CUERPOS FINITOS. ALGORITMO DE BERLEKAMP

¿Cómo factorizar polinomios sobre cuerpos finitos ?

ugr Universidad de Granada

Enrique R. Aznar

Dpto. de Álgebra

ugr Universidad de Granada

Enrique R. Aznar

Dpto. de Álgebra

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

1. Cuerpos finitos

Sabemos que las clases de resto, $\mathbb{Z}_p$ módulo un entero p, tiene estructura de cuerpo si y sólo si p es primo. En lo que sigue, estudiamos cuerpos finitos.

Como $x^p - x = x(x-1)\cdots(x-(p-1)) \pmod{p}$ ya que el polinomio diferencia tiene grado menor que p pero admite p raíces módulo p. Tiene que ser idénticamente cero porque un polinomio no nulo con coeficientes en un cuerpo no puede tener mas raíces que las que indica su grado.

Por tanto, el cuerpo $\mathbb{Z}_p$ está formado por las p raíces $0, 1 \ldots, p-1 \pmod{p}$ y es el menor cuerpo que las contiene. O sea, $\mathbb{Z}_p$ es el cuerpo de descomposición de $f(x) = x^p - x \in \mathbb{Z}_p[x]$. También es el cuerpo de descomposición de $x^{p-1} - 1$ y de cualquier polinomio ciclotómico de orden p en $\mathbb{Z}_p[x]$. Como cualquier cuerpo de descomposición es único salvo isomorfía.

Como todo cuerpo K finito, satisface que $n \cdot 1 = m \cdot 1 \Leftrightarrow (m-n) \cdot 1 = 0$ para ciertos naturales $n < m$, existe el mínimo $p \in \mathbb{N}$ tal que $p \cdot 1 = 0$ y necesariamente es primo porque si no $(n \cdot 1)(m \cdot 1) = 0$ y si $m \cdot 1 \neq 0$, multiplicando por su inverso se tiene $n \cdot 1 = 0$ contradiciendo la mínimalidad. Así, si K finito

Lema 1. *K tiene característica p primo y contiene una copia de $\mathbb{Z}_p$.*

Como $Z_p \subset K$, todo cuerpo finito es un Z_p-esp. vect. Si la dimensión es $[K : \mathbb{Z}_p] = n$. Entonces, su tamaño es $|K| = p^m$. Además, claramente

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Página web personal
Página de Abertura
Contenido
Página 4 de 21
Atrás
Pantalla grande/pequeña
Cerrar

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Teorema 1. *Si $K \subset F$ cuerpos finitos. Entonces, $|F| = q^m$, donde $m = [F : K]$. En particular, $|K| = q = p^n$ con $p = car(K) = car(F)$.*

Podemos construir cuerpos finitos partiendo de $\mathbb{Z}_p$ adjuntando raíces de polinomios. O sea, si $f(x) \in \mathbb{Z}_p[x]$ es irreducible el cociente $K = \mathbb{Z}_p[x]/(f(x))$ es un cuerpo[1] y claramente su tamaño es $|K| = p^m$ donde $m = \text{gr}(f(x))$.

Veremos mas adelante que existen polinomios irreducibles de cualquier grado con coeficientes en $\mathbb{Z}_p[x]$. De momento vemos algunos resultados previos.

Lema 2. *Si F es un cuerpo y $|F| = q$. Todo $a \in F$ satisface $a^q = a$.*

Demostración: $0^q = 0$. Y si $a \neq 0$, como $F^* = F - \{0\}$ es un grupo multiplicativo, por el teorema de Lagrange, $a^{p-1} = 1$ y multiplicando por a, $a^q = a$.

Lema 3. *Si F es un cuerpo, $|F| = q$ y $K \subset F$ subcuerpo. Entonces, F es el cuerpo de descomposición de $f(x) = x^q - x$ sobre K y factoriza como*

$$x^q - x = \prod_{a \in F} (x - a)$$

Demostración: Por el lema anterior, $x^q - x$ tiene por raíces los q elementos de F. También el segundo miembro $\prod_{a \in F}(x - a)$. Luego también su diferencia que tiene grado menor que q pero si es no nulo no puede tener mas raíces que su grado. Contradicción que demuestra la igualdad.

[1] $Z_p[x]$ es un DE y todo ideal primo es maximal.

