Ciclos y Raíces Primitivas: Unificación de Sistemas Dinámicos Tipo Artin

Miguel Cerdá Bennassar

14 de Agosto de 2025

Resumen

Presentamos una generalización de los sistemas dinámicos tipo Collatz que unifica el estudio de ciclos periódicos con la teoría de raíces primitivas módulo primos. Para un primo impar $k \geq 3$ y una base $g \geq 2$ coprima con k, definimos la transformación $f_{g,k}(n) = \frac{n+a(n)k}{g}$ donde $a(n)$ es el único entero en $\{0, 1, \ldots, g-1\}$ tal que $n+a(n)k \equiv 0$ (mód g).

Demostramos que todas las órbitas periódicas no triviales de $f_{g,k}$ tienen longitud exactamente $\mathrm{ord}_k(g)$, y que el número total de ciclos es $\frac{k-1}{\mathrm{ord}_k(g)}$. Esto establece una equivalencia funcional: k admite un único ciclo largo si y solo si g es raíz primitiva módulo k, proporcionando así un *criterio dinámico* para la conjetura de Artin.

Introducimos el concepto de "huella Artin" $\mathcal{H}_k(g) = \left(\frac{k-1}{\mathrm{ord}_k(g)}, \mathrm{ord}_k(g)\right)$ que caracteriza completamente la estructura orbital del sistema. La demostración se basa en una semiconjugación entre $f_{g,k}$ y la multiplicación por g^{-1} en el grupo $(\mathbb{Z}/k\mathbb{Z})^\times$, reduciendo el análisis dinámico al estudio de automorfismos lineales en grupos multiplicativos finitos.

1. Introducción y motivación

La teoría de raíces primitivas establece que, dado un número primo p, existen enteros g que generan el grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^\times$ mediante sus potencias sucesivas. Dichos generadores, denominados *raíces primitivas*, desempeñan un papel fundamental en teoría de números, criptografía y en la formulación de la Conjetura de Artin.

El objetivo de este trabajo es proponer un marco dinámico que unifique el estudio de las raíces primitivas con sistemas iterativos del tipo *Collatz parametrizado*. A través de funciones de la forma

$$f_{g,k}(n) = \begin{cases} \frac{n}{2}, & n \text{ par}, \\ \frac{gn+k}{2}, & n \text{ impar}, \end{cases}$$

con k primo impar y g coprimo con k, se obtiene una correspondencia directa entre la dinámica de órbitas y la estructura multiplicativa de $(\mathbb{Z}/k\mathbb{Z})^\times$. Este enfoque permite caracterizar la existencia y longitud de ciclos en términos del orden multiplicativo de g módulo k, introduciendo la noción de *huella Artin* como herramienta conceptual.

De esta manera, el estudio se sitúa en la intersección entre sistemas dinámicos discretos y teoría algebraica de números, ofreciendo un lenguaje unificado para describir ciclos periódicos y propiedades de raíces primitivas.

2. Definiciones y enunciado principal

Sea $k \geq 3$ un primo impar y $g \geq 2$ un entero con $\gcd(g, k) = 1$. Definimos la transformación

$$f_{g,k}(n) = \frac{n + a(n)k}{g}$$

donde $a(n) \in \{0, 1, \ldots, g-1\}$ es el **único** entero tal que $n + a(n)k \equiv 0 \pmod{g}$.

Observación 2.1. La unicidad de $a(n)$ se garantiza porque k es invertible módulo g (ya que $\gcd(g, k) = 1$). Explícitamente, $a(n) \equiv -nk^{-1} \pmod{g}$.

Ejemplo 1 (Caso $g = 2$). Cuando $g = 2$, obtenemos

$$f_{2,k}(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \frac{n+k}{2} & \text{si } n \text{ es impar} \end{cases}$$

que generaliza la función de Collatz con parámetro k en lugar del valor fijo 3.

Teorema 2.1 (Regla General de Ciclos)**.** *Sea $L = \mathrm{ord}_k(g)$ el orden multiplicativo de g módulo k. Entonces:*

1. ***Dinámica inducida:*** *$f_{g,k}$ induce sobre $(\mathbb{Z}/k\mathbb{Z})^\times$ la aplicación lineal*

   $$\varphi(\bar{n}) = g^{-1}\bar{n}$$

   donde g^{-1} es el inverso multiplicativo de g módulo k.

