Matrices circulantes módulo potencias de primos

El problema

Dado un vector $\alpha \in \mathbb{Z}^d$, $d = p^n$, queremos caracterizar los $\beta \in \mathbb{Z}^d$, tales que

$$\mathsf{C}_\alpha \beta \equiv 0 \pmod{d} , \tag{1}$$

donde C_α es la *matriz circulante* asociada al vector α: si $\alpha = (\alpha_0, \ldots, \alpha_{d-1})$, entonces

$$\mathsf{C}_\alpha = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{d-1} \\ \alpha_{d-1} & \alpha_0 & \cdots & \alpha_{d-2} \\ \vdots & \vdots & & \vdots \\ \alpha_1 & \alpha_2 & \cdots & \alpha_0 \end{bmatrix} . \tag{2}$$

La *suma de las coordenadas de α saltando de a t lugares* es una suma de la forma:

$$\sum_r \alpha_{i+rt}$$

donde $0 \leq i < t$ y $0 \leq r < d/t$. En general, suponemos que $t = p^k$ con $k \leq n$. La conjetura es que, si las sumas de las coordenadas de α saltando de a p no son todas cero módulo p, entonces todo β que cumple (1) (que *está en el núcleo de C_α módulo p^n*), verifica que la suma de sus coordenadas es congruente a cero módulo d, es decir,

$$\sum_j \beta_j \equiv 0 \pmod{d} . \tag{3}$$

Podemos reformular el problema en términos de polinomios. Sea $d = p^n$ una potencia arbitraria de un primo p. Dado $\alpha = (\alpha_0, \ldots, \alpha_{d-1}) \in \mathbb{Z}^d$, definimos un polinomio de grado $d-1$ asociado, $f_\alpha \in \mathbb{Z}[X]$, por:

$$f_\alpha = \alpha_0 + \alpha_1 X + \cdots + \alpha_{d-1} X^{d-1} . \tag{4}$$

Tenemos un isomorfismo de $\mathbb{Z}$-módulos:

$$\mathbb{Z}^d \simeq \mathbb{Z}[X]/\langle X^d - 1 \rangle , \tag{5}$$

dado por $\alpha \mapsto f_\alpha$. Vía este isomorfismo, la transformación $\mathbb{Z}$-lineal C_α se corresponde con multiplicar por f_α, es decir,

$$f_{\mathsf{C}_\alpha \beta} \equiv f_\alpha f_\beta \pmod{X^d - 1} .$$

Por otro lado, la operación dada por sumar coordenadas saltando de a p se corresponde con pasar del cociente por $X^d - 1$ al cociente por $X^p - 1$; como $p|d$, se deduce que $X^p - 1 | X^d - 1$ y esta operación está definida. Expresado de otra manera, el siguiente diagrama conmuta:

$$\begin{tikzcd} \mathbb{Z}^d \arrow[r] \arrow[d] & \mathbb{Z}[X]/\big\langle X^d - 1\big\rangle \arrow[d] \\ \mathbb{Z}^p \arrow[r] & \mathbb{Z}[X]/\big\langle X^p - 1\big\rangle \end{tikzcd} ,$$

donde:

- la flecha horizontal superior es el isomorfismo (5),
- la flecha horizontal inferior es el isomorfismo análogo con $n = 1$,
- la flecha vertical izquierda es la operación de sumar coordenadas saltando de a p y
- la flecha vertical derecha es el paso al cociente.

Similarmente, la operación de sumar todas las coordenadas se corresponde con pasar al cociente por $X - 1$. Finalmente, condiciones de divisibilidad sobre las coordenadas de un vector α se traducen en exactamente las mismas condiciones de divisibilidad sobre los coeficientes del polinomio asociado:

$$\alpha \equiv 0 \,(\mathsf{mod}\, p^l) \quad \Leftrightarrow \quad f_\alpha = 0 \quad \text{en} \quad \frac{\big(\mathbb{Z}/p^l\mathbb{Z}\big)\,[X]}{\langle X^d - 1\rangle} \quad \Leftrightarrow \quad f_\alpha \in \big\langle X^d - 1, p^l\big\rangle \subset \mathbb{Z}[X]\ .$$

En definitiva,

$$\mathsf{C}_\alpha\,\beta \equiv 0 \,(\mathsf{mod}\, d) \quad \Leftrightarrow \quad f_\alpha f_\beta = 0 \quad \text{en} \quad \frac{\big(\mathbb{Z}/d\mathbb{Z}\big)\,[X]}{\langle X^d - 1\rangle} \quad \Leftrightarrow \quad f_\alpha f_\beta \in \big\langle X^d - 1, d\big\rangle\ .$$

La conjetura se puede reformular de la siguiente manera: si $f_\alpha \in \mathbb{Z}[X]$ y $f_\alpha \notin \big\langle X^p - 1, p\big\rangle$, entonces $f_\alpha f_\beta \in \big\langle X^d - 1, d\big\rangle$ implica $f_\beta \in \big\langle X - 1, d\big\rangle$.