Eso demuestra que F es el menor cuerpo que contiene a todas esas raíces y es el cuerpo de descomposición de $f(x)$. $\square$

Ahora, estamos en condiciones de demostrar el

Teorema 2. ***de existencia y unicidad de c.f.*** *Para cada primo p y cada n existe un con p^n elementos. Y cualquiera es isomorfo al c.d. de $x^{p^n} - x$.*

Demostración: Para la existencia: tomamos $q = p^n$ y el polinomio $x^q - x \in \mathbb{Z}_p[x]$. Su derivada es $qx^{q-1} - 1 \equiv 1 \pmod{p}$. Por tanto, no tiene raíces en ningún cuerpo y $x^q - x$ tiene todas sus raíces simples.

Las q raíces están en su cuerpo de descomposición F sobre $\mathbb{Z}_p$. Pero el conjunto $S = \{a \in F : \ a^q - a = 0\}$ tiene estructura de cuerpo porque si $a, b \in S$

$$\left.\begin{array}{l}(a-b)^q \equiv a^q - b^q = a - b \pmod{p} \Longrightarrow a - b \in S \\ \text{Si } b \neq 0,\ (ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1} \Longrightarrow ab^{-1} \in S\end{array}\right\} \Longrightarrow F = S$$

Para la unicidad: Si $|F| = q = p^n$ entonces por 1, $p = car(F)$. Contiene una copia de $\mathbb{Z}_p$ y es el c.d. de $x^q - x$ sobre $\mathbb{Z}_p$. La unicidad es consecuencia de la unicidad salvo isomorfismos de los cuerpos de descomposición. $\square$

Por lo visto hasta aquí, toda extensión $K \subset F$ de c.f. es una extensión separable y normal ya que es el c.d. de un polinomio con raíces simples y contiene a todas las raíces. Por tanto, es una extensión de Galois. En particular, $K/\mathbb{Z}_p$ lo es si $|K| = p^n$ y por la unicidad que acabamos de ver tiene sentido la

Definición 1. *Si $|K| = q = p^n$, lo denotamos $K = GF(q)$ o a veces $K = F_q$.*

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Teorema 3. ***Criterio de subcuerpo*** *Si F_q es un c.f. con $q = p^n$ elementos. Todo subcuerpo suyo tiene orden p^m con m divisor de n. Recíprocamente, para cada divisor m existe un único subcuerpo de orden p^m.*

Demostración: Todo subcuerpo de F_q tiene la misma característica p. Luego su orden es p^m para algún m. Como F_q es un esp. vect. sobre el subcuerpo que a su vez es un esp. vect. sobre $\mathbb{Z}_p$. El producto de sus dimensiones es n.

Recíprocamente, si m es un divisor de n, $x^m - 1$ divide a $x^n - 1$. Sustituyendo $p^m - 1$ es un divisor de $p^n - 1$. Y de nuevo, $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$. Por tanto, $x^{p^m} - x$ divide a $x^{p^n} - x$ y cada raíz del primero es también una raíz del segundo. O sea, el c.f., F_{p^m}, es un subcuerpo de $F_{p^n} = F_q$.

Finalmente, si hubiera mas de una copia de F_{p^m} en F_q, el polinomio $x^{p^m} - x \in \mathbb{Z}_p[x]$ tendría mas raíces de las que indica su grado. $\square$

Corolario 1. *El retículo de subcuerpos de F_{p^n} es isomorfo al retículo de divisores positivos de $n \in \mathbb{N}$.*

Ejemplo 1. *$F_{2^{15}}$ tiene sólo dos subcuerpos propios que son F_{2^3} y F_{2^5}.*

Dado F_q, denotamos por $F_q^* = F_q - \{0\}$ a su grupo multiplicativo. Entonces

Teorema 4. *Dado un c.f., su grupo multiplicativo F_q^* es cíclico.*

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Demostración: Como $F_2^* = \{1\}$, suponemos $3 \le q$. Sea $h = q-1 = p_1^{e_1} \cdots p_r^{e_r}$ su descomposición en primos. Ahora, para cada i, $x^{h/p_i} - 1$ tiene como máximo h/p_i raíces en F_q^*.

