

Collatz e indecidibilidad

VI. La divisibilidad de los numeradores de ciclo: equidistribución módulo p y el caso de 139

Miguel Cerdá Bennassar

Septiembre de 2026

Resumen

Un collar de palabras de paridades con K pasos y o pasos impares genera un ciclo entero de la función de Collatz acelerada si y solo si $D = 2^K - 3^o$ divide a su numerador $\varphi(s)$. El escrito V preguntó por qué $139 = |2^{11} - 3^7|$ divide al numerador del ciclo de -17 (Problema 6.3). Este escrito separa las divisibilidades estructurales de las aleatorias. Entre las estructurales, se demuestra que la divisibilidad es invariante por rotación y que las potencias de una palabra heredan el ciclo de su raíz, de modo que ciertos factores de D , como $2^{K'} + 3^{o'}$, dividen automáticamente a muchos numeradores. Entre las aleatorias, se demuestra que para cada primo $p \geq 5$ fijo los numeradores se equidistribuyen módulo p cuando la longitud de la palabra crece (Teorema 4.1), y un recuento exacto por programación dinámica muestra la misma equidistribución cuando se fija además el número de pasos impares. Para $p = 139$, el retículo de relaciones entre 2 y 3 es genérico, la palabra del ciclo de -17 no es la palabra equilibrada que distinguen las cotas de Halbeisen y Hungerbühler, y no aparece ninguna divisibilidad estructural. La respuesta al Problema 6.3 es, pues, que no hay razón estructural visible: bajo el modelo uniforme, el número esperado de collares con numerador divisible por 139 es $30/139 \approx 0,22$, y se observa exactamente uno. El régimen relevante para ciclos largos, en el que el primo crece con K , queda abierto.

1. Introducción

Seguimos la notación de los escritos IV y V [1, 2]. Para una palabra de paridades $s \in \{0, 1\}^K$ con o unos, el numerador $\varphi(s)$ se define por

$$\varphi(\emptyset) = 0, \quad \varphi(s0) = \varphi(s), \quad \varphi(s1) = 3\varphi(s) + 2^{|s|},$$

y el único punto fijo racional de la composición de ramas asociada es $x_s = \varphi(s)/(2^K - 3^o)$ (Lagarias [4]). El ciclo generado por s es entero si y solo si $D = 2^K - 3^o$ divide a $\varphi(s)$.

El escrito V estudió el número esperado de ciclos enteros bajo el supuesto de que los numeradores se comportan como enteros aleatorios módulo D , y señaló que ese supuesto no está demostrado. Este escrito lo examina factor a factor: para cada primo $p \mid D$, ¿se distribuyen los numeradores uniformemente módulo p ?

2. Divisibilidad módulo un primo

Definición 2.1. Para un primo $p \geq 5$, el *retículo de relaciones* es

$$\Lambda_p = \{(a, b) \in \mathbb{Z}^2 : 2^a \equiv 3^b \pmod{p}\}.$$

Es un subgrupo de índice finito de $\mathbb{Z}^2$, y $p \mid 2^K - 3^o$ si y solo si $(K, o) \in \Lambda_p$.

Proposición 2.2 (Invariancia por rotación). *Sea p un primo que divide a $2^K - 3^o$, sea s una palabra con esos parámetros y sea s' la rotación de s que empieza en su segunda letra. Entonces $p \mid \varphi(s)$ si y solo si $p \mid \varphi(s')$.*

Demostración. Los puntos x_s y $x_{s'}$ son consecutivos en el mismo ciclo racional: $x_{s'} = T(x_s)$. Si s empieza por 0, esto da $\varphi(s') = \varphi(s)/2$; si empieza por 1, da $\varphi(s') = (3\varphi(s) + D)/2$. En ambos casos $\varphi(s') \equiv u\varphi(s) \pmod{p}$ con $u \in \{2^{-1}, 3 \cdot 2^{-1}\}$ invertible módulo p . $\square$

La divisibilidad por p es, por tanto, una propiedad de collares, no de palabras.

