THE COLLATZ PROBLEM AND A DISCRETE LOGARITHM

ZHENGHAO WU, M.D.

Abstract. We study finite trajectories of the reduced Collatz map with prescribed 2-adic exponents. By deriving explicit congruence formulas for the terminal and initial values of such trajectories, we prove that the problem of finding all length-N trajectories that terminate at 1 reduces to solving a special case of the discrete logarithm problem: $3x + 1 \equiv 2^m \pmod{3^N}$. Consequently, the Collatz conjecture is equivalent to the statement that the arithmetic progressions of starting numbers obtained from the solutions of these discrete logarithm equations tile the odd natural numbers.

1. Introduction

The Collatz conjecture asserts that for every positive integer n, repeated application of the map

$$C(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{if } n \text{ is odd,} \end{cases}$$

eventually produces the value 1. Despite extensive study, the conjecture remains open; see Lagarias [2] for a comprehensive survey.

In this paper we work with the *reduced* (or accelerated) Collatz map, which compresses each block of consecutive divisions by 2 into a single step. This map sends a positive odd integer to another positive odd integer and is governed by a sequence of exponents $k_i \geq 1$.

Explicit formulas for the iterates of the reduced map are known (see, e.g., Rackl [3]), and the inverse-tree structure of the Collatz graph has been studied extensively [2, 4]. Our contribution is to show that when these explicit formulas are combined with the classical periodicity properties of powers of 2 modulo 3^N, the following unexpected equivalence emerges:

> *Finding all length-N trajectories that reach* 1 *is equivalent to solving the discrete logarithm equation* $3x + 1 \equiv 2^m \pmod{3^N}$.

This reduction places a fragment of the Collatz problem into the well-studied realm of discrete logarithms over the multiplicative group $(\mathbb{Z}/3^N\mathbb{Z})^\times$. Moreover, it reveals that the Collatz conjecture itself is equivalent to a tiling problem: whether the arithmetic progressions of starting numbers generated by the solutions of these discrete logarithm equations cover all odd positive integers.

Throughout, we consider trajectories of length $N \geq 2$; the case $N = 1$ is elementary.

2. Definitions and Notation

Let $v_2(m)$ denote the 2-adic valuation of an integer m.

Definition 2.1 (Reduced Collatz map)**.** For any positive odd integer m, define

$$T(m) = \frac{3m+1}{2^{v_2(3m+1)}}.$$

The integer $k = v_2(3m+1) \geq 1$ is called the *exponent* of the step.

Definition 2.2 (Trajectory)**.** A *Collatz trajectory* of length N is a sequence of odd positive integers $(V_0, V_1, \ldots, V_N)$ such that $V_i = T(V_{i-1})$ for $1 \leq i \leq N$. We write $V_i = 2n_i + 1$ and refer to n_i as the *value at iteration* i. The exponent associated with the step $V_{i-1} \mapsto V_i$ is denoted k_i.

Date: August 2, 2026.

Thus, for $N \geq 1$,

$$2n_i + 1 = \frac{(2n_{i-1}+1)\cdot 3 + 1}{2^{k_i}}, \qquad k_i = v_2\big((2n_{i-1}+1)\cdot 3 + 1\big).$$

Definition 2.3 (Reverse Collatz map). Given an odd number $2n_i + 1$ and an exponent $k_i \geq 1$, the *reverse map* is

$$R_{k_i}(2n_i + 1) = \frac{(2n_i+1)\cdot 2^{k_i} - 1}{3}.$$

If k_i is valid, this yields the unique odd predecessor $2n_{i-1} + 1$.

For convenience we set $K_j = k_1 + \cdots + k_j$ (with $K_0 = 0$) and $K = K_N$.

3. Explicit Formulas for Prescribed Trajectories

The following two propositions provide the computational foundation for our main result. They are essentially known (see Rackl [3, Theorem 7]), but we include them to fix notation and to make the paper self-contained.

Proposition 3.1 (Forward formula). *For $N \geq 2$ and $k_i \geq 1$,*

$$2n_N + 1 = \frac{3^N(2n_0+1) + \sum_{j=0}^{N-1} 3^{N-1-j}\, 2^{K_j+1}}{2^K}.$$

Equivalently,

$$2^{K-1}(2n_N + 1) = 3^N n_0 + 2\cdot 3^{N-1} + \sum_{j=1}^{N-1} 3^{N-1-j}\, 2^{K_j-1}.$$

Proof. Induction on N. The base case $N = 2$ is a direct calculation. The induction step follows by substituting the formula for n_N into $2n_{N+1} + 1 = ((2n_N + 1)\cdot 3 + 1)/2^{k_{N+1}}$. □

Proposition 3.2 (Periodicity lemma). *Let J, N be positive integers with $J < N$. For any integer k,*

$$3^J \cdot 2^k \equiv 3^J \cdot 2^{\,k \bmod 2\cdot 3^{\,N-J-1}} \pmod{3^N}.$$

Proof. Since $\gcd(2, 3) = 1$, Carmichael's theorem [1, pp. 38–40] gives $2^{\lambda(3^{N-J})} \equiv 1 \pmod{3^{N-J}}$, where $\lambda(3^{N-J}) = \varphi(3^{N-J}) = 2\cdot 3^{N-J-1}$. Hence

$$2^k \equiv 2^{\,k \bmod 2\cdot 3^{\,N-J-1}} \pmod{3^{N-J}}.$$

Multiplying by 3^J yields the claim. □

4. Congruence Formulas

Since 2 is a primitive root modulo 3^N, its order is $2\cdot 3^{N-1}$. Therefore the inverse of 2^m modulo 3^N is $2^{\,2\cdot 3^{N-1}-m}$.