Como $h/p_i < h$, existe al menos un $0 \ne a_i \in F_q$ tal que a_i no es raíz del polinomio $x^{h/p_i} - 1$. Definimos $b_i = a_i^{h/p_i^{e_i}}$. Por tanto, su orden es

$$\left.\begin{array}{l} b_i^{p_i^{e_i}} = a_i^h = 1 \\ b_i^{p_i^{e_i-1}} = a_i^{h/p_i} \ne 1 \end{array}\right\} \Longrightarrow O(b_i) = p_i^{e_i}$$

Ahora su producto $b = b_1 \cdots b_r$ tiene orden multiplicativo $h = q-1$ ya que en caso contrario sería un divisor propio de h y por tanto divisor de alguno de los exponentes, suponemos el primero $h/p_1^{e_1}$. Pero entonces

$$1 = b^{h/p_1} = b_1^{h/p_1} \cdots b_r^{h/p_r} = b_1^{h/p_1}$$

lo que es una contradicción. Y F_q^* es cíclico con generador b. $\square$

Definición 2. *Llamamos* ***elemento primitivo*** *a cualquier generador de* F_q^*.

Como los generadores de un grupo cílclico $C_n = \langle b \rangle$, son b^k con $(n,k) = 1$. El número de elementos primitivos en un c.f., F_q, es $\phi(q-1)$[2].

Teorema 5. *Toda una extensión de c.f.,* $F_q \subset F_r$*, es una extensión simple.*

[2] ϕ es la función de Euler.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Demostración: Claramente F_r es el menor cuerpo que contiene a b y a F_q con b cualquier elemento primitivo de F_r. O sea, $F_r = F_q(b)$. $\square$

Corolario 2. *Para cualquier c.f., F_q, y cualquier $m \in \mathbb{N}$ existe un polinomio irreducible $f(x) \in F_q[x]$ de grado m.*

Demostración: Si $q = p^n$, tomamos $r = q^m = p^{nm}$. Entonces, F_r/F_q es una extensión de grado $[F_r : F_q] = m$. Por el teorema anterior, si b es cualquier elemento primitivo de F_r, $F_r = F_q(b)$.

Entonces una base de F_r sobre F_q está formada por $1, b, \ldots, b^{m-1}$ y el polinomio mínimo de b sobre F_q, $f x) = Irr_{F_q}(b) \in F_q[x]$ tiene grado m. $\square$

Ejemplo 2. *En $Z_2[x]$ hay 4 polinomios mónicos de grado 2, de los cuales sólo uno $f(x) = x^2 + x + 1$ es irreducible porque ni 0 ni 1 son raíces en $\mathbb{Z}_2$. Por tanto, el anillo cociente $F = \mathbb{Z}_2[x]/(f(x))$ es un c.f. De hecho tiene 2^2 elementos porque hay sólo 4 clases de polinomios módulo $x^2 + x + 1$ que son las clases de $0,\ 1,\ x,\ x+1$. O sea, $F = F_4$ es el menor c.f. después de $\mathbb{Z}_2$.*

$$F_4 = \{\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1}\}$$

Su grupo aditivo es $(F_4, +) \cong C_2 \times C_2$ y su multiplicativo es cíclico

$$\left.\begin{array}{l} x^2 \equiv x + 1 \pmod{f(x)} \\ x^3 \equiv x^2 + x \equiv 1 \pmod{f(x)} \end{array}\right\} \Longrightarrow F_4^* \cong C_3$$

Lo que hace que no sea isomorfo al anillo $\mathbb{Z}_4$ cuyo grupo multiplicativo es un C_2. O sea, F_4 y $\mathbb{Z}_4$ son el c.f. y el a.f. más pequeños que existen.

Enrique R. Aznar
Dpto. de Álgebra

2. Raíces de polinomios irreducibles

Si $f(x) \in F_q[x]$ es un polinomio irreducible y $\alpha \in F_r$ con $F_q \subset F_r$ y $f(\alpha) = 0$. Ambos c.f. tienen la misma caraterística, $f(x)$ está asociado al $\mathrm{Irr}_{F_q}(\alpha)$ y

$$h(\alpha) = 0 \Longleftrightarrow f(x)|h(x) \text{ para todo } h(x) \in F_q[x]$$

En particular, como $\alpha^{r-1} = 1$, α es raíz del polinomio $x^r - x$ que tiene coeficientes en cualquier cuerpo y por lo anterior $f(x)|x^r - x$. Además,

Lema 4. *Si $f \in F_q[x]$ irreducible y $gr(f) = m$, $f(x)|x^{q^n} - x$ si y sólo si $m|n$*

Demostración: Si $f(x)|x^{q^n} - x$ y α es una raíz de $f(x)$ en su cuerpo de descomposición entonces $\alpha^{q^n} - \alpha = 0$ y α es un elemento de F_{q^n}.

