

Caracterización dinámica del conjunto de Artin $S(2)$

Miguel Cerdá Bennassar

Julio de 2025 (revisión de septiembre de 2026)

Resumen

Se aplica al conjunto $S(2)$ de la conjetura de Artin la descripción algebraica de las funciones

$$g_k(n) = \begin{cases} n/2, & n \text{ par}, \\ (n+k)/2, & n \text{ impar}, \end{cases} \quad k \text{ impar},$$

establecida en la sección precedente. Se demuestra que un primo impar p pertenece a $S(2)$ si y sólo si g_p genera un único ciclo, necesariamente de longitud $p-1$, sobre $\{1, 2, \dots, p-1\}$.

Se precisa además la estructura fuera de $S(2)$: el número de ciclos es exactamente $(p-1)/\text{ord}_p(2)$ y todos tienen longitud $\text{ord}_p(2)$. En consecuencia, el caso de dos ciclos no caracteriza al complemento de $S(2)$, sino únicamente a los primos con $\text{ord}_p(2) = (p-1)/2$, para los cuales $\langle 2 \rangle$ es el subgrupo de los residuos cuadráticos. Se discute la extensión a módulos impares compuestos, donde el recuento $\varphi(k)/\text{ord}_k(2)$ vale sobre el grupo de unidades y el resto de los elementos se trata mediante la autosemejanza de la sección precedente.

La caracterización es exacta pero no es un método de cálculo: contar ciclos por iteración cuesta $O(k)$, mientras que el orden multiplicativo de 2 se obtiene en tiempo polilogarítmico. Su valor es de reformulación, no computacional.

1. Introducción

La conjetura de Artin sobre raíces primitivas, formulada en 1927, afirma que todo entero a que no sea -1 ni un cuadrado perfecto es raíz primitiva módulo infinitos primos. En el caso $a = 2$, el conjunto

$$S(2) = \{p \text{ primo impar} : 2 \text{ es raíz primitiva módulo } p\}$$

ocupa un lugar central en teoría de números.

Aquí lo estudiamos desde la dinámica discreta inducida por

$$g_k(n) = \begin{cases} \frac{n}{2}, & n \text{ par}, \\ \frac{n+k}{2}, & n \text{ impar}, \end{cases} \quad k \text{ impar}.$$

Cuando $k = p$ es primo impar, g_p actúa sobre $\{1, 2, \dots, p-1\}$, que se identifica con $(\mathbb{Z}/p\mathbb{Z})^*$, y esa acción es la multiplicación por 2^{-1} . La estructura de ciclos queda entonces determinada por el orden multiplicativo de 2.

El objetivo es formular con exactitud esa correspondencia. En particular se corrige una interpretación demasiado fuerte, según la cual todo primo fuera de $S(2)$ produciría dos ciclos: el número de ciclos es el índice del subgrupo generado por 2, y el caso de dos ciclos corresponde sólo al subcaso $\text{ord}_p(2) = (p-1)/2$.

2. La conjetura de Artin y el conjunto $S(2)$

Definición 2.1 (Conjunto de Artin para $a = 2$). $S(2)$ está formado por los primos impares p tales que 2 es raíz primitiva módulo p , es decir, tales que $\text{ord}_p(2) = p-1$.

Sus primeros elementos son

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, \dots$$

y la conjetura de Artin predice que el conjunto es infinito.

3. Fundamento algebraico

Teorema 3.1 (Acción multiplicativa). Sea k impar. Para toda clase $x \in (\mathbb{Z}/k\mathbb{Z})^*$, la función g_k induce la transformación $x \mapsto 2^{-1}x$ (mód k).

Demostración. Sea n coprimo con k . Si n es par, $g_k(n) = n/2$ y $2g_k(n) = n$, luego $g_k(n) \equiv 2^{-1}n$. Si n es impar, $g_k(n) = (n+k)/2$ y $2g_k(n) = n+k \equiv n$, luego también $g_k(n) \equiv 2^{-1}n$. $\square$

Corolario 3.2 (Longitud de las órbitas). Toda órbita de g_k sobre $(\mathbb{Z}/k\mathbb{Z})^*$ tiene longitud $\text{ord}_k(2^{-1}) = \text{ord}_k(2)$.

