THE CONGRUENCE STRUCTURE OF THE $3x+1$ MAP

ROGER E. ZARNOWSKI

Abstract. Let $T : \mathbb{Z} \to \mathbb{Z}$ be defined by $T(x) = \frac{1}{2}x$ if x is even, and $T(x) = \frac{1}{2}(3x+1)$ if x is odd. The $3x+1$ Conjecture asserts that every positive x has an iterate $T^n(x) = 1$. It is known that T^n maps congruence classes with modulus 2^n to those with modulus equal to a power of 3. We describe properties of the image class residues and use those properties to show that, under iteration by T, any congruence class with modulus of the form $2^a 3^b$ generates all integers not divisible by 3. This has negative implications for the study of sufficient sets for the $3x+1$ Conjecture. The analysis also provides insight into a particular permutation function associated with T.

1. Introduction

The $3x+1$ Problem concerns iteration of the following function defined on the set $\mathbb{Z}$ of integers

$$T(x) = \begin{cases} \frac{x}{2}, & \text{if } x \text{ is even,} \\ \frac{3x+1}{2}, & \text{if } x \text{ is odd.} \end{cases}$$

A well-known conjecture, widely attributed to Lothar Collatz, states that for every $x \geq 1$ the sequence of iterates $\{T^k(x)\}_{k=0}^{\infty}$ eventually reaches the cycle $(2, 1)$. The $3x+1$ Problem, to either prove or disprove this conjecture, remains unsolved after decades of attention and appears to be intractable. Yet the problem continues to attract interest, and much has been learned about some aspects of its perplexing nature. The works of Lagarias [7] and Wirsching [11] contain significant foundational results on this problem. Chamberland [3] provides an overview of different approaches to the problem and a survey of results from many authors. Numerous additional references are available in the extensive bibliography compiled by Lagarias [8].

We adopt the following notation throughout: The group $\mathbb{Z}/n\mathbb{Z}$ is denoted by $\mathbb{Z}_n$ and, for $0 \leq r < n$, $[r]_n$ denotes the congruence class of r modulo n.

In describing the T-iterates of a number x, it is often useful to introduce the *parity vector* $\vec{v}(x) = (v_0(x), v_1(x), \ldots)$, where $v_i(x)$ is the $\{0,1\}$-valued function defined by

$$v_i(x) \equiv T^i(x) \pmod 2.$$

We also define

$$s_0(x) = 0, \text{ and } s_n(x) = v_0(x) + \cdots + v_{n-1}(x), \quad n = 1, 2, \ldots.$$

For $n \geq 1$, $s_n(x)$ is then the number of odd numbers in $\{x, T(x), \ldots, T^{n-1}(x)\}$.

The relationship between an integer x and its parity vector $\vec{v}(x)$ seems central to an understanding of the $3x+1$ Problem. Some aspects of this relationship were described by Terras [10], and in more detail by Lagarias [7]; a fundamental result is that for $n \geq 1$ the function

$$\overline{Q}_n(x) = \sum_{i=0}^{n-1} v_i(x) 2^i \tag{1}$$

is a permutation on $\mathbb{Z}_{2^n}$. The cycle structure of this function was investigated by Bernstein and Lagarias [2].

It is also well-known (see Terras [10, proof of Theorem 1.2]) that

$$T^n(x + m2^n) = T^n(x) + m3^{s_n(x)}. \tag{2}$$

If $0 \leq x \leq 2^n - 1$, it follows from the definition of T that $0 \leq T^n(x) \leq 3^{s_n(x)} - 1$, so that $T^n(x)$ is the least nonnegative residue of a congruence class modulo $3^{s_n(x)}$. To set the stage for subsequent analysis, we therefore adopt the notation $r_n(x) := T^n(x)$, and rewrite (2) as

$$T^n(x + m2^n) = r_n(x) + m3^{s_n(x)}, \quad \text{for } 0 \leq x < 2^n. \tag{3}$$

Equation (3) expresses the fact that T^n maps the 2^n distinct congruence classes of $\mathbb{Z}_{2^n}$ to congruence classes with modulus $3^{s_n(x)}$. Some properties of T-iterates of the classes of $\mathbb{Z}_{2^n}$ were described by Terras [10] and Everett [4], and used by them to establish density estimates on the proportion of numbers less than a given number for which the $3x+1$ Conjecture holds. Lagarias [7] extended those results to obtain lower bounds on the growth rate of this density.