2. ***Punto fijo único:*** *$n = k$ es punto fijo de $f_{g,k}$ y se tiene $a(k) = g - 1$.*

3. ***Longitud uniforme:*** *Toda órbita periódica no trivial de $f_{g,k}$ tiene longitud exactamente L.*

4. ***Conteo de ciclos:*** *El número de ciclos no triviales es $\frac{k-1}{L}$.*

3. Demostración del teorema principal

3.1. Semiconjugación fundamental

Proposición 3.1. *Para todo n, se cumple $f_{g,k}(n) \equiv g^{-1}n \pmod{k}$. ("inverso multiplicativo módulo k")*

Demostración. Como $k \mid a(n)k$, tenemos $n + a(n)k \equiv n \pmod{k}$. Sea $u = g^{-1} \pmod{k}$, entonces $gu = 1 + tk$ para algún $t \in \mathbb{Z}$. Por tanto:

$$g \cdot f_{g,k}(n) = n + a(n)k \equiv n \pmod{k}$$

$$\Rightarrow u \cdot g \cdot f_{g,k}(n) \equiv un \pmod{k}$$

Sustituyendo $ug = 1 + tk$ y reduciendo módulo k:

$$f_{g,k}(n) \equiv un = g^{-1}n \pmod{k}$$

□

La Proposición 3.1 establece la **semiconjugación**:

$$\pi \circ f_{g,k} = \varphi \circ \pi$$

donde $\pi : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ es la proyección canónica y $\varphi(\bar{n}) = g^{-1}\bar{n}$.

3.2. Análisis del punto fijo

Por definición, $a(k)$ satisface $k + a(k)k \equiv 0 \pmod{g}$, es decir:

$$k(1 + a(k)) \equiv 0 \pmod{g}$$

Como $\gcd(k, g) = 1$, se deduce $1 + a(k) \equiv 0 \pmod{g}$, lo que implica $a(k) \equiv -1 \pmod{g}$. En el rango $0 \leq a(k) \leq g - 1$, esto fuerza $a(k) = g - 1$. Por tanto:

$$f_{g,k}(k) = \frac{k + (g-1)k}{g} = \frac{gk}{g} = k$$

3.3. Estructura orbital en $(\mathbb{Z}/k\mathbb{Z})^\times$

El grupo $(\mathbb{Z}/k\mathbb{Z})^\times$ tiene $k - 1$ elementos y es cíclico. La transformación $\varphi(\bar{n}) = g^{-1}\bar{n}$ es un automorfismo cuyas órbitas son las clases laterales del subgrupo cíclico:

$$H = \langle g^{-1} \rangle = \{(g^{-1})^t : t \in \mathbb{Z}\}$$

Como $|H| = \mathrm{ord}_k(g) = L$, por el teorema de Lagrange:

- Toda órbita no nula de φ tiene longitud L
- El número de órbitas no nulas es $\frac{k-1}{L}$

3.4. Levantamiento de órbitas

Lema 3.2 (Levantamiento de órbitas)**.** *Cada órbita no nula de φ se levanta a un ciclo de $f_{g,k}$ de longitud exactamente L.*

Demostración. Sea $(n_0, n_1, \ldots, n_{\ell-1})$ un ciclo no trivial de $f_{g,k}$. Iterando la relación de recurrencia:

$$n_{t+1} = \frac{n_t + a_t k}{g} \Rightarrow n_\ell = \frac{n_0 + k\sum_{j=0}^{\ell-1} a_j g^j}{g^\ell}$$

Multiplicando por g^ℓ y usando la condición cíclica $n_\ell = n_0$:

$$(g^\ell - 1)n_0 = k\sum_{j=0}^{\ell-1} a_j g^j$$

Esto implica $k \mid (g^\ell - 1)n_0$. En un ciclo no trivial, $k \nmid n_0$ (pues de lo contrario la órbita sería eventualmente periódica hacia el punto fijo k), así que necesariamente:

$$k \mid (g^\ell - 1) \Leftrightarrow g^\ell \equiv 1 \pmod{k}$$

Por definición de $L = \mathrm{ord}_k(g)$, esto implica $L \mid \ell$.