Demostración. La órbita de x es $x, 2^{-1}x, 2^{-2}x, \dots$, y retorna a x cuando $2^{-m} \equiv 1$, es decir para $m = \text{ord}_k(2^{-1})$, que coincide con $\text{ord}_k(2)$. $\square$

Corolario 3.3 (Número de ciclos sobre las unidades). El número de ciclos de g_k sobre $(\mathbb{Z}/k\mathbb{Z})^*$ es $\varphi(k)/\text{ord}_k(2)$, y todos tienen longitud $\text{ord}_k(2)$.

Demostración. Las órbitas particionan un conjunto de $\varphi(k)$ elementos en bloques de $\text{ord}_k(2)$ elementos cada uno. $\square$

Comentario 3.4. Si k es compuesto, el Corolario 3.3 describe únicamente los elementos coprimos con k . Los restantes se tratan mediante la relación de autosemejanza $g_k(du) = d g_{k/d}(u)$ establecida en la sección precedente, que reduce cada clase de divisibilidad al mismo problema para el módulo k/d . Conviene tener presente esa distinción al leer los ejemplos compuestos de la Sección 7.

4. Caracterización dinámica de $S(2)$

Teorema 4.1 (Caracterización dinámica). Sea p un primo impar. Son equivalentes:

1. $p \in S(2)$;
2. $\text{ord}_p(2) = p-1$;

3. g_p genera un único ciclo sobre $\{1, 2, \dots, p-1\}$;

4. ese único ciclo tiene longitud $p-1$.

Demostración. $(1) \Leftrightarrow (2)$ es la definición. Por el Teorema 3.1, g_p actúa sobre $\{1, \dots, p-1\} = (\mathbb{Z}/p\mathbb{Z})^*$ como multiplicación por 2^{-1} , y por el Corolario 3.3 el número de ciclos es $(p-1)/\text{ord}_p(2)$, todos de longitud $\text{ord}_p(2)$. Ese número vale 1 si y sólo si $\text{ord}_p(2) = p-1$, lo que prueba $(2) \Leftrightarrow (3) \Leftrightarrow (4)$. $\square$

4.1. Punto fijo

La función g_p posee siempre el punto fijo p , pues $g_p(p) = (p+p)/2 = p$. Dicho punto no pertenece a $\{1, \dots, p-1\}$ y no interviene en el recuento de ciclos.

5. Estructura fuera de $S(2)$

Teorema 5.1 (Estructura general). *Sea p un primo impar. Entonces g_p induce sobre $\{1, 2, \dots, p-1\}$ exactamente $(p-1)/\text{ord}_p(2)$ ciclos disjuntos, todos de longitud $\text{ord}_p(2)$. Si $p \notin S(2)$, ese número es estrictamente mayor que 1, pero no necesariamente igual a 2.*

Demostración. Es el Corolario 3.3 con $k = p$ y $\varphi(p) = p-1$. $\square$

Observación 5.2 (Corrección conceptual). Que p no pertenezca a $S(2)$ significa únicamente que $\langle 2 \rangle$ es un subgrupo propio de $(\mathbb{Z}/p\mathbb{Z})^*$. Su índice puede ser 2, 3, 4, 6 o cualquier divisor de $p-1$ mayor que uno, y la fragmentación dinámica tiene exactamente ese número de bloques.

5.1. El caso de índice dos

Proposición 5.3 (Dos ciclos). *Sea p un primo impar. Son equivalentes: que g_p induzca exactamente dos ciclos sobre $\{1, \dots, p-1\}$; que $\text{ord}_p(2) = (p-1)/2$; y que $\langle 2 \rangle$ tenga índice 2 en $(\mathbb{Z}/p\mathbb{Z})^*$.*

Demostración. Por el Teorema 5.1, el número de ciclos es $(p-1)/\text{ord}_p(2)$, que vale 2 exactamente cuando $\text{ord}_p(2) = (p-1)/2$; y el orden del subgrupo $\langle 2 \rangle$ es precisamente $\text{ord}_p(2)$. $\square$