Notación

Para que el argumento sea más claro, introducimos algo de notación. Dado $\alpha \in \mathbb{Z}^d$, definimos $\mathsf{S}_k(\alpha) \in \mathbb{Z}^{p^k}$ como el vector cuya coordenada i está dada por:

$$\mathsf{S}_k(\alpha)_i = \sum_r \alpha_{i+rp^k}\ , \tag{6}$$

donde $0 \le r < d/p^k$. Esencialmente la misma fórmula define una aplicación $\mathbb{Z}$-lineal

$$\mathsf{S}_k : \mathbb{Z}^{p^n} \to \mathbb{Z}^{p^k}$$

siempre que $n \geq k$. Cualquiera sea el dominio denotaremos esta operación por S_k. Para todo k, el siguiente diagrama conmuta:

$$
\begin{tikzcd}
\mathbb{Z}^{p^k} \arrow[r, "\sim"] \arrow[d, "\mathsf{S}_{k-1}"'] & \frac{\mathbb{Z}[X]}{\left\langle X^{p^k}-1\right\rangle} \arrow[d] \\
\mathbb{Z}^{p^{k-1}} \arrow[r, "\sim"] & \frac{\mathbb{Z}[X]}{\left\langle X^{p^{k-1}}-1\right\rangle}
\end{tikzcd} .
$$

Como $\mathsf{S}_{k-1}\mathsf{S}_k \,=\, \mathsf{S}_{k-1}$ para todo k, recuperamos inductivamente el diagrama conmutativo de la sección anterior. La conmutatividad del diagrama equivale a

$$
f_{\mathsf{S}_k(\alpha)} \,\equiv\, f_\alpha \pmod{X^{p^k}-1} \;. \tag{7}
$$

En consecuencia, por (7), el siguiente diagrama conmuta:

$$
\begin{tikzcd}
\mathbb{Z}^{p^n} \arrow[rrr, "\mathsf{C}_\alpha"] \arrow[dr] \arrow[ddd, "\mathsf{S}_k"'] & & & \mathbb{Z}^{p^n} \arrow[dl] \arrow[ddd, "\mathsf{S}_k"] \\
& \frac{\mathbb{Z}[X]}{\left\langle X^{p^n}-1\right\rangle} \arrow[r, "f_\alpha"] \arrow[d] & \frac{\mathbb{Z}[X]}{\left\langle X^{p^n}-1\right\rangle} \arrow[d] & \\
& \frac{\mathbb{Z}[X]}{\left\langle X^{p^k}-1\right\rangle} \arrow[r, "f_{\mathsf{S}_k(\alpha)}"'] & \frac{\mathbb{Z}[X]}{\left\langle X^{p^k}-1\right\rangle} & \\
\mathbb{Z}^{p^k} \arrow[rrr, "\mathsf{C}_{\mathsf{S}_k(\alpha)}"'] \arrow[ur] & & & \mathbb{Z}^{p^k} \arrow[ul]
\end{tikzcd} ;
$$

es decir, dado que multiplicar por un elemento en un anillo pasa a un cociente como multiplicar por la clase del elemento y que C_α está dada por multiplicar por f_α, se deduce que

$$
\mathsf{S}_k(\mathsf{C}_\alpha\,\beta) \,=\, \mathsf{C}_{\mathsf{S}_k(\alpha)}\,\mathsf{S}_k(\beta) \;, \tag{8}
$$

para todo $k \leq n$.

Por otro lado, tenemos las aplicaciones dadas por reducir coordenadas módulo una potencia p^l del primo p. Dado $l \geq 0$, el siguiente diagrama también conmuta:

$$
\begin{tikzcd}
\frac{\mathbb{Z}[X]}{\left\langle X^{p^k}-1\right\rangle} \arrow[r] \arrow[d, "f_\alpha"'] & \frac{\left(\mathbb{Z}/p^l\mathbb{Z}\right)\left[X\right]}{\left\langle X^{p^k}-1\right\rangle} \arrow[d, "\overline{f_\alpha}"] \\
\frac{\mathbb{Z}[X]}{\left\langle X^{p^k}-1\right\rangle} \arrow[r] & \frac{\left(\mathbb{Z}/p^l\mathbb{Z}\right)\left[X\right]}{\left\langle X^{p^k}-1\right\rangle}
\end{tikzcd} ,
$$

donde $\overline{f_\alpha}$ denota la clase de f_α reduciendo coordenadas módulo p^l. En términos de la matriz circulante, si $\overline{\mathsf{C}_\alpha}$ denota la matriz que se obtiene reduciendo las coordenadas de C_α módulo p^l, entonces

$$\overline{\mathsf{C}_\alpha\,\beta} \;=\; \overline{\mathsf{C}_\alpha}\,\overline{\beta}\ . \tag{9}$$