Pero entonces $F_q \subset F_q(\alpha) \subset F_{q^n}$. Como los grados son multiplicativos y $[F_q(\alpha) : F_q] = \mathrm{gr}(f) = m$, se tiene que $m|n$.

Recíprocamente, si $m|n$, por el criterio de subcuerpo 3, $F_{q^m} \subset F_{q^n}$ y por la unicidad de los c.f. para toda raíz de $f(x)$ en su c.d. se tiene $F_q(\alpha) = F_{q^m}$, $\alpha \in F_{q^m}$ y $\alpha^{q^n} - \alpha = 0$. Luego $f(x)|x^{q^n} - x$ como queremos. $\square$

Teorema 6. *Si $f \in F_q[x]$ irreducible y $gr(f) = m$. Entonces, tiene una raíz $\alpha \in F_{q^m}$ y todas sus raíces $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}} \in F_{q^m}$ son simples.*

Página web personal
Página de Abertura
Contenido
Página 10 de 21
Atrás
Pantalla grande/pequeña
Cerrar

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Demostración: Por lo anterior, $F_q(\alpha) = F_{q^m}$ y si $f(x) = a_m x^m + \cdots + a_0 \in F_q[x]$. Como $a_i^q = a_i$ para todo $i = 0, \ldots, m-1$, se tiene

$$f(\alpha) = 0 \Longrightarrow 0 = f(\alpha)^q = a_m^q \alpha^{qm} + \cdots + a_0^q = f(\alpha^q)$$

repitiendo el proceso $f(\alpha^{q^i}) = 0$ para todo $i = 0, \ldots, m-1$. Ahora, si no fueran diferentes, $\alpha^{q^j} = \alpha^{q^k}$ para ciertos $0 \leq j < k \leq m-1$. Elevando a q^{m-k}

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha \Longrightarrow f(x) | x^{q^{m-k+j}} - x$$

Poro entonces, $m | m-k+j$. Lo que es imposible porque $m-k+j < m$. □

Corolario 3. *$x^{p^n} - x \in \mathbb{Z}_p[x]$ es el producto de todos los $f(x) \in \mathbb{Z}_p$ irreducibles mónicos con grado divisor de n.*

Ejemplo 3. $x^4 - x = x(x+1)(x^2+x+1) \in \mathbb{Z}_2[x]$
$x^9 - x = x(x-1)(x-2)(x^2+1)(x^2+x+2)(x^2+2x+2) \in \mathbb{Z}_3[x]$

Corolario 4. *Si $f \in F_q[x]$ irreducible y $gr(f) = m$. Entonces, el cuerpo de descomposición de $f(x)$ sobre F_q es F_{q^m}.*

Demostración: Por el teorema, el c.d. de $f(x)$ sobre F_q es

$$F_q\left(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right) = F_q(\alpha) = F_{q^m}$$

Corolario 5. *Dos irreducibles con mismo grado tienen el mismo c.d.* □

Ahora, si F_{q^m}/F_q es una extensión de c.f., para cualquier $\alpha \in F_{q^m}$,

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Definición 3. *A* $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ *los llamamos los* ***conjugados de*** α *respecto de la extensión* F_{q^m}/F_q.

Los conjugados de un $\alpha \in F_{q^m}$ son distintos si y sólo si $\mathrm{gr}\left(\mathrm{Irre}_{F_q}(\alpha)\right) = m$.

Si el grado es del irreducible es $d < m$. Entonces, $d|m$, el c.d. de α es F_{q^d} y los conjugados distintos de α se repiten $\frac{m}{d}$ veces y son $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$.

Teorema 7. *Los conjugados de un* $\alpha \in F_{q^m}^*$ *respecto a* F_{q^m}/F_q *tienen el mismo orden multiplicativo.*

Demostración: Por el teorema 4, $F_{q^m}^*$ es cíclico. Luego el subgrupo multiplicativo generado por cualquier $\alpha \in F_{q^m}^*$ también es cíclico de tamaño d divisor de $q^m - 1$ y sus generadores son las potencias α^k con $(k, d) = 1$.