Our purpose is to describe properties of the residues $r_n(x)$, including some special periodicity relationships that are expressed in Theorem 2. We then explore specific consequences of those properties, one of which is the fact that any congruence class with modulus of the form $2^a 3^b$ generates, under iteration by T, all numbers $x \not\equiv 0 \pmod 3$ infinitely many times. This is our main result and is presented in Theorem 3. We also show in Theorem 4 that the structure of the permutation function $\overline{Q}_n(x)$ is determined by the parities of the residues $r_0(x), \ldots, r_{n-1}(x)$.

2. The $3x+1$ Congruence Class Triangle

The following useful lemma follows immediately from the definition of T, and may also be viewed as a special case of (2).

Lemma 1. *If x_e is even, then $T(x + x_e) = T(x) + 3^{v_0(x)} \frac{x_e}{2}$.*

We are interested in describing the iteration under T of congruence classes with modulus equal to a power of 3. A key to doing this is to replace ordinary divisions by 2 with divisions modulo powers of 3, motivated by the fact that the multiplicative inverse of $2 \pmod{3^k}$ is

$$2^{-1}_{3^k} := \frac{1}{2}(3^k + 1).$$

Definition 1. *For $k \geq 0$ we define $H_k : \mathbb{Z} \to \mathbb{Z}$ by $H_0(x) = 0$ and, for $k \geq 1$,*

$$H_k(x) = \left(\frac{1}{2}(3^k + 1) \cdot x \right) \bmod 3^k.$$

$H_k(x)$ therefore denotes the least nonnegative residue of a congruence class $\bmod 3^k$. The relationship of H_k to T is as follows.

Theorem 1. *Let r and k be nonnegative integers. Then:*

(a) *If* $r < 2 \cdot 3^k - (r \bmod 2)3^k$, *then for every integer* n,

$$T\left(r + 2n3^k + (r \bmod 2)3^k\right) = H_k(r) + n3^k, \tag{4}$$

(b) *If* $r < 3^k + (r \bmod 2)3^k$, *then for every integer* n,

$$T\left(r + (2n+1)3^k - (r \bmod 2)3^k\right) = H_{k+1}(3r+1) + n3^{k+1}. \tag{5}$$

Proof. If $r = 2m < 2 \cdot 3^k$, then

$$\begin{aligned} H_k(r) &= \left(\frac{1}{2}(3^k+1)(2m)\right) \bmod 3^k \\ &= m \\ &= \frac{1}{2}\left(r + (r \bmod 2)3^k\right). \end{aligned}$$

On the other hand, if $r = 2m + 1 < 3^k$, then

$$\begin{aligned} H_k(r) &= \left(\frac{1}{2}(3^k+1)(2m+1)\right) \bmod 3^k \\ &= \left(m3^k + \frac{1}{2}(3^k + 2m + 1)\right) \bmod 3^k \\ &= \frac{1}{2}(3^k + r) \quad (\text{since } r < 3^k) \\ &= \frac{1}{2}\left(r + (r \bmod 2)3^k\right). \end{aligned}$$

In either case, $r + (r \bmod 2)3^k$ is even, and so

$$H_k(r) = T\left(r + (r \bmod 2)3^k\right).$$

Then, by Lemma 1,

$$\begin{aligned} T\left(r + (r \bmod 2)3^k + 2n3^k\right) &= T\left(r + (r \bmod 2)3^k\right) + 3^0 \cdot n3^k \\ &= H_k(r) + n3^k, \end{aligned}$$

which establishes (4). Next, if $r = 2m \le 3^k - 1$, then

$$\begin{aligned} H_{k+1}(3r+1) &= \left(\frac{1}{2}(3^{k+1}+1)(6m+1)\right) \bmod 3^{k+1} \\ &= \left(3^{k+1}3m + \frac{1}{2}(6m + 1 + 3^{k+1})\right) \bmod 3^{k+1} \\ &= \frac{1}{2}(6m + 1 + 3^{k+1}) \quad (\text{since } 6m + 1 \le 3(3^k - 1) + 1 < 3^{k+1}) \\ &= \frac{1}{2}\left(3(2m + 3^k) + 1\right) \\ &= T(2m + 3^k) \\ &= T\left(r + 3^k - (r \bmod 2)3^k\right). \end{aligned}$$