En relación a las distintas sumas de coordenadas,

$$\overline{\mathsf{S}_k(\alpha)} \;=\; \mathsf{S}_k(\overline{\alpha})\ , \tag{10}$$

pues ambas operaciones consisten en tomar cocientes: el diagrama

$$\begin{tikzcd}
\frac{\mathbb{Z}[X]}{\langle X^{p^n}-1\rangle} \arrow[r] \arrow[d] & \frac{\mathbb{Z}[X]}{\langle X^{p^n}-1,p^l\rangle} \arrow[r, "\sim"] \arrow[d] & \frac{(\mathbb{Z}/p^l\mathbb{Z})[X]}{\langle X^{p^n}-1\rangle} \arrow[d] \\
\frac{\mathbb{Z}[X]}{\langle X^{p^k}-1\rangle} \arrow[r] & \frac{\mathbb{Z}[X]}{\langle X^{p^k}-1,p^l\rangle} \arrow[r, "\sim"] & \frac{(\mathbb{Z}/p^l\mathbb{Z})[X]}{\langle X^{p^k}-1\rangle}
\end{tikzcd}$$

conmuta.

¿Solución?

Proposición. *Sean p primo $n \geq 1$ y $d = p^n$. Dado $\alpha \in \mathbb{Z}^d$ tal que $\mathsf{S}_1(\alpha) \not\equiv 0 \,(\mathsf{mod}\, p)$, si $\beta \in \mathbb{Z}^d$ es solución de* (1)*, entonces $\mathsf{S}_0(\beta) \equiv 0 \,(\mathsf{mod}\, d)$.*

Demostración. Que β sea solución de (1) equivale a que $f_\alpha f_\beta \in \langle X^{p^n}-1, p^n\rangle$. La condición $\mathsf{S}_1(\alpha) \not\equiv 0 \,(\mathsf{mod}\, p)$ equivale a que $f_\alpha \notin \langle X^p - 1, p\rangle$. Supongamos que $\mathsf{C}_\alpha\,\beta \equiv 0 \,(\mathsf{mod}\,) p^n$. Si reducimos coeficientes módulo p,

$$(X-1)^{p^n} \;\mid\; \overline{f_\alpha}\,\overline{f_\beta} \quad \text{y} \quad (X-1)^p \nmid \overline{f_\alpha}\ ,$$

en $(\mathbb{Z}/p\mathbb{Z})[X]$. Pero $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo y el anillo de polinomios es un DFU. En particular, $(X-1)^{p^n-p+1}$ divide a $\overline{f_\beta}$. Es decir,

$$f_\beta \in \langle (X-1)^{p^n-p+1}, p\rangle \subset \left\langle (X-1)^{p^{n-1}}, p\right\rangle = \left\langle X^{p^{n-1}} - 1, p\right\rangle\ .$$

Si $n = 1$, esto quiere decir que $f_\beta \in \langle X-1, p\rangle$, que es justamente el resultado que queremos demostrar, en este caso particular. En general, esto quiere decir que

$$\mathsf{S}_{n-1}(\beta) \;\equiv\; 0 \quad (\mathsf{mod}\, p)\ , \tag{11}$$

es decir, las coordenadas de $\mathsf{S}_{n-1}(\beta) \in \mathbb{Z}^{p^{n-1}}$ son todas múltiplos de p.

Supongamos, inductivamente, que el resultado es cierto para $n-1$. Si

$$\mathsf{C}_\alpha\,\beta \;=\; p^n\,\delta \;\equiv\; 0 \quad (\mathsf{mod}\, p^n)$$

y $\tilde{\beta} \in \mathbb{Z}^{p^{n-1}}$ cumple que

$$\mathsf{S}_{n-1}(\beta) \,=\, p\,\tilde{\beta}\ ,$$

entonces, por (8),

$$p\,\mathsf{C}_{\mathsf{S}_{n-1}(\alpha)}(\tilde{\beta}) \,=\, p^n\,\delta$$

y

$$\mathsf{C}_{\mathsf{S}_{n-1}(\alpha)}(\tilde{\beta}) \,\equiv\, 0 \pmod{p^{n-1}}\ .$$

Como $\mathsf{S}_1\,\mathsf{S}_{n-1}(\alpha) = \mathsf{S}_1(\alpha)$, aplicamos la hipótesis inductiva y concluimos que $\mathsf{S}_0(\tilde{\beta}) \equiv 0 \,(\mathsf{mod}\, p^{n-1})$. Pero, entonces

$$\mathsf{S}_0(\beta) \,=\, \mathsf{S}_0(\mathsf{S}_{n-1}(\beta)) \,=\, p\,\mathsf{S}_0(\tilde{\beta}) \,\equiv\, 0 \pmod{p^n}\ .$$

□