Los exponentes, q^i, de los distintos conjugados son primos con $q^m - 1$. Luego son primos con cualquier divisor d suyo. En consecuencia, los distintos conjugados generan el mismo subgrupo de tamaño d. □

Corolario 6. *Si* α *es un elemento primitivo de* F_q. *Entonces, sus conjugados son también primitivos respecto de cualquier subcuerpo de* F_q.

Ejemplo 4. *Si* $\alpha \in F_{16}$ *es raíz del polinomio* $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. *Entonces, sus conjugados respecto a la extensión* F_{16}/F_2 *son distintos entre si*

$$\alpha,\ \alpha^2,\ \alpha^4 = \alpha + 1,\ \alpha^8 = \alpha^2 + 1$$

porque $f(x)$ es irreducible en $\mathbb{Z}_2[x]$. Por tanto, cualquiera de ellos genera al grupo multiplicativo F_{16}^* y son todos los elementos primitivos que tiene. Si consideramos la extensión F_{16}/F_4, los conjugados son α, $\alpha^4 = \alpha + 1$.*

Definición 4. *Si $\sigma : F_{q^m} \longrightarrow F_{q^m}$ es un automorfismo de cuerpos que satisface $\sigma(\alpha) = \alpha$ para todo $\alpha \in F_q$, decimos que σ es un F_q-**automorfismo**.*

Teorema 8. *Los distintos F_q-automorfismos de F_{q^m} son los $\sigma_0, \dots, \sigma_{m-1}$ definidos por $\sigma_j(\alpha) = \alpha^{q^j}$ para todo $\alpha \in F_{q^m}$.*

Demostración: Como para todo $j = 0, 1, \dots, m-1$

$$\left.\begin{array}{l} \sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta) \\ \sigma_j(\alpha+\beta) = \sigma_j(\alpha) + \sigma_j(\beta) \\ \sigma_j(\alpha) = 0 \Longleftrightarrow \alpha = 0 \\ \alpha^q = \alpha \Longleftrightarrow \alpha \in F_q \end{array}\right\} \Longrightarrow \sigma_j \text{ es un } F_q - \text{automorfismo}$$

Y los σ_j son distintos entre si porque las m imágenes de un α primitivo son distintas entre si. Por otro lado, si $\sigma : F_{q^m} \longrightarrow F_{q^m}$ es un F_q-automorfismo. Si consideramos cualquier $\beta \in F_{q^m}$ primitivo, su polmin sobre F_q, $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in F_q[x]$, tiene grado m y se tiene

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \cdots + a_0$$

O sea, $f(\sigma(\beta)) = 0$ y $\sigma(\beta)$ es una raíz de un irreducible $f(x)$. Luego por el teorema 6 debe ser de la forma $\sigma(\beta) = \beta^{q^j}$ y de ahí $\sigma(\alpha) = \alpha^{q^j}$ para todo $\alpha \in F_{q^m}$ como queremos demostrar.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

3. Algoritmo de Berlekamp

Cualquier polinomio con coeficientes en un cuerpo factoriza de forma única como producto de irreducibles ya que $K[x]$ es un DE y también DIP y DFU. En particular, para todo $f \in F_q[x]$, $q = p^n$, existen irreducibles f_i tales que

$$f = f_1^{e_1} \cdots f_r^{e_r}$$

Definición 5. *$f(x)$ es* ***libre de cuadrados*** *si todos los exponentes son $e_i = 1$.*

Como una raíz repetida de un polinomio es una raíz común con su derivada y $f'(x)$ siempre tiene grado menor. Si $f(x) \in F_q[x]$ irreducible la única posibilidad de que tenga raíces repetidas es $f'(x) = 0$ pero entonces $f(x) = g(x)^p$ con p la característica del cuerpo, absurdo. O sea,

Lema 5. *Los irreducibles en $F_q[x]$ tienen raíces distintas y los cuerpos finitos son cuerpos perfectos.*

En particular, un polinomio con coeficientes en un cuerpo perfecto es libre de cuadrados si no tiene raíces repetidas. En particular,

Lema 6. *$f(x) \in F_q[x]$ es libre de cuadrados si y sólo si* $\gcd\left(f, f'\right) = 1$

Pero si el mcd $d(x) = \gcd(f(x), f'(x))$ es distinto de 1 y de $f(x)$, entonces es un factor propio de $f(x)$ y el cociente $g(x) = f(x)/d(x)$ es un polinomio libre de cuadrados. La factorización de $f(x)$ se reduce a factorizar ambos.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Página web personal
Página de Abertura
Contenido
◀◀ ▶▶
◀ ▶

Atrás
Pantalla grande/pequeña
Cerrar

Si de nuevo el polinomio $d(x)$ tiene raíces repetidas se le aplica el mismo procedimiento. Como en cada etapa se baja el grado del polinomio la factorización final se reduce a factorizar polinomios libres de cuadrados.

