15 Apéndice: factorización en cuerpos finitos

Voy a presentar ahora, como broche de oro sobre la caracterización de cuerpos finitos, el *Algoritmo de Berlekamp*, para factorizar $f \in \mathbb{F}_{p^n}[X]$ de una forma para nada trivial y mucho más eficiente que usar fuerza bruta (Elwyn Berlekamp, 1940-2019). Este algoritmo es históricamente importante por ser el primer algoritmo de factorización que funciona bien en la práctica, aunque tiene sus bemoles.

Por simplicidad, porque lo que me interesa aquí es solamente mostrar todo lo que significa la caraceterización que vimos de cuerpos finitos, la potencia que tiene, voy a asumir que $f \in \mathbb{F}_p[X]$ es mónico y libre de cuadrados, y lo quiero factorizar en $\mathbb{F}_p[X]$. O sea sabemos que

$$f = p_1 \cdots p_s \quad \text{con} \quad p_1, \ldots, p_s \in \mathbb{F}_p[X] \ \text{ irreducibles mónicos distintos,}$$

y los queremos encontrar.

(1) Sea

$$A := \mathbb{F}_p[X]/\langle f \rangle,$$

que es una $\mathbb{F}_p$-álgebra (anillo con las operaciones módulo f y $\mathbb{F}_p$-espacio vectorial), con base como $\mathbb{F}_p$-álgebra

$$(1, X, \cdots, X^{d-1}) \quad \text{donde} \quad d := \operatorname{gr}(f).$$

Por el *Teorema Chino del Resto*, dado que f es producto de irreducibles distintos, tenemos que

$$\begin{array}{rccl} \pi: & A := \mathbb{F}_p[X]/\langle f \rangle & \underset{\simeq}{\longrightarrow} & \rangle \oplus \cdots \oplus \mathbb{F}_p[X]/\langle p_s \rangle \\ & \overline{g} & \longmapsto & (\overline{g}^1 \quad , \ \ldots \ , \quad \overline{g}^s) \end{array}$$

es un isomorfismo de álgebras (tanto de anillos como de $\mathbb{F}_p$-e.v.). Aquí $\overline{g}$ denota la clase de g mod f y $\overline{g}^i$ denota la clase de g mod p_i, $1 \le i \le s$:
Esto lo vieron en Algebra II pero por las dudas lo repasamos: $\pi = \pi_1 \times \cdots \times \pi_s$ donde

- $\pi_i : \mathbb{F}_p[X]/\langle f \rangle \to \mathbb{F}_p[X]/\langle p_i \rangle$, $\overline{g} \mapsto \overline{g}^i$ está b.d.:

$$\overline{g} = \overline{h} \ \Leftrightarrow \ f \,|\, g - h \ \Rightarrow \ p_i \,|\, g - h \ \Leftrightarrow \ \overline{g}^i = \overline{h}^i.$$

- Es morfismo de anillos y de $\mathbb{F}_p$-e.v. pues $a, b \in \mathbb{F}_p$ satisfacen $\overline{a}^i = \overline{b}^i \Leftrightarrow a = b$.

  (Notar que $\pi_i(\overline{g}) = \overline{g_i}^i \Leftrightarrow p_i \,|\, g - g_i$ y $\pi_i(\overline{g}) = a \in \mathbb{F}_p \Leftrightarrow p_i \,|\, g - a$).

- Es mono pues $\overline{g}^i = 0 \Leftrightarrow p_i \,|\, g$ y por lo tanto $\overline{g}^i = 0,\ \forall\, i \Leftrightarrow f \,|\, g \Leftrightarrow \overline{g} = 0$.

- Es epi: son dos $\mathbb{F}_p$-e.v. con $\mathrm{gr}(f) = \dim_{\mathbb{F}_p}(A) = \dim_{\mathbb{F}_p}(\pi(A))$ por ser π mono, y $\dim_{\mathbb{F}_p}(\prod_i \mathbb{F}_p[X]/\langle p_i\rangle) = \sum_i \mathrm{gr}(p_i) = \mathrm{gr}(f)$. Por lo tanto como la dimensión de la imagen y del codominio coinciden, π es epi.

Conclusión:

$$\pi : A \longrightarrow E_1 \times \cdots \times E_s \quad \text{con } A = \mathbb{F}_p[X]/\langle f\rangle \quad \text{y} \quad E_i = \mathbb{F}_p[X]/\langle p_i\rangle,\ 1 \le i \le s,$$

es isomorfismo de álgebras, y notar que $E_i = \mathbb{F}_p[X]/\langle p_i\rangle$ es un cuerpo que contiene a $\mathbb{F}_p$, i.e.

$$E_i = \mathbb{F}_{p^{d_i}} = \mathbb{F}_p(X^{p^{d_i}} - X) \ \text{ si } \mathrm{gr}(p_i) = d_i.$$

(2) Sean ahora

$$\begin{aligned} L &: A \longrightarrow A \quad , \quad g \longmapsto g^p - g \\ L_i &: E_i \longrightarrow E_i \quad , \quad g_i \longmapsto g_i^p - g_i,\ 1 \le i \le s. \end{aligned}$$

