 155 (1933).

[4] L. Carlitz, *A theorem on higher congruences*, Bull. Am. Math. Soc. **41**, 844 (1935).

[5] R. Dedekind, *Abriss einer Theorie der höheren Congruenzen in Bezug aus einer reellen Primzahl–Modulus*, J. f. d. reine u. angew. Math. **54**, 1 (1857).

[6] P. Dubreil & M. L. Dubreil–Jacotin, *Leçons d'algèbre moderne* (Dunod, Paris, 1961).

[7] H. Hasse, *Zahlentheorie* (1949, 1969); *Number Theory* (Springer–Verlag, Berlin, 1980).

[8] I. N. Herstein, *Topics in Algebra* (Blaisell Pub. Co., New York, 1964).

[9] Thomas W. Hungerford, *Algebra* (Springer–Verlag, New York, 1980).

[10] K. Ireland & M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer–Verlag, New York, 1982).

[11] S. Lang, *Algebra* (Addison–Wesley, Reading MA, 1984).

[12] O. Ore, *Contributions to the theory of finite fields*, Trans. Am. Math. Soc. **36**, 243 (1934).

[13] F. K. Schmidt, *Zahlentheorie in Körpern von der Charakteristik p*, Erlangen Sitzungsberichte **58–59**, 159 (1928).

[14] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lect. Notes Math. **536** (Springer–Verlag, Berlin, 1976).

[15] T. H. M. Smits, *On the group of units of* $\mathrm{GF}(q)[x]/(a(x))$, Indag. Math. **44**, 335 (1982).

[16] I. M. Vinogradov, *Fundamentos de la Teoría de los Números* (Mir, Moscú, 1971).