Teorema 9. *Si $f, h \in F_q[x]$ con f mónico y $h^q \equiv h \pmod{f}$. Entonces,*

$$f(x) = \prod_{c \in F_q} \gcd\big(f(x), h(x) - c\big)$$

Demostración: Como para $c_1 \neq c_2$, $\gcd(h(x)-c_1, h(x)-c_2) = \gcd(h(x)-c_1, c_1-c_2) = 1$, entonces los $\gcd\big(f(x), h(x)-c_i\big)$ son primos entre si y su mcm es su producto. Y como cada uno divide a $f(x)$ su mcm divide a $f(x)$.

Para todo cuerpo finito $x^q - x = x\left(x^{q-1} - 1\right) = \prod_{c \in F_q}(x - c)$. Entonces,

$$h(x)^q - h(x) = \prod_{c \in F_q} \big(h(x) - c\big)$$

Y por la hipótesis, $f(x)$ divide a ese producto. Por tanto, se dividen mutuamente y como son polinomios mónicos[3] deben ser iguales. □

Corolario 7. *Si $0 < gr(h) < gr(f)$ y $h^q \equiv h \pmod{f}$. Entonces el producto $\prod_{c \in F_q} \gcd\big(f(x), h(x) - c\big)$ es una factorización propia de $f(x)$.*

Definición 6. *Si $h(x) \in F_q[x]$ tal que $h^q \equiv h \pmod{f}$ conduce a una factorización propia decimos que es un* ***polinomio f-reductor***.

[3] El mcd de dos polinomios con coeficientes en un cuerpo se toma mónico.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

En general, una factorización propia no es completa cuando alguno de los factores es reducible. En cuyo caso, se procede a buscar un polinomio f-reductor para ese factor. El proceso recursivo acaba con éxito si somos capaces de encontrar polinomios f-reductores para cada $f(x)$ reducible.

Si $n = \mathrm{gr}(f)$, para cada $0 \le i \le n-1$ existen $b_{ij} \in F_q$ únicos tal que

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \mod f(x) \Longrightarrow B = (b_{ij})_{0\le i,j\le n-1} \in M_{n\times n}(F_q)$$

Teorema 10. $h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in F_q[x]$ *satisface* $h^q \equiv h \pmod f$ *si y sólo si* $(a_0,\ldots,a_{n-1})B = (a_0,\ldots,a_{n-1})$.

Demostración: La igualdad matricial se da si y sólo si $a_j = \sum_{j=0}^{n-1} a_i b_{ij}$ para todo $0 \le i \le n-1$ y por tanto si y sólo si

$$h(x) = \sum_{j=0}^{n-1} a_j x^j = \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i b_{ij} x^j \equiv \sum_{i=0}^{n-1} a_i x^{iq} \equiv h(x)^q \mod f(x)$$

Corolario 8. $h(x) = \sum_{j=0}^{n-1} a_j x^j \in F_q[x]$ *satisface* $h^q \equiv h \pmod f$ *si y sólo si* $(a_0,\ldots,a_{n-1})$ *es un vector propio de* B *correspondiente al autovalor* 1.

Demostración: Basta darse cuenta de que la matriz B tiene la primera fila $(1,0,\ldots,0)$ ya que cuando $i=0$, $x^{iq}=1$. Además,
$(a_0,\ldots,a_{n-1})B = (a_0,\ldots,a_{n-1}) \Longleftrightarrow (a_0,\ldots,a_{n-1})(B - Id) = 0$
Por tanto, la matriz $B - Id$ tiene la primera fila de ceros y 1 es un valor propio.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Por lo anterior, el conjunto de los polinomios $h \in F_q[x]$ con $\mathrm{gr}(h)<\mathrm{gr}(f)$ tales que $h^q \equiv h \pmod{f}$ corresponden al espacio propio del autovalor 1 de la matriz B. Tienen estructura de espacio vectorial sobre el cuerpo finito F_q y su tamaño es q^r donde r es la dimensión del espacio propio

$$V_1 = \left\{(x_1,\dots,x_n) \in F_q^n : \ (x_1,\dots,x_n)(B - Id) = 0\right\}$$