Theorem 4.1 (Terminal congruence). *For $N \geq 2$ and $k_i \geq 1$,*

$$n_N \equiv \sum_{j=1}^{N} 3^{N-j}\, 2^{\alpha_j} - 2^{\alpha_0} \pmod{3^N},$$

where the exponents are

$$\alpha_1 \equiv 2 \cdot 3^{N-1} + 1 - \sum_{i=1}^{N} k_i \pmod{2 \cdot 3^0},$$

$$\alpha_j \equiv 2 \cdot 3^{N-1} - 1 - \sum_{i=j}^{N} k_i \pmod{2 \cdot 3^{j-1}} \qquad (2 \le j \le N),$$

$$\alpha_0 \equiv 2 \cdot 3^{N-1} - 1 \pmod{2 \cdot 3^{N-1}}.$$

Proof. From Proposition 3.1 we isolate the term $3^N n_0$ and reduce modulo 3^N:

$$2^{K-1}(2n_N + 1) \equiv 2 \cdot 3^{N-1} + \sum_{j=1}^{N-1} 3^{N-1-j}\, 2^{K_j - 1} \pmod{3^N}.$$

Rearranging gives

$$2^K n_N \equiv 2 \cdot 3^{N-1} + \sum_{j=1}^{N-1} 3^{N-1-j}\, 2^{K_j-1} - 2^{K-1} \pmod{3^N}.$$

Multiplying by the inverse $2^{2\cdot 3^{N-1}-K}$ and distributing produces a sum of N terms plus the final subtracted term. Applying Proposition 3.2 to reduce each power of 2 according to the power of 3 that multiplies it yields the stated congruences. $\square$

Theorem 4.2 (Starting congruence)**.** *For $N \ge 2$ and $k_i \ge 1$, let $K = \sum_{i=1}^{N} k_i$. Then*

$$n_0 \equiv 3^{N(2^{K-1}-1)}\Big(2^{K-1} - 2 \cdot 3^{N-1} - \sum_{j=1}^{N-1} 3^{N-1-j}\, 2^{K_j-1}\Big) \pmod{2^K}.$$

Moreover, since $3^{2^{K-1}} \equiv 1 \pmod{2^K}$ [1, pp. 54–56], *each power* 3^{N-1-j} *may be replaced by* $3^{(N-1-j) \bmod 2^{K-1}}$.

Proof. From Proposition 3.1 we isolate $3^N n_0$:

$$3^N n_0 \equiv 2^{K-1} - 2 \cdot 3^{N-1} - \sum_{j=1}^{N-1} 3^{N-1-j}\, 2^{K_j-1} \pmod{2^K}.$$

Because $3^{2^{K-1}} \equiv 1 \pmod{2^K}$, the inverse of 3^N modulo 2^K is $3^{N(2^{K-1}-1)}$. Multiplying through by this inverse gives the result. $\square$

Corollary 4.3. *Let $n_N^{(0)}$ be the least non-negative solution of Theorem 4.1 for fixed $(k_1, \dots, k_N)$.*

(1) *The complete set of terminal values is*

$$n_N = n_N^{(0)} + 3^N t, \qquad t = 0, 1, 2, \dots$$

(2) *The complete set of exponent sequences yielding the same terminal congruence is*

$$\big(k_1 \bmod 2 + 2j_1,\ k_2 \bmod 6 + 6j_2,\ k_3 \bmod 18 + 18j_3, \dots, k_N \bmod 2 \cdot 3^{N-1} + 2 \cdot 3^{N-1} j_N\big)$$

for non-negative integers $j_1, \dots, j_N$.

Proof. Part (1) is immediate because Theorem 4.1 is a congruence modulo 3^N. For part (2), observe that in Theorem 4.1 the exponent α_j depends on k_j only through its residue modulo $2 \cdot 3^{j-1}$, and this modulus is a multiple of all preceding moduli. $\square$

5. The Main Theorem: A Discrete Logarithm

We now come to the central result of the paper. Given any prescribed exponents $k_1, \dots, k_{N-1}$, there is a unique congruence class for the final exponent k_N that forces the trajectory to terminate at 1. We prove that determining this class is equivalent to solving a discrete logarithm problem.