3. Divisibilidades estructurales

Lema 3.1 (Concatenación). *Para palabras u, v , $\varphi(uv) = 3^{o(v)}\varphi(u) + 2^{|u|}\varphi(v)$.*

Demostración. Por inducción sobre $|v|$, a partir de la definición recursiva. $\square$

Proposición 3.2 (Potencias). *Si u tiene K' letras y o' unos, y $j \geq 1$, entonces*

$$\varphi(u^j) = \varphi(u) \frac{2^{jK'} - 3^{jo'}}{2^{K'} - 3^{o'}}, \quad \text{y por tanto} \quad x_{u^j} = x_u.$$

En particular, para $j = 2$, el factor $2^{K'} + 3^{o'}$ de $2^{2K'} - 3^{2o'}$ divide a $\varphi(u^2)$ para toda palabra u .

Demostración. Aplicando el Lema 3.1 repetidamente, $\varphi(u^j) = \varphi(u) \sum_{i=0}^{j-1} 3^{o'(j-1-i)} 2^{K'i}$, que es la suma geométrica indicada. $\square$

Estas divisibilidades son automáticas y no dicen nada nuevo sobre ciclos: la potencia u^j genera el mismo ciclo que u . Pero sesgan cualquier recuento que no las descarte.

Ejemplo 3.3. Para $(K, o) = (20, 4)$ se tiene $2^{20} - 3^4 = 5 \cdot 7 \cdot 29 \cdot 1033$, con $1033 = 2^{10} + 3^2$. Entre las 4845 palabras con esos parámetros, la proporción de numeradores divisibles por 1033 es unas 9,6 veces la esperada bajo uniformidad; el exceso procede de los cuadrados de palabras con parámetros $(10, 2)$.

En lo que sigue, cuando se comparen recuentos con la predicción uniforme, conviene recordar que las palabras no primitivas aportan divisibilidades estructurales de este tipo.

4. Equidistribución para un primo fijo

Teorema 4.1. *Sea $p \geq 5$ primo. Si s se elige uniformemente entre las 2^K palabras de longitud K , entonces, para todo $a \in \mathbb{F}_p$,*

$$\lim_{K \rightarrow \infty} \Pr(\varphi(s) \equiv a \pmod{p}) = \frac{1}{p}.$$

Demostración. Sea m el orden de 2 módulo p ; como $p \geq 5$, $m \geq 2$. Sea X_L el resto de $\varphi(s_1 \cdots s_L)$ módulo p . Por la definición recursiva,

$$X_{L+1} = X_L \quad \text{o} \quad X_{L+1} = 3X_L + 2^L,$$

cada caso con probabilidad $1/2$ e independientemente del pasado. Así, la distribución de X_{L+1} se obtiene de la de X_L aplicando el núcleo de transición M_ℓ , con $\ell = L \pmod{m}$, dado por

$$M_\ell(x, \cdot) = \frac{1}{2} \delta_x + \frac{1}{2} \delta_{g_\ell(x)}, \quad g_\ell(x) = 3x + 2^\ell.$$

Como 3 es invertible módulo p , cada g_ℓ es una biyección de $\mathbb{F}_p$, y cada M_ℓ es una media de dos matrices de permutación, luego doblemente estocástica. El núcleo de un periodo completo, $P = M_0 M_1 \cdots M_{m-1}$, es también doblemente estocástico.

P es aperiódico, porque $P(x, x) \geq 2^{-m} > 0$ (todas las letras iguales a 0). Es irreducible: $P(x, g_\ell(x)) \geq 2^{-m}$ para cada ℓ (una sola letra igual a 1, en la posición ℓ), y las biyecciones $g_0, \dots, g_{m-1}$ generan un grupo que contiene la traslación

$$g_0 \circ g_1^{-1}(x) = x - 1,$$

luego actúa transitivamente sobre $\mathbb{F}_p$. Una cadena de Markov finita, irreducible, aperiódica y con matriz doblemente estocástica converge a la distribución uniforme. Escribiendo $K = nm + r$ con $0 \leq r < m$, la distribución de X_K es $\delta_0 P^n M_0 \cdots M_{r-1}$, que converge a la uniforme, pues la uniforme es invariante por cada M_ℓ . $\square$

El teorema no fija el número de unos. Para la cuestión de los ciclos interesa el caso en que se fijan (K, o) con $(K, o) \in \Lambda_p$. La misma recursión permite contar exactamente, por programación dinámica sobre los estados $(o, \varphi \bmod p)$, cuántas palabras con parámetros (K, o) tienen $p \mid \varphi(s)$, sin enumerar las palabras.