Similarly, if $r = 2m + 1 \leq 2 \cdot 3^k - 1$, then $T(r) = 3m + 2 < 3^{k+1}$, and

$$\begin{aligned} H_{k+1}(3r+1) &= \left(\frac{1}{2}(3^{k+1}+1)(6m+4)\right) \bmod 3^{k+1} \\ &= \left((3m+2)3^{k+1} + (3m+2)\right) \bmod 3^{k+1} \\ &= 3m+2 \\ &= T(2m+1) \\ &= T\left(r + 3^k - (r \bmod 2)3^k\right). \end{aligned}$$

In either case,

$$H_{k+1}(3r+1) = T\left(r + 3^k - (r \bmod 2)3^k\right).$$

Again by Lemma 1, since $\left(r + 3^k - (r \bmod 2)3^k\right)$ is odd, we have

$$\begin{aligned} T\left(r + 3^k - (r \bmod 2)3^k + 2n3^k\right) &= T\left(r + 3^k - (r \bmod 2)3^k\right) + 3^1 \cdot n3^k \\ &= H_{k+1}(3r+1) + n3^{k+1}. \end{aligned}$$

This establishes (5), which completes the proof. □

The following corollary provides a preliminary description of the T-images of congruence classes mod 3^k.

Corollary 1. *Let r and k be nonnegative integers, with $r < 3^k$. Then*

$$T\left([r]_{3^k}\right) = [H_k(r)]_{3^k} \cup [H_{k+1}(3r+1)]_{3^{k+1}}, \tag{6}$$

with the even numbers in $[r]_{3^k}$ being mapped onto $[H_k(r)]_{3^k}$ and the odd numbers onto $[H_{k+1}(3r+1)]_{3^{k+1}}$.

Proof. The statement follows immediately from (4) and (5) by considering separately the cases of even and odd values of r. □

From (6), a straightforward counting argument yields the following.

Corollary 2. *$T^n([r]_{3^k})$ consists of the union of 2^n congruence classes, of which $\binom{n}{i}$ have modulus 3^{k+i}, for each $i = 0, \ldots, n$.*

Corollary 2 with $r = k = 0$ shows that $T^n(\mathbb{Z})$ consists of 2^n congruence classes, of which $\binom{n}{i}$ are of modulus 3^i. When tracing the trajectory $\{T^n(x)\}$ of a particular x, Corollary 1 also shows that the modulus 3^i of the class containing $T^n(x)$ increases only with iterates of odd numbers, so that

$$i = s_n(x),$$

in accordance with (2). We now index the least nonnegative residues of the congruence classes of $T^n(\mathbb{Z})$ by $r_{n,i,j}$ where $i = 0, \ldots, n$ and $j = 1, \ldots, \binom{n}{i}$. (Note that $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.) By using (6), the residues may be described recursively as follows where, for notational convenience, we define $\binom{n}{n+1} = 0$. We set

$$r_{0,0,1} = 0,$$

and, for $n \geq 0$,

$$\begin{cases} r_{n+1,i,j} = H_i(r_{n,i,j}), \ i = 0, \ldots, n, \ j = 1, \ldots, \binom{n}{i}, \\ r_{n+1,i,\binom{n}{i}+j} = H_i(3r_{n,i-1,j} + 1), \ i = 1, \ldots, n+1, \ j = 1, \ldots, \binom{n}{i-1}. \end{cases} \tag{7}$$

As special cases, we have $r_{n,0,1} = 0$ and $r_{n,n,1} = 3^n - 1$, for all n. With this method of indexing, (6) now becomes

$$T([r_{n,i,j}]_{3^i}) = [r_{n+1,i,j}]_{3^i} \cup [r_{n+1,i+1,\binom{n}{i+1}+j}]_{3^{i+1}}. \tag{8}$$

Equations (7) and (8) provide a complete description of the T-iterates of congruence classes mod 3^i. These congruence classes can be diagrammed in a triangular array as shown in Figure 1, with even numbers iterating to the left and odd numbers to the right. We call this array the $3x + 1$ *Congruence Class Triangle* (CCT).