Por otro lado, si f libre de cuadrados, $f = f_1 \cdots f_r$ con $f_i \in F_q[x]$ irreducibles distintos y por tanto primos entre si. Por el teorema chino de los restos

$$\frac{F_q[x]}{(f(x))} \cong \frac{F_q[x]}{(f_1(x))} \oplus \cdots \oplus \frac{F_q[x]}{(f_r(x))}$$

Y para cada tupla $(c_1,\dots,c_r) \in F_q^r$, existe un único $h \in F_q[x]$, con gr(h)<gr(f)

$$\begin{aligned} h(x) \equiv c_i \mod f_i(x) &\Longrightarrow h(x)^q \equiv c_i^q \equiv c_i \equiv h(x) \pmod{f_i(x)} \\ \text{Y por ser } f \text{ libre de cuadrados } &\Longrightarrow h(x)^q \equiv h(x) \pmod{f(x)} \end{aligned}$$

Como hay q^r tuplas $(c_1,\dots,c_r)$ en F_q^r, hay exactamente q^r polinomios $h \in F_q[x]$ de grado menor que $\mathrm{gr}(f)$ tal que $h^q \equiv h \pmod{f}$ con r el número de factores irreducibles de f. Por todo lo anterior, si f libre de cuadrados

Corolario 9. *$f(x) \in F_q[x]$, tiene r factores irreducibles con $r = \dim_{F_q} V_1$.*

Por el teorema de Rouché-Frobenius el número de soluciones independientes es $\dim_{F_q} V_1 = n - \mathrm{rango}(B - Id)$ con $n = \mathrm{gr}(f)$. Por tanto,

Corolario 10. *$f(x) \in F_q[x]$, es irreducible si y sólo si $\mathrm{rango}(B - Id) = n - 1$.*

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Ejemplo 5. *Si* $f(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$, *como* $mcd(f(x), f'(x)) = 1$, f *es libre de cuadrados. Las potencias* $x^{2i} \pmod{f(x)}$ *para* $0 \le i \le 4$ *son*

$$x^0 = 1,\ x^2,\ x^4,\ x^6 \equiv x + x^3,\ x^8 \equiv 1 + x^2 + x^3 \pmod{f(x)}$$

sus coeficientes dan las filas de la matriz $B \in M_5(\mathbb{Z}_2)$. *Y como* $1 = -1 \in \mathbb{Z}_2$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix} \Longrightarrow B - Id = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

donde la matriz de la derecha es la FNHC de $B - Id$. *O sea, son equivalentes. El rango* $(B - Id) = 4 \Longleftrightarrow r = \dim_{F_q} V_1 = 5 - 4 = 1$ *y* $f(x)$ *es irreducible.*

Como siempre un autovector para el valor propio 1 es $(1, 0, \ldots, 0)$ corresponde al polinomio $h(x) = 1$ que no es f-reductor. Cuando hay el resto de los $r - 1$ autovectores tienen grado entre cero y $n = \mathrm{gr}(f)$ y son f-reductores.

O sea, para factorizar un $f(x) \in F_q[x]$ libre de cuadrados, hay que calcular una base del espacio propio V_1 y calcular los polinomios $h_2(x), \ldots, h_r(x)$.

Para el primero de estos, calculamos el $\mathrm{mcd}\big(f(x), h_2(x) - c\big)$ para cada $c \in F_q$. Su producto nos da una factorización propia de $f(x)$. Si ya conseguimos r factores, estos serán irreducibles y el proceso termina. En caso contrario, repetimos con $h_3, \ldots, h_r$, hasta conseguir r factores propios de $f(x)$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Ejemplo 6. *Si* $f(x) = x^5 + x + 1 \in \mathbb{Z}_2[x]$*, como* $mcd(f(x), f'(x)) = 1$*,* f *es libre de cuadrados. Las potencias* $x^{2i} \pmod{f(x)}$ *para* $0 \le i \le 4$ *son*

$$x^0 = 1,\ x^2,\ x^4,\ x^6 \equiv x + x^2,\ x^8 \equiv x^3 + x^4 \pmod{f(x)}$$

sus coeficientes dan las filas de la matriz $B \in M_5(\mathbb{Z}_2)$*. Y como* $1 = -1 \in \mathbb{Z}_2$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \Longrightarrow B - Id = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