Proposición 5.4 (Interpretación por clases laterales). *Si $\text{ord}_p(2) = (p-1)/2$, los dos ciclos son las dos clases laterales de $\langle 2 \rangle$ en $(\mathbb{Z}/p\mathbb{Z})^*$: uno es $\langle 2 \rangle$ y el otro $g\langle 2 \rangle$ para cualquier g fuera del subgrupo.*

Demostración. La multiplicación por 2^{-1} preserva cada clase lateral de $\langle 2 \rangle$. Como cada una tiene $(p-1)/2$ elementos y la longitud de cada órbita es también $(p-1)/2$, cada clase lateral constituye un único ciclo. $\square$

Observación 5.5 (Residuos cuadráticos). Como $(\mathbb{Z}/p\mathbb{Z})^*$ es cíclico, su único subgrupo de índice 2 es el de los residuos cuadráticos. Por tanto, cuando $\text{ord}_p(2) = (p-1)/2$, el subgrupo $\langle 2 \rangle$ coincide con los residuos cuadráticos y el otro ciclo con los no residuos. Esto ocurre sólo en ese caso, y no describe la situación general fuera de $S(2)$.

6. Ejemplos

6.1. Casos en $S(2)$

Ejemplo 6.1. Para $p = 37$ se tiene $\text{ord}_{37}(2) = 36$, luego $37 \in S(2)$ y g_{37} induce un único ciclo de longitud 36. Lo mismo ocurre con $p = 53$ y $p = 61$, de órdenes 52 y 60.

6.2. Casos con exactamente dos ciclos

Ejemplo 6.2. Para $p = 7$, $\text{ord}_7(2) = 3 = (7 - 1)/2$, luego hay dos ciclos de longitud 3, de mínimos 1 y 3. Para $p = 23$, $\text{ord}_{23}(2) = 11 = (23 - 1)/2$, luego hay dos ciclos de longitud 11, de mínimos 1 y 5. Para $p = 71$, $\text{ord}_{71}(2) = 35$ y los mínimos son 1 y 7; para $p = 719$, $\text{ord}_{719}(2) = 359$ y los mínimos son 1 y 11; para $p = 7193$, $\text{ord}_{7193}(2) = 3596$ y los mínimos son 1 y 3.

6.3. Casos con más de dos ciclos

Ejemplo 6.3. Para $p = 43$ se tiene $\text{ord}_{43}(2) = 14$, de modo que g_{43} induce $42/14 = 3$ ciclos de longitud 14, con mínimos 1, 3 y 7. Para $p = 31$, $\text{ord}_{31}(2) = 5$ y aparecen $30/5 = 6$ ciclos de longitud 5, con mínimos 1, 3, 5, 7, 11, 15. Para $p = 73$, $\text{ord}_{73}(2) = 9$ y aparecen 8 ciclos de longitud 9.

Estos casos son la razón de la Observación 5.2: la aparición de exactamente dos ciclos caracteriza el índice 2, no el complemento de $S(2)$.

6.4. Tabla representativa

p	$\text{ord}_p(2)$	Ciclos	Longitud	Mínimos	Situación
7	3	2	3	1, 3	índice 2
23	11	2	11	1, 5	índice 2
31	5	6	5	1, 3, 5, 7, 11, 15	índice 6
37	36	1	36	1	$p \in S(2)$
43	14	3	14	1, 3, 7	índice 3
53	52	1	52	1	$p \in S(2)$
71	35	2	35	1, 7	índice 2
719	359	2	359	1, 11	índice 2
7193	3596	2	3596	1, 3	índice 2

7. Extensión al caso compuesto

Teorema 7.1 (Caso compuesto). *Sea k impar. La dinámica de g_k sobre $(\mathbb{Z}/k\mathbb{Z})^*$ se descompone en $\varphi(k)/\text{ord}_k(2)$ ciclos, todos de longitud $\text{ord}_k(2)$.*

Demostración. Es el contenido del Corolario 3.3. □

Observación 7.2 (Precaución interpretativa). Para k compuesto, la lectura en términos de la conjetura de Artin deja de tener sentido directo, porque $S(2)$ es un conjunto de primos. La estructura dinámica sobre las unidades sigue siendo válida, pero los ejemplos compuestos no permiten extraer conclusiones sobre pertenencia a $S(2)$.