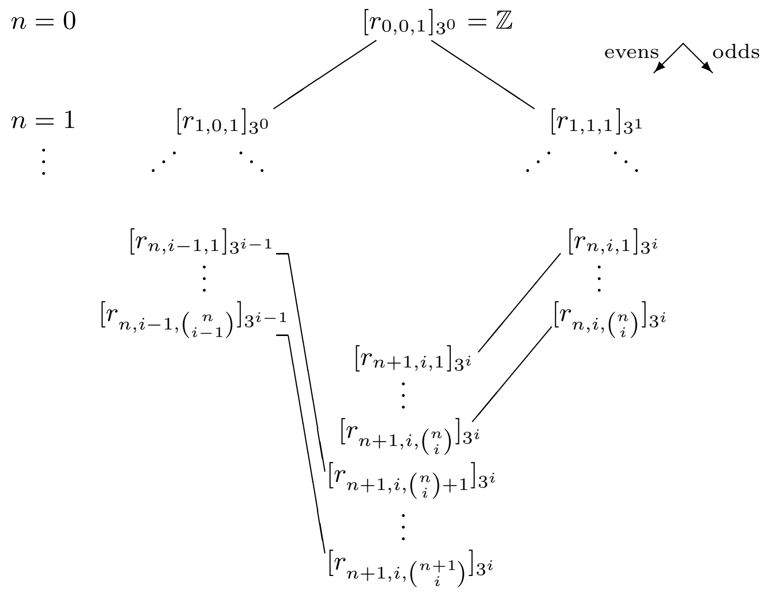

Figure 1. Schematic of the $3x + 1$ Congruence Class Triangle (CCT).

With the notation described above, (3) may be rewritten as

$$\begin{aligned} T^n(x_{n,i,j} + m2^n) &= T^n(x_{n,i,j}) + m3^i \\ &= r_{n,i,j} + m3^i, \end{aligned} \tag{9}$$

where $x_{n,i,j} \in \{0, 1, \ldots, 2^n - 1\}$ and $T^n(x_{n,i,j}) = r_{n,i,j} < 3^i$. Figure 2 shows the CCT through level $n = 4$ with the actual values of the residues. Also indicated parenthetically in Figure 2 are the "seed" values $x_{n,i,j}$ from (9); the relationships expressed by (9) are therefore represented in the diagram by entries of the form $[r_{n,i,j}]_{3^i}(x_{n,i,j})$.

The CCT as shown in Figure 2 reveals apparent periodicities of the residues along diagonals $i =$ constant. By computing residues for larger values of n, we may observe that the first few cycles are

$$\begin{aligned} &i = 1 : (2, 1) \\ &i = 2 : (8, 4, 2, 1, 5, 7) \\ &i = 3 : (26, 13, 20, 10, 5, 16, 8, 4, 2, 1, 14, 7, 17, 22, 11, 19, 23, 25). \end{aligned}$$

This is explained by the following theorem, which is central to our subsequent analysis.