$L,\ L_i,\ 1 \le i \le s$ son transformaciones lineales de $\mathbb{F}_p$-e.v. pues por Frobenius,

- $L(g+h) = (g+h)^p - (g+h) = g^p + h^p - g - h = L(g) + L(h)$
- $L(a\,g) = (a\,g)^p - (a\,g) = a^p g^p - a\,g = a\,g^p - a\,g = a(g^p - g) = aL(g)$.

y lo mismo para L_i.
Se tiene

$$L|_{E_i} = L_i \quad \text{y} \quad L = L_1 \times \cdots \times L_s :$$

Si $\pi(g) = (g_1, \ldots, g_s)$ donde $g_i = \pi_i(g) \equiv g \mod p_i$, entonces

$$\pi(L(g)) = \pi(g^p - g) = (g_1^p - g_1, \cdots, g_s^p - g_s) = \big(L_1(g), \cdots, L_s(g)\big)$$

pues π es isomorfismo de álgebras.

(3) Estudio de $\mathrm{Nu}(L)$:

$$\mathrm{Nu}(L) = \{g \in A :\ g^p - g = 0\} \simeq \mathrm{Nu}(L_1) \times \cdots \times \mathrm{Nu}(L_s)$$

donde

$$\mathrm{Nu}(L_i) = \{g_i \in E_i :\ g_i^p - g_i = 0\} \subset E_i = \mathbb{F}_{p^{d_i}} \quad \Longrightarrow \quad \mathrm{Nu}(L_i) = \mathbb{F}_p \subset E_i.$$

Por lo tanto,

$$\mathrm{Nu}(L) \simeq \underbrace{\mathbb{F}_p \times \cdots \times \mathbb{F}_p}_{s} = \mathbb{F}_p^s.$$

Segunda conclusión:

$$\dim_{\mathbb{F}_p}(\mathrm{Nu}(L)) = s := \#\text{ factores irreducibles de } f.$$

Podemos calcular facilmente una base de $\mathrm{Nu}(L)$, por ejemplo triangulando la matriz de la t.l. L en la base canónica $\big(1, X, \ldots, X^{d-1}\big)$ de A. Y de paso deducir s.
Notar que el hecho que $\mathrm{Nu}(L_i) = \mathbb{F}_p \subset E_i = \mathbb{F}_p^{d_i}$ implica en particular que en el teorema chino del resto,

$$g \in \mathrm{Nu}(L) \quad \Longleftrightarrow \quad \pi(g) = \big(\pi_1(g), \ldots, \pi_s(g)\big) \in \mathbb{F}_p^s. \tag{1}$$

(4) Afirmaciones:

(a) Sea $g \in A$. Entonces,

$$g \in \mathrm{Nu}(L) \quad \Longleftrightarrow \quad f = \prod_{a \in \mathbb{F}_p} \mathrm{mcd}(f, g-a).$$

Prueba.– Sabemos que para todo $g \in A$, $g^p - g = \prod_{a \in \mathbb{F}_p} (g-a)$. Entonces

$$\begin{aligned} g \in \mathrm{Nu}(L) &\iff g^p - g = 0 \text{ en } A \iff f \mid g^p - g \\ &\iff f \mid \prod_{a \in \mathbb{F}_p} (g-a) \iff \mathrm{mcd}\big(f, \prod_{a \in \mathbb{F}_p} (g-a)\big) = f \\ &\underset{g-a \perp g-b}{\Longleftrightarrow} \prod_{a \in \mathbb{F}_p} \mathrm{mcd}(f, g-a) = f. \end{aligned}$$

■

Usando distintos $g \in \mathrm{Nu}(L)$ conseguiremos eventualmente "quebrar" f. Pero no todos los $g \in \mathrm{Nu}(L)$ sirven. Por ejemplo $g = 1 \in \mathrm{Nu}(L)$ no aporta nada pues

$$\mathrm{mcd}(f, 1-a) = f \text{ si } a = 1 \text{ y } \mathrm{mcd}(f, 1-a) = 1 \text{ si } a \neq 1.$$

Tenemos que garantizar que recorriendo $g \in \mathrm{Nu}(f)$ conseguimos quebrar completamente f.

(b) Sean $g \in \mathrm{Nu}(L)$ y $a \in \mathbb{F}_p$. Entonces

$$\mathrm{mcd}(f, g-a) \neq 1 \quad \Longleftrightarrow \quad \text{existe } i,\ 1 \leq i \leq s,\ \text{tq } \pi_i(g) = a.$$

Prueba.– Se tiene

$$\begin{aligned}\operatorname{mcd}(f, g-a) \neq 1 &\iff \text{existe } \ i,\ 1 \leq i \leq s,\ \text{tq } \ p_i \,|\, g-a \\ &\iff \text{existe } \ i,\ 1 \leq i \leq s,\ \text{tq } \ g \equiv a \bmod p_i \\ &\iff \text{existe } \ i,\ 1 \leq i \leq s,\ \text{tq } \ \pi_i(g) = a.\end{aligned}$$

■

De **(a)** y **(b)** se deduce:

(c) Sea $g \in \operatorname{Nu}(L)$ tq $\pi(g) = (a_1, \ldots, a_s) \in \mathbb{F}_p^s$, y sea $\{b_1, \ldots, b_t\}$ el conjunto de elementos distintos entre $\{a_1, \ldots, a_s\}$. Entonces

$$f = \prod_{1 \leq i \leq t} \operatorname{mcd}(f, g - b_i).$$

(d) Sea $\mathcal{B} := \big(1, g_2, \ldots, g_s\big)$ base de $\operatorname{Nu}(L)$, y sea $g \in \mathcal{B}$ con $g \neq 1$. Entonces existe $1 \leq i \neq j \leq s$ tq $\pi_i(g) \neq \pi_j(g)$.