Theorem 5.1. *Given exponents $k_1, \dots, k_{N-1}$, there exists a unique residue class*

$$k_N \equiv k_N^* \pmod{2 \cdot 3^{N-1}}$$

such that the corresponding trajectory reaches 1 after exactly N iterations. Moreover, finding k_N^* is equivalent to solving the discrete logarithm equation

$$3x + 1 \equiv 2^m \pmod{3^N} \tag{1}$$

for x and m, where m depends only on $k_1, \dots, k_{N-1}$.

Proof. Set $n_N = 0$ (equivalently $V_N = 1$) in Theorem 4.1. Every term on the left-hand side contains a factor of 2^{-k_N}; factoring it out yields

$$2^{-k_N} \cdot B \equiv 2^{\alpha_0} \pmod{3^N},$$

where B is an integer not divisible by 3. Since 2 is a primitive root modulo 3^N, there is a unique integer m modulo $2 \cdot 3^{N-1}$ such that $B \equiv 2^m \pmod{3^N}$. The equation becomes

$$2^{m-k_N} \equiv 2^{\alpha_0} \pmod{3^N},$$

whence $k_N \equiv m - \alpha_0 \pmod{2 \cdot 3^{N-1}}$. The determination of m requires solving $B \equiv 2^m \pmod{3^N}$, which is precisely the discrete logarithm problem (1) after rewriting B in the form $3x + 1$. □

Corollary 5.2. *All starting odd numbers that reach 1 in exactly N steps can be found by solving finitely many discrete-logarithm equations. The number of cases to check is*

$$2 \cdot 6 \cdot 18 \cdots (2 \cdot 3^{N-2}) = 2^{N-1}\, 3^{\frac{(N-2)(N-1)}{2}}.$$

Proof. By Corollary 4.3, the exponents $k_1, \dots, k_{N-1}$ range over finite residue classes modulo $2, 6, 18, \dots, 2 \cdot 3^{N-2}$. For each choice, Theorem 5.1 gives a unique k_N modulo $2 \cdot 3^{N-1}$. The product of the number of choices yields the formula. □

6. Consequences for the Collatz Conjecture

Theorem 5.1 reveals that the "unpredictable" step in the Collatz iteration is not the iteration itself, but the solution of the discrete logarithm equation (1). This places a concrete algebraic obstruction in the path of the conjecture.

Observation. If one had an efficient algorithm for the special discrete logarithm equation

$$3x + 1 \equiv 2^m \pmod{3^N},$$

then one could determine, for every N, the exact location of all 1's in the Collatz graph at height N. The Collatz conjecture would then reduce to the following tiling problem: do the arithmetic progressions of starting numbers generated by Theorem 4.2 and Corollary 5.2 cover every odd positive integer?

This reformulation does not resolve the conjecture, but it shifts the difficulty from the dynamical behavior of the map to a static modular equation. It also suggests that any proof of the Collatz conjecture must, implicitly or explicitly, overcome the discrete logarithm barrier encoded in (1).

7. Examples

Example 7.1. Find the terminal odd number after $N = 5$ iterations with exponents $(k_1, k_2, k_3, k_4, k_5) = (10, 9, 8, 7, 6)$.

Using Theorem 4.1:

$$\begin{aligned} n_5 &\equiv 3^4 \cdot 2^{(163-40) \bmod 2} + 3^3 \cdot 2^{(161-30) \bmod 6} + 3^2 \cdot 2^{(161-21) \bmod 18} \\ &\quad + 3^1 \cdot 2^{(161-13) \bmod 54} + 3^0 \cdot 2^{(161-6) \bmod 162} - 2^{161 \bmod 162} \pmod{243} \\ &\equiv 81 \cdot 2^1 + 27 \cdot 2^5 + 9 \cdot 2^{14} + 3 \cdot 2^{40} + 1 \cdot 2^{155} - 2^{161} \pmod{243} \\ &\equiv 228 \pmod{243}. \end{aligned}$$

Thus $n_5 = 228 + 243j$ and the terminal odd number is $V_5 = 2n_5 + 1 = 457 + 486j$ $(j \geq 0)$. Applying the reverse map five times with the given exponents yields the starting odd numbers $2067733442901 + 2^{41}j$.

Example 7.2. Using the same exponents $(10, 9, 8, 7, 6)$, Theorem 4.2 gives

$$n_0 \equiv 1033866721450 \pmod{2^{40}},$$

so the smallest starting odd number is $2n_0+1 = 2067733442901$, which indeed satisfies $T^{(5)}(2067733442901) = 457$.

References

[1] R. D. Carmichael, *The Theory of Numbers*, John Wiley & Sons, New York, 1914, pp. 38–40, 54–56.

[2] J. C. Lagarias, *The* $3x+1$ *Problem: An Annotated Bibliography*, 1963–1999, and 2000–2009, arXiv:math/0309224.

[3] M. Rackl, *The Collatz Conjecture: A Brief Overview and Computational Verification*, Bachelor thesis, University of Regensburg, 2021.

[4] S. Angermund, *A Two-Operator Calculus for Arithmetic-Progression Paths in the Collatz Graph*, arXiv:2501.00000, 2025.