Observación 4.2 (Recuentos exactos). La tabla da, para varios pares (K, o) con $p \mid 2^K - 3^o$, el cociente $\rho = p \cdot N / \binom{K}{o}$, donde N es el número exacto de palabras con $p \mid \varphi(s)$. Bajo uniformidad, $\rho = 1$.

p	(K, o)	N	$\binom{K}{o}$	ρ
5	(8, 4)	22	70	1,571
5	(20, 12)	26 700	125 970	1,060
5	(40, 24)	$1,258 \cdot 10^{10}$	$6,285 \cdot 10^{10}$	1,001
5	(80, 52)	$5,821 \cdot 10^{20}$	$2,910 \cdot 10^{21}$	1,000
73	(15, 8)	150	6435	1,702
73	(30, 16)	2 010 690	145 422 675	1,009
73	(48, 28)	$2,293 \cdot 10^{11}$	$1,674 \cdot 10^{13}$	1,000
139	(11, 7)	11	330	4,633
139	(22, 14)	2607	319 770	1,133
139	(33, 21)	2 563 517	354 817 320	1,004
139	(44, 28)	$2,998 \cdot 10^9$	$4,167 \cdot 10^{11}$	1,000

En los tres casos, las desviaciones para longitudes pequeñas desaparecen rápidamente al crecer K . En las longitudes pequeñas, una sola coincidencia pesa mucho: para (11, 7) y $p = 139$, las 11 palabras divisibles son las rotaciones de un único collar, el del ciclo de -17 .

Conjetura 4.3. Sea $p \geq 5$ primo y sea (K_n, o_n) una sucesión de pares de Λ_p con $K_n \rightarrow \infty$ y o_n/K_n en un compacto de $(0, 1)$. Entonces la proporción de palabras con parámetros (K_n, o_n) cuyo numerador es divisible por p tiende a $1/p$.

Observación 4.4. La Conjetura 4.3 es una versión condicionada del Teorema 4.1. La dificultad es que fijar el número de unos introduce una condición global en la cadena de Markov; técnicas de tipo teorema local del límite, o un análisis espectral del núcleo con un parámetro de inclinación para los unos, deberían permitir demostrarla. La rapidez de la convergencia observada sugiere una brecha espectral apreciable.

5. El caso de 139

Para el par $(11, 7)$, $D = 2^{11} - 3^7 = -139$ es primo. Como 11 es primo, las $\binom{11}{7} = 330$ palabras son primitivas y forman 30 collares. Exactamente uno de ellos tiene numerador divisible por 139: el del ciclo de -17 , con palabra de paridades

$$s_{-17} = 11110111000$$

leída desde -17 . La predicción uniforme es $30/139 \approx 0,216$ collares.

Ninguna divisibilidad estructural. Como 139 es primo y todas las palabras son primitivas, no interviene ninguno de los mecanismos de la Sección 3.

Un retículo genérico. Módulo 139, tanto 2 como 3 son raíces primitivas. El retículo Λ_{139} tiene índice 138 y base reducida

$$(-4, 10), \quad (11, 7),$$

de longitudes $\sqrt{116} \approx 10,8$ y $\sqrt{170} \approx 13,0$, comparables a $\sqrt{138} \approx 11,7$. No hay relaciones multiplicativas anormalmente cortas entre 2 y 3 módulo 139; la relación más corta es $2^4 \cdot 3^{10} \equiv 1 \pmod{139}$.

No es la palabra extremal. Halbeisen y Hungerbühler [3] demostraron que, para parámetros (K, o) fijos, el máximo sobre los collares del menor numerador de sus rotaciones se alcanza en el collar de la palabra equilibrada (de Christoffel), dada por $\lceil jo/K \rceil - \lceil (j-1)o/K \rceil$. Para $(11, 7)$ esa palabra es 11011011010, y s_{-17} no es ninguna de sus rotaciones: tiene bloques de cuatro unos y tres ceros, lejos del equilibrio. La teoría de extremos no distingue el collar del ciclo de -17 .

Equidistribución módulo 139. La tabla de la sección anterior muestra que, en longitudes mayores, los numeradores se reparten módulo 139 tal como predice la uniformidad.

Observación 5.1 (Respuesta al Problema 6.3 del escrito V). No hemos encontrado ninguna razón estructural para que 139 divida al numerador del ciclo de -17 : el primo no tiene relaciones multiplicativas cortas, la palabra es primitiva y no extremal, y el mismo primo se comporta de forma uniforme en longitudes mayores. Bajo el modelo uniforme, que el Teorema 4.1 y los recuentos exactos respaldan para primos fijos, el número esperado de collares con numerador divisible por 139 es $30/139 \approx 0,22$; se observa exactamente uno. En este sentido, el ciclo de -17 no se deduce de ninguna estructura identificable.

6. Consecuencias para la heurística de los ciclos

El escrito V formuló el número esperado de ciclos enteros bajo el supuesto de que los numeradores son aleatorios módulo D . Los resultados anteriores permiten matizar el estatus de ese supuesto.

1. *Primos fijos.* Para cada primo fijo $p \geq 5$ hay equidistribución demostrada sin fijar el número de unos (Teorema 4.1) y comprobada exactamente fijándolo (tabla). El supuesto es sólido en este régimen, salvo por las divisibilidades estructurales de la Sección 3, que se identifican y descartan.
2. *Primos que crecen con K .* Los ciclos largos, si existen, tendrían $|D|$ enorme, y la divisibilidad relevante sería por primos de tamaño comparable a $|D|$, que crecen

con K . En ese régimen la cadena de Markov del Teorema 4.1 no tiene tiempo de mezclarse: hay unas $2^{0,95K}$ palabras y $|D| \approx 2^K \varepsilon$ residuos. Nada de lo demostrado aquí cubre este caso, que es precisamente el que decide si hay ciclos enteros de longitud grande.

7. Preguntas abiertas

Problema 7.1. *Demostrar la Conjetura 4.3, con una tasa de convergencia explícita en función de p .*

Problema 7.2. *¿Existe una versión cuantitativa del Teorema 4.1 válida para primos p que crecen con K , por ejemplo $p \leq 2^{cK}$ para algún $c > 0$? Una tal versión, con c suficientemente grande, daría fundamento parcial a la heurística de los ciclos.*

Problema 7.3. *¿Hay primos p para los que la equidistribución módulo p falle de forma persistente al fijar $(K, o) \in \Lambda_p$, por razones distintas de las potencias de palabras?*

8. Resumen

Resultado	Estatus	Papel
Invariancia por rotación (Proposición 2.2)	Demostrado	La divisibilidad es de collares
Potencias y factor $2^{K'} + 3^{o'}$ (Proposición 3.2)	Demostrado	Divisibilidades estructurales
Equidistribución módulo p fijo (Teorema 4.1)	Demostrado	Respalda el modelo aleatorio
Equidistribución con (K, o) fijado	Recuento exacto y Conjetura 4.3	Respalda el modelo aleatorio
El caso de 139	Análisis completo	Responde al Problema 6.3 del escrito V: sin estructura visible
Primos que crecen con K	Abierto	Régimen decisivo para los ciclos largos

Verificación. Los recuentos de la tabla se han obtenido por programación dinámica exacta sobre los estados $(o, \varphi \bmod p)$. La palabra del ciclo de -17 , la base de Λ_{139} y el ejemplo del factor 1033 se han comprobado por cálculo directo.

Referencias

- [1] M. Cerdá Bennassar, *Collatz e indecidibilidad. IV. Catalan, los dos orígenes y la contracción en la iteración de Collatz*, septiembre de 2026.
- [2] M. Cerdá Bennassar, *Collatz e indecidibilidad. V. Memoria en valuaciones: la cota de borrado, los límites de la simulación de contadores y el ciclo de -17* , septiembre de 2026.
- [3] L. Halbeisen y N. Hungerbühler, Optimal bounds for the length of rational Collatz cycles, *Acta Arithmetica* 78 (1997), 227–239.

- [4] J. C. Lagarias, The set of rational cycles for the $3x + 1$ problem, *Acta Arithmetica* 56 (1990), 33–53.