Ejemplo 7.3. La tabla siguiente recoge cuatro módulos compuestos. Las tres primeras columnas se refieren a los ciclos sobre $(\mathbb{Z}/k\mathbb{Z})^*$; la última indica el número total de ciclos sobre $\{1, \dots, k-1\}$, que incluye los elementos no coprimos con k según el Comentario 3.4.

k	$\varphi(k)$	$\text{ord}_k(2)$	Ciclos en $(\mathbb{Z}/k\mathbb{Z})^*$	Mínimos	Ciclos totales
15	8	4	2	1, 7	4
371	312	156	2	1, 3	5
713	660	55	12	—	20
9713	8820	4410	2	1, 3	4

El caso $k = 713$ muestra que la aparición de dos ciclos no es estable al pasar a módulos compuestos. En $k = 15$, los dos ciclos sobre las unidades son $\{1, 2, 4, 8\}$ y $\{7, 11, 13, 14\}$; obsérvese que 3 no es unidad módulo 15 y no interviene en ellos.

8. Alcance

8.1. La caracterización no es un método de cálculo

El Teorema 4.1 permite decidir la pertenencia a $S(2)$ contando ciclos, pero ese procedimiento es peor que el directo. Iterar g_p sobre $\{1, \dots, p-1\}$ y contar órbitas exige recorrer los $p-1$ elementos, con coste $O(p)$, mientras que $\text{ord}_p(2)$ se calcula factorizando $p-1$ y realizando exponenciaciones modulares, en tiempo polilogarítmico una vez conocida esa factorización. En una prueba sobre $p = 200\,003$, el recuento de ciclos tardó unas trescientas cuarenta veces más que el cálculo directo del orden, y la diferencia crece con p .

La caracterización es, por tanto, una reformulación exacta y no una herramienta de cómputo. Su interés reside en traducir el índice del subgrupo $\langle 2 \rangle$ en un rasgo visible de la descomposición orbital.

8.2. Qué no se obtiene

El resultado no aporta información sobre la conjetura de Artin. Que $S(2)$ sea infinito, o que su densidad sea la constante de Artin, son afirmaciones sobre la distribución de $\text{ord}_p(2)$ al variar p , y la lectura dinámica no cambia esa distribución: sólo la nombra de otro modo. El enunciado del Teorema 4.1 es una reescritura de la definición de orden multiplicativo.

8.3. Extensiones

El mismo argumento se aplica a $S(a)$ para cualquier a coprimo con el módulo, sin más que sustituir g_k por la función que realiza la multiplicación por a^{-1} . Queda abierta, como cuestión independiente, la clasificación de los enteros impares k con $\text{ord}_k(2) = \varphi(k)/2$, que son exactamente los que producen dos ciclos sobre las unidades.

9. Conclusiones

Un primo impar p pertenece a $S(2)$ si y sólo si g_p genera un único ciclo sobre $\{1, 2, \dots, p-1\}$, necesariamente de longitud $p-1$. Con mayor precisión, el número de ciclos es siempre $(p-1)/\text{ord}_p(2)$ y todos tienen la misma longitud, de modo que:

- un único ciclo corresponde exactamente a $p \in S(2)$;
- dos ciclos corresponden exactamente a $\text{ord}_p(2) = (p-1)/2$, caso en el que $\langle 2 \rangle$ es el subgrupo de los residuos cuadráticos;
- los demás primos fuera de $S(2)$ producen tantos ciclos como indique el índice del subgrupo, que puede ser cualquier divisor de $p-1$ mayor que uno.

La descomposición orbital reproduce, pues, el índice de $\langle 2 \rangle$ con exactitud. Se trata de una traducción fiel de una propiedad algebraica conocida a un lenguaje dinámico, sin ventaja computacional ni consecuencias sobre la conjetura de Artin.

Referencias

- [1] M. Cerdá Bennassar, *Las funciones g_k como acción multiplicativa: estructura cíclica completa*, 2025.
- [2] E. Artin, *Über eine neue Art von L -Reihen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **3** (1927), 89–108.
- [3] C. Hooley, *On Artin's conjecture*, Journal für die reine und angewandte Mathematik **225** (1967), 209–220.
- [4] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, The Quarterly Journal of Mathematics **37** (1986), 27–38.
- [5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer-Verlag, 1990.