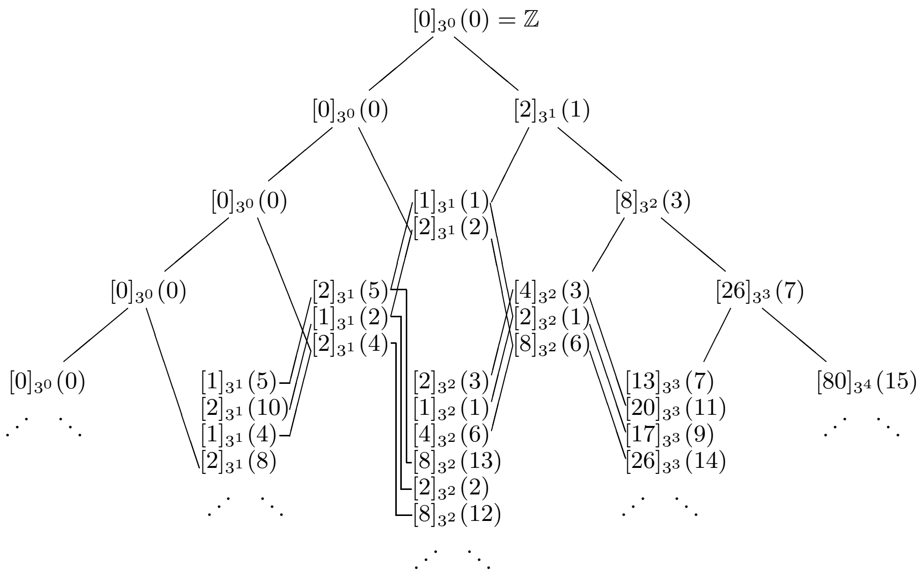

FIGURE 2. The CCT with residue values and corresponding initial "seeds".

Theorem 2. *For $i \geq 1$, each residue $r_{n,i,j}$ is a unit modulo 3^i and, if $P_i = 2 \cdot 3^{i-1}$, any set of the form*

$$\{r_{n,i,j}, r_{n+1,i,j}, \ldots, r_{n+(P_i-1),i,j}\}$$

is the set of all units modulo 3^i, which is a cyclic group under division by 2 $\pmod{3^i}$.

Proof. We use (7) and the following two facts: (a) the units modulo 3^i are the $2 \cdot 3^{i-1}$ positive integers less than 3^i that are not divisible by 3, and (b) 2 is a primitive root modulo 3^i, so that successive multiplication or division of any unit modulo 3^i by either 2 or $2_{3^i}^{-1}$ generates the group of units modulo 3^i, which is cyclic. (See, for example, Jones and Jones [5].)

As a special initial case we have $T([0]_{3^0}) = [0]_{3^0} \cup [2]_{3^1}$, and so $r_{1,1,1} = 2$, which is a unit modulo 3^1. For even $r > 0$, if $r < 3^i$ is a unit modulo 3^i then so is $H_i(r) = \left(2_{3^i}^{-1} r\right) \bmod 3^i$. For odd $r > 0$, if $r < 3^i - 1$ then $3r + 1 < 3^{i+1}$. Also, 3 does not divide $3r + 1$. So $3r + 1$ is a unit modulo 3^{i+1}, and then $\left(2_{3^{i+1}}^{-1}(3r + 1)\right) \bmod 3^{i+1}$ is also; i.e., $H_{i+1}(3r + 1)$ is a unit modulo 3^{i+1}. We then have, from (7), that if $r_{n,i,j}$ is a unit modulo 3^i, then $r_{n+1,i,j}$ is a unit modulo 3^i and $r_{n+1,i+1,\binom{n}{i+1}+j}$ is a unit modulo 3^{i+1}. Since these are the only two residues arising from one iteration of $[r_{n,i,j}]_{3^i}$, it follows inductively that every residue $r_{n,i,j}$ is a unit modulo 3^i. Then also, since $r_{n+1,i,j} = (2_{3^i}^{-1} r_{n,i,j}) \bmod 3^i$ and $2_{3^i}^{-1}$ is a primitive root of 3^i, the set $\{r_{n,i,j}, r_{n+1,i,j}, \ldots, r_{n+(P_i-1),i,j}\}$ is the cyclic group of units modulo 3^i. □

3. CONSEQUENCES OF THE CCT STRUCTURE

The structure of the CCT provides insight into a variety of properties of the $3x+1$ iteration. We examine two of these in detail.