Prueba.– Si para $g \in \mathcal{B}$, $g \neq 1$, fuera $\pi_i(g) = \pi_j(g)$ para todo i, j, entonces se tendría

$$\pi(g) = (a, \cdots, a) = a(1, \ldots, 1) \ \in \ \mathbb{F}_p^s \quad \Longrightarrow \quad g = a \cdot 1 \in A.$$

Pero g l.i. con 1 pues forma parte de $\mathcal{B}$. ¡Absurdo!

■

(e) Sea $1 \leq i \neq j \leq s$. Entonces

$$\text{existe } \ g \in \mathcal{B} := \big(1, g_2, \ldots, g_s\big) \ \text{ tq } \ \pi_i(g) \neq \pi_j(g).$$

Prueba.– Si no fuera así, existen $i \neq j$ tq $\pi_i(g) = \pi_j(g)$ para todo $g \in \mathcal{B}$ y por lo tanto se tendría

$$\pi(\mathcal{B}) \ \subset \ \{(x_1, \ldots, x_s) \in \mathbb{F}_p^s : \ x_i - x_j = 0\},$$

o sea $\mathcal{B}$ que genera $\mathbb{F}_p^s$ estaría incluido en un subespacio propio de $\mathbb{F}_p^s$. ¡Absurdo!

■

Conclusión: Dado que $\pi_i(g) = a \ \Leftrightarrow \ p_i \,|\, g - a$, **(e)** se tiene que interpretar como que para todo $i \neq j$, existe $g \in \mathcal{B}$ tq $p_i \,|\, g - a_i$ y $p_j \,|\, g - a_j$: los irreducibles $p_i \neq p_j$ son "separados"por algún elemento de la base.

Algoritmo:

1. Calculo base $\mathcal{B} = \{1, g_2, \ldots, g_s\}$ de $\mathrm{Nu}(L)$.
2. Tomo sucesivamente $g \neq 1$ en $\mathcal{B}$ y $a \in \mathbb{F}_p$ y calculo $\mathrm{mcd}(f, g - a)$, hasta llegar a s factores distintos, que forsozamente serán los s factores irreducibles p_i si los consigo con el mismo g. Sino ¿me las rebusco?

- La correctitud del algoritmo está garantizada por las afirmaciones anteriores.
- Costo: $O(pd^3)$ si $d = \mathrm{gr}(f)$ (contra $O(p^d)$ si se aplica fuerza bruta).

Ejemplo

Sea $f = X^5 - 2X^4 - X^3 + X^2 + 1$ en $\mathbb{F}_7[X]$.

- Base de A: $(1, X, X^2, X^3, X^4)$ y $L(g) = g^7 - g$. Calculemos $[L]$ en esa base.
  - $1 \mapsto 0$
  - $X \mapsto X^7 - X = 4X^4 + 3X^3 + X^2 + 4X + 2$
  - $X^2 \mapsto X^{14} - X^2 = 6X^4 + 6X^3 + 2X^2 + X + 6$
  - $X^3 \mapsto X^{21} - X^3 = 5X^4 + 5X^3 + 4X^2 + 2X + 5$
  - $X^4 \mapsto X^{28} - X^4 = 6X^3 + 2X^2 + X + 5$

$$[L] = \begin{pmatrix} 0 & 2 & 6 & 5 & 5 \\ 0 & 4 & 1 & 2 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 3 & 6 & 5 & 6 \\ 0 & 4 & 6 & 5 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- $\dim \mathrm{Nu}(L) = 3$ y $\mathcal{B} = (1, g_2 = X^3 - 2X^2, g_3 = X^4 - 4X^2 - X)$.
  - $\mathrm{mcd}(f, g_2) = 1$
  - $\mathrm{mcd}(f, g_2 - 1) = X^3 - 2X^2 - 1$
  - $\mathrm{mcd}(f, g_2 - 2) = 1$
  - $\mathrm{mcd}(f, g_2 - 3) = 1$
  - $\mathrm{mcd}(f, g_2 - 4) = X + 1$
  - $\mathrm{mcd}(f, g_2 - 5) = 1$
  - $\mathrm{mcd}(f, g_2 - 6) = X - 1$

  Encontramos 3 factores y son coprimos entre sí: son todos.

$$f = (X^3 - 2X^2 - 1)(X + 1)(X - 1) \quad \text{en } \mathbb{F}_7[X].$$