Recíprocamente, la proyección $\pi(n_i) \equiv n_i \pmod{k}$ debe recorrer una órbita completa de φ de longitud L antes de que el ciclo se cierre. Por tanto, $\ell = L$. □

4. Aplicaciones a la conjetura de Artin

Corolario 4.1 (Criterio dinámico de Artin)**.**

Número de ciclos no triviales $= 1 \Leftrightarrow \mathrm{ord}_k(g) = k - 1 \Leftrightarrow g$ *es raíz primitiva módulo* k

Definición 4.2 (Huella Artin)**.** Para un primo k y base g coprima con k, definimos la **huella Artin** como:

$$\mathcal{H}_k(g) = \left(\frac{k-1}{\mathrm{ord}_k(g)}, \mathrm{ord}_k(g)\right)$$

La huella Artin codifica completamente la estructura orbital:

- Si $\mathcal{H}_k(g) = (1, k-1)$, entonces g es raíz primitiva módulo k
- Si $\mathcal{H}_k(g) = (d, (k-1)/d)$, entonces el subgrupo $\langle g \rangle$ tiene índice d en $(\mathbb{Z}/k\mathbb{Z})^\times$

Observación 4.1 (Test múltiple). Para un conjunto de bases candidatas $G = \{g_1, \ldots, g_t\}$, el vector de huellas $(\mathcal{H}_k(g_i))_{i=1}^t$ permite determinar simultáneamente cuáles de las bases son raíces primitivas módulo k.

Nota sobre conexiones con OEIS. Para el caso en que $k = p$ es primo, el número de ciclos de $f_{g,k}$ es

$$\frac{p-1}{\mathrm{ord}_p(g)},$$

donde $\mathrm{ord}_p(g)$ es el menor entero positivo x tal que $g^x \equiv 1 \pmod{p}$. Este cociente coincide exactamente con secuencias catalogadas en OEIS. Por ejemplo, para $g = 2$ corresponde a la sucesión A001917, definida como $a(n) = (p-1)/\mathrm{ord}_p(2)$ con $p = \mathrm{prime}(n)$. De forma análoga, para $g = 3$ se obtiene A094593, y para otros generadores existen sucesiones similares (cf. A211452 para $g = 7$, A211454 para $g = 9$).
Nuestro aporte no consiste en tabular estos valores, sino en mostrar que son precisamente el *número de ciclos* de $f_{g,k}$, mientras que la *longitud de cada ciclo* viene dada por $\mathrm{ord}_k(g)$. De este modo, las sucesiones de OEIS aparecen aquí interpretadas como invariantes dinámicos de un sistema tipo Collatz, lo que permite unificar su lectura con la teoría de raíces primitivas y la *huella Artin*.

5. Extensiones y comentarios

Observación 5.1 (Caso k compuesto e impar). Cuando k es compuesto e impar, la estructura de los ciclos bajo $f_{g,k}$ se vuelve más compleja: ya no se garantiza un único ciclo largo asociado a una raíz primitiva. En su lugar, aparecen descomposiciones en ciclos de longitudes que dividen a $\varphi(k)$. Esto refleja la factorización de $(\mathbb{Z}/k\mathbb{Z})^\times$ en producto de grupos cíclicos.

Ejemplo 5.1 (Caso k=9, g=2)**.** El grupo $(\mathbb{Z}/9\mathbb{Z})^\times$ es isomorfo a C_6, generado por 2. Aquí $\mathrm{ord}_9(2) = 6$ y $\varphi(9) = 6$, de modo que 2 es raíz primitiva módulo 9. La función $f_{2,9}$ presenta un ciclo de longitud 6 sobre el bloque de unidades. En cambio, los elementos no coprimos con 9 (múltiplos de 3) generan órbitas degeneradas que no aparecen en el caso primo.

Ejemplo 5.2 (Caso k=15, g=2)**.** El grupo $(\mathbb{Z}/15\mathbb{Z})^\times$ es isomorfo a $C_4 \times C_2$. Aquí $\mathrm{ord}_{15}(2) = 4$, y la estructura orbital de $f_{2,15}$ refleja esta factorización: aparecen ciclos de longitud 4, pero no existe un ciclo único de longitud $\varphi(15) = 8$. Esto muestra cómo los módulos compuestos generan dinámicas más fragmentadas.

Observación 5.2 (Dominancia por la base). Para k primo, el comportamiento de $f_{g,k}$ está dominado por la base g: si g es raíz primitiva, se obtiene un único ciclo de longitud $k-1$; si no lo es, los ciclos tienen longitudes que dividen $\mathrm{ord}_k(g)$. Esta dicotomía conecta de forma directa con la teoría de órdenes multiplicativos y raíces primitivas.