donde la matriz de la derecha es la FNHC de $B - Id$*. O sea, son equivalentes por columnas y los s.l. homogéneos asociados tienen las mismas soluciones. El rango* $(B - Id) = 3 \Longleftrightarrow r = \dim_{F_q} V_1 = 5 - 3 = 2$ *y hay dos soluciones. Ahora, buscamos las soluciones del s.l. correspondiente a las columnas*

$$\left.\begin{array}{l} x_1 + x_4 = 0 \\ x_2 = 0 \\ x_3 + x_4 = 0 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x_2 = 0 \\ x_1 = x_3 = x_4 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} (1,0,0,0,0) \\ (0,1,0,1,1) \end{array}\right\} \Longrightarrow \left.\begin{array}{l} f_1 = 1 \\ f_2 = x + x^3 + x^4 \end{array}\right\}$$

El rango $(B - Id) = 3 \Longleftrightarrow r = \dim_{F_q} V_1 = 5 - 3 = 2$*. Hay dos soluciones. Sólo* f_2 *es* f*-reductor y nos dará una factorización de* $f(x) = x^5 + x + 1$ *en* $\mathbb{Z}_2[x]$*. Para eso, calculamos dos mcd. Aunque basta con uno de los dos.*

$$\left.\begin{array}{l} \gcd(x^5 + x + 1, x^4 + x^3 + x) = x^3 + x^2 + 1 \\ \gcd(x^5 + x + 1, x^4 + x^3 + x + 1) = x^2 + x + 1 \end{array}\right\} \Longrightarrow f(x) = (x^3 + x^2 + 1)(x^2 + x + 1)$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Ejemplo 7. *Si* $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$, *como* $f'(x) \equiv x^2 \pmod 2$ *se tiene* $mcd(f(x), f'(x)) = \gcd(1, x^2) = 1$. *Por tanto,* f *es libre de cuadrados. Ahora, calculamos las potencias* $x^{2i} \pmod{f(x)}$ *para* $0 \le i \le 7$

$$
\begin{array}{ll}
x^0 = 1, x^2, x^4, x^6 & \\
x^8 \equiv 1 + x^3 + x^4 + x^6 & \pmod{f(x)} \\
x^{10} \equiv x^2 + x^5 + x^6 + x^8 \equiv 1 + x^2 + x^3 + x^4 + x^5 & \pmod{f(x)} \\
x^{12} \equiv x^2 + x^4 + x^5 + x^6 + x^7 & \pmod{f(x)} \\
x^{12} \equiv x^4 + x^6 + x^7 + x^8 + x^9 \equiv 1 + x + x^3 + x^4 + x^5 & \pmod{f(x)}
\end{array}
$$

sus coeficientes dan las filas de la matriz $B \in M_8(\mathbb{Z}_2)$. *O sea,*

$$
B = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}
\Longrightarrow B - Id = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
\end{pmatrix}
$$

$B - Id$ *tiene rango 6. El s.l. tiene* $8 - 6 = 2$ *soluciones independientes. Sólo la segunda corresponde a un polinomio,* $h_2(x) = x + x^2 + x^5 + x^6 + x^7$, f*-reductor.*

$$
\left.\begin{array}{l}
\gcd(f(x), h_2(x) - 0) = x^6 + x^5 + x^4 + x + 1 \\
\gcd(f(x), h_2(x) - 1) = x^2 + x + 1
\end{array}\right\} \Longrightarrow f(x) = (x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1)
$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Página web personal
Página de Abertura
Contenido
◀◀ ▶▶
◀ ▶
Página 20 de 21
Atrás
Pantalla grande/pequeña
Cerrar

4. Referencias.

[1] Lidl R., Nieferreiter, JH.: *Finite Fields*, Cambridge University Press, 1997.
[2] David Bressoud, Stan Wagon: *A Course in Computational Number Theory*, John Wiley & Sons, Hoboken, NJ, USA, 2000.
[3] Hans Riesel: *Prime Numbers and Computer Methods for Factorization*, Springer Science+Business Media, LLC 2012, (first edition Birkhäuser, 1994).
[4] Samuel S. Wagstaff, Jr: *The joy of factoring*, AMS, Providence, Rhode island, 2013.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra