Escrito CXXXIV

El índice de selección $k(p)$ y su espacio de restricciones:
la fibra de k dado el observable κ

Miguel Cerdá Bennassar

Junio de 2026

Resumen

El parámetro $k(p) \in \{0, \ldots, g-1\}$ es el único componente de la identidad de síntesis que no está determinado por la estructura de reciprocidad de $A(p)$ y $B(p)$. Se demuestra que la restricción fundamental $k(p) \cdot qh \equiv \kappa(p) \pmod{g}$ convierte el mapa $\varphi : k \mapsto k \cdot qh \bmod g$ en una aplicación δ-a-1 de $\mathbb{Z}/g\mathbb{Z}$ en $\delta \cdot (\mathbb{Z}/g\mathbb{Z})$, donde $\delta = \gcd(qh, g)$. El grado de libertad residual de $k(p)$, dado el observable $\kappa(p) = A(p) - B(p)$, es exactamente δ: cuando $\delta = 1$, k está unívocamente determinado por κ; cuando $\delta > 1$, hay δ valores de k compatibles con κ. Este resultado completa el Teorema de recuperabilidad del Escrito CXXIV y cuantifica con precisión la indeterminación residual de $k(p)$.

1. La restricción fundamental sobre $k(p)$

La identidad $\kappa(p) = k(p) \cdot qh \bmod g$ (Escrito CXXIII) expresa el observable $\kappa(p) = A(p) - B(p) \bmod g$ en términos del índice de selección $k(p)$.

Definición 1.1 (El mapa de restricción)**.** *Sea $\varphi_{q,h,g} : \mathbb{Z}/g\mathbb{Z} \to \mathbb{Z}/g\mathbb{Z}$ el mapa de multiplicación:*

$$\varphi_{q,h,g}(k) = k \cdot q \cdot h \bmod g.$$

La restricción sobre $k(p)$ es $\varphi_{q,h,g}(k(p)) = \kappa(p)$.

Teorema 1.2 (Estructura de la fibra de k)**.** *Sea $\delta = \gcd(q \cdot h,\, g)$.*

1. *La imagen de $\varphi_{q,h,g}$ es el subgrupo $\delta \cdot (\mathbb{Z}/g\mathbb{Z}) = \{0, \delta, 2\delta, \ldots, g - \delta\}$, de índice δ en $\mathbb{Z}/g\mathbb{Z}$.*

2. *Para cada $\kappa \in \delta \cdot (\mathbb{Z}/g\mathbb{Z})$, la fibra $\varphi^{-1}(\kappa) = \{k \in \mathbb{Z}/g\mathbb{Z} : k \cdot qh \equiv \kappa \pmod{g}\}$ tiene exactamente δ elementos.*

3. *En particular, $\delta \mid \kappa(p)$ siempre, y el número de valores de $k(p)$ compatibles con $\kappa(p)$ es exactamente δ.*

Demostración. La imagen de $x \mapsto x \cdot n$ en $\mathbb{Z}/g\mathbb{Z}$ es $\gcd(n, g) \cdot (\mathbb{Z}/g\mathbb{Z})$. Con $n = qh$: imagen $= \delta \cdot (\mathbb{Z}/g\mathbb{Z})$, de orden g/δ. Cada fibra tiene $|\mathbb{Z}/g\mathbb{Z}|/(g/\delta) = \delta$ elementos. Como $\kappa(p) = \varphi(k(p))$ con $k(p)$ existente, se sigue $\kappa(p) \in \delta \cdot (\mathbb{Z}/g\mathbb{Z})$, i.e., $\delta \mid \kappa(p)$. □

2. Tres tipos de fibra según δ

Definición 2.1 (Tipos de fibra)**.** *Según el valor de* $\delta = \gcd(qh, g)$*:*

(a) Fibra puntual *(*$\delta = 1$*):* $k(p)$ *está unívocamente determinado por* $\kappa(p)$*. Específicamente,* $k(p) \equiv \kappa(p) \cdot (qh)^{-1} \pmod{g}$*.*

(b) Fibra múltiple *(*$1 < \delta < g$*): hay* δ *valores de* $k(p)$ *compatibles con* $\kappa(p)$*, equiespaciados en* $\mathbb{Z}/g\mathbb{Z}$ *con paso* g/δ*.*

(c) Fibra total *(*$\delta = g$*, equivalentemente* $g \mid qh$*): todo* $k \in \{0, \ldots, g-1\}$ *es compatible con* $\kappa(p) = 0$*.* $k(p)$ *es completamente indeterminado dado* κ*.*

Observación 2.2 (Conexión con el Escrito CXXIV)**.** *El Teorema de recuperabilidad del Escrito CXXIV afirmaba:* $k(p)$ *es recuperable desde* $\kappa(p)$ *si y solo si* $\gcd(qh, g) = 1$*. El Teorema 1.2 completa ese resultado: cuando* $\delta > 1$*, la indeterminación no es cualitativa sino cuantitativa: la fibra tiene exactamente* δ *elementos.*

3. Tabla de fibras para los diecinueve primos

m	p	g	$qh \bmod g$	δ	κ	$k(p)$	Fibra
2	499	2	1	1	1	1	$\{1\}$
3	186 793	3	2	1	0	0	$\{0\}$
4	5	4	1	1	3	3	$\{3\}$
4	24 917	4	1	1	2	2	$\{2\}$
5	11	5	2	1	3	4	$\{4\}$
5	191	5	3	1	2	4	$\{4\}$
5	36 791	5	3	1	0	0	$\{0\}$
6	19	6	3	3	0	4	$\{0, 2, 4\}$
6	67	6	5	1	3	3	$\{3\}$
7	778 247	7	4	1	4	1	$\{1\}$
8	769	8	0	8	0	3	$\{0, 1, 2, 3, 4, 5, 6, 7\}$
9	3 673	9	3	3	6	8	$\{2, 5, 8\}$
10	9 931	10	3	1	9	3	$\{3\}$
11	23	11	2	1	5	8	$\{8\}$
11	14 939	11	5	1	0	0	$\{0\}$
15	2 866 441	15	11	1	0	0	$\{0\}$
16	97	16	6	2	4	6	$\{6, 14\}$
18	37	18	2	2	8	13	$\{4, 13\}$
20	7 807 441	20	12	4	0	15	$\{0, 5, 10, 15\}$

Distribución de δ: $\delta = 1$ en 13/19 casos (68 %); $\delta \in \{2, 3, 4, 8\}$ en los 6 restantes. El caso $m = 8$, $p = 769$ es el único con fibra total ($\delta = g = 8$): $k(p) = 3$ no puede inferirse desde $\kappa = 0$.

4. $k(p)$ como componente irreducible

Teorema 4.1 (Variabilidad de $k(p)$)**.** *El índice* $k(p)$ *es el único componente de la identidad de síntesis* $\kappa(p) = A(p) - B(p) \bmod g$ *que no está determinado por los*

datos de reciprocidad de $A(p)$ y $B(p)$. Dado $\kappa(p) = A(p) - B(p)$, la variabilidad residual de $k(p)$ está gobernada enteramente por $\delta = \gcd(q_p h_p,\, g)$: $k(p)$ puede tomar exactamente δ valores en $\mathbb{Z}/g\mathbb{Z}$, todos ellos en la fibra $\varphi^{-1}(\kappa(p))$.

Observación 4.2 (Lo que $k(p)$ sabe que $\kappa(p)$ no sabe)**.** *Cuando $\delta > 1$, $k(p)$ contiene información que no está en $\kappa(p)$. Esa información adicional es exactamente lo que el Escrito CXXX mostró que no puede capturarse por congruencias de p: la distribución de $k(p)$ dentro de su fibra depende de la aritmética fina de $d(p) = \mathrm{ord}(2, p)$, conectando con la conjetura de Artin.*

Problema abierto 4.3 (Distribución de $k(p)$ dentro de la fibra)**.** *Cuando $\delta > 1$, ¿se distribuye $k(p)$ uniformemente entre los δ elementos de su fibra $\varphi^{-1}(\kappa(p))$? Una distribución uniforme dentro de la fibra, combinada con la distribución de $\kappa(p)$, daría la distribución completa de $k(p)$ en $\mathbb{Z}/g\mathbb{Z}$.*