Ejemplo 5.3 (Cálculo explícito con k=7, g=3)**.** Se tiene $\mathrm{ord}_7(3) = 6$ (pues $3^6 \equiv 1 \pmod{7}$ y $3^d \not\equiv 1$ para $d < 6$). La huella de Artin es $\mathcal{H}_7(3) = (1, 6)$, de donde se concluye que 3 es raíz primitiva módulo 7. En consecuencia, $f_{3,7}$ presenta un único ciclo no trivial de longitud 6 en el bloque de unidades. Computacionalmente, cualquier $n \not\equiv 0 \pmod{7}$ entra en un ciclo de exactamente 6 elementos bajo la iteración de $f_{3,7}$.

Conexión conceptual con la Conjetura de Artin. La Conjetura de Artin establece la existencia de infinitos primos para los cuales una base fija g es raíz primitiva. Nuestro

planteamiento no avanza en su demostración, pero sí ofrece una perspectiva conceptual distinta: la dinámica asociada permite "iluminar" la estructura de estos casos, haciendo visibles los ciclos completos en los que g actúa como generador del grupo multiplicativo. En otras palabras, lo que antes se intuía sólo como una propiedad aritmética abstracta, aquí aparece representado como un fenómeno dinámico concreto: la presencia de un ciclo máximo de longitud $p-1$.

Consideraciones de complejidad. Para un primo p y una base g, la condición "g es raíz primitiva módulo p" equivale a $\mathrm{ord}_p(g) = p-1$. La verificación es eficiente siempre que se disponga de la factorización de $p-1$: basta comprobar que $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ para cada primo $q \mid (p-1)$. Dicho certificado de factorización permite un test en tiempo polinómico. En ausencia de esta factorización, no se conoce un algoritmo determinista en tiempo polinómico que resuelva el problema en general.

En contraste, *encontrar* primos p para los cuales g sea raíz primitiva es un problema mucho más delicado: está directamente relacionado con la conjetura de Artin sobre raíces primitivas y con resultados de tipo Chebotarev en teoría analítica de números. Actualmente no se dispone de un procedimiento incondicional en tiempo polinómico (en $\log p$) que genere sistemáticamente tales primos; bajo hipótesis analíticas fuertes se obtienen densidades y cotas efectivas, pero el caso general sigue abierto.

6. Conclusiones y perspectivas

Hemos establecido una correspondencia biunívoca entre la estructura de ciclos de los sistemas dinámicos $f_{g,k}$ y las propiedades de raíz primitiva en teoría de números. Esta conexión sugiere nuevas direcciones de investigación:

- **Métodos probabilísticos:** Análisis estadístico de huellas de Artin para grandes conjuntos de primos.
- **Algoritmos mejorados:** Explotación de la estructura dinámica para acelerar tests de primitividad.
- **Generalizaciones algebraicas:** Extensión a cuerpos finitos y variedades aritméticas.

El teorema principal proporciona así no solo una unificación conceptual de dos áreas clásicas, sino también herramientas concretas para abordar problemas abiertos desde perspectivas renovadas.

Referencias

[1] E. Artin, *Über eine neue Art von L-Reihen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **3** (1924), 89–108.

[2] C. Hooley, *On Artin's conjecture*, Journal für die reine und angewandte Mathematik **225** (1967), 209–220.

[3] M.R. Murty, *Artin's conjecture for primitive roots*, The Mathematical Intelligencer **10** (1988), 59–67.

[4] J.C. Lagarias, *The 3x+1 problem and its generalizations*, American Mathematical Monthly **92** (1985), 3–23.

[5] T. Tao, *Almost all orbits of the Collatz map attain almost bounded values*, Forum of Mathematics, Pi **10** (2022), e12.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[7] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 2000.

[8] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979.

[9] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

[10] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999.

[11] A. Wieferich, *Zum letzten Fermat'schen Theorem*, Journal für die reine und angewandte Mathematik **136** (1909), 293–302.

[12] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.

[13] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics **210**, Springer-Verlag, New York, 2002.

[14] P.J. Stephens, *Prime divisors of second-order linear recurrences, I*, Journal of Number Theory **8** (1976), 313–332.

[15] P. Moree, *Artin's primitive root conjecture - a survey*, Integers **12** (2012), 1305–1416.