3.1. Sufficient Sets of Vanishing Density.

A natural area of inquiry involves the identification of *sufficient sets* for the $3x + 1$ Problem, i.e., sets S with the property that if the $3x+1$ Conjecture holds on S, then it holds for all positive integers. Korec and Znam [6] gave a very concise proof that arithmetic progressions of the form $\{a + mp^n\}_{m=0}^{\infty}$ are sufficient when n is a positive integer, p is an odd prime, 2 is a primitive root modulo p^2, and $p \nmid a$. This is significant in that the choice of m allows such sets to be chosen with arbitrarily small density in $\mathbb{Z}^+$. Subsequently, Andaloro [1] showed that $\{1+16m\}_{m=0}^{\infty}$ is sufficient, a case not covered by Korec and Znam. All of these results have more recently been subsumed by the remarkable result of Monks [9] that any nonconstant nonnegative arithmetic progression is a sufficient set.

The typical approach to showing a set S is sufficient is to show that for any $x \in \mathbb{Z}^+$, there is an integer $y \in S$ that "merges" with x, in the sense that

$$T^k(x) = T^l(y) \tag{10}$$

for some integers k and l. The properties of the CCT, however, provide a relatively simple means to establish a more significant property for some arithmetic progressions.

We require the following well-known result, which is a direct consequence of the definition of T.

Lemma 2. *For every nonzero integer x, there exists a constant K such that $T^k(x) \not\equiv 0 \pmod 3$ for all $k \geq K$.*

The set

$$I = \{x \in \mathbb{Z} : x \not\equiv 0 \pmod 3\}$$

is therefore an attracting invariant set for T on $\mathbb{Z} - \{0\}$. Although the next results are established for congruence classes, by restricting to positive integers these results imply that arithmetic progressions with modulus of the form $2^a 3^b$ are sufficient for the $3x+1$ Conjecture. However, we show that these sets have a much stronger property than the merging property (10); under iteration by T any one of these sets generates every number in I infinitely many times.

Lemma 3. *Let $1 \leq i_1 \leq i_2$ and let u_1 and u_2 be units modulo 3^{i_1} and 3^{i_2}, respectively. Then there exists a subset A of $[u_1]_{3^{i_1}}$ and an integer $k > 0$ such that $T^k(A) = [u_2]_{3^{i_2}}$.*

Proof. First, note that by iterating (8),

$$\begin{aligned} T^m\left([r_{n,i,j}]_{3^i}\right) &= T^{m-1}\left([r_{n+1,i,j}]_{3^i} \cup [r_{n+1,i+1,\binom{n}{i+1}+j}]_{3^{i+1}}\right) \\ &\ \vdots \\ &= [r_{n+m,i,j}]_{3^i} \cup \cdots \cup [r_{n+m,i+m,\binom{n}{i+1}+\binom{n+1}{i+2}+\cdots+\binom{n+m-1}{i+m}+j}]_{3^{i+m}}. \end{aligned} \tag{11}$$

Next, by Theorem 2, we may choose m_0 so that $r_{m_0,i_1,1} = u_1$. Set $m_1 = i_2 - i_1$. Then, applying (11),

$$\begin{aligned} T^{m_1}([u_1]_{3^{i_1}}) &= T^{m_1}([r_{m_0,i_1,1}]_{3^{i_1}}) \\ &= [r_{m_0+m_1,i_1,1}]_{3^{i_1}} \cup \cdots \cup [r_{m_0+m_1,i_1+m_1,J_1}]_{3^{i_1+m_1}}, \end{aligned}$$

where J_1 is some integer. So there is a subset A_1 of $[u_1]_{3^{i_1}}$ such that

$$\begin{aligned} T^{m_1}(A_1) &= [r_{m_0+m_1,i_1+m_1,J_1}]_{3^{i_1+m_1}} \\ &= [r_{m_0+m_1,i_2,J_1}]_{3^{i_2}}. \end{aligned}$$

Again using (11), we have that for any integer m_2,

$$\begin{aligned} T^{m_1+m_2}(A_1) &= T^{m_2}([r_{m_0+m_1,i_2,J_1}]_{3^{i_2}}) \\ &= [r_{m_0+m_1+m_2,i_2,J_1}]_{3^{i_2}} \cup \cdots \cup [r_{m_0+m_1+m_2,i_2+m_2,J_2}]_{3^{i_2+m_2}}, \end{aligned}$$

where J_2 is some integer. By Theorem 2, we may choose $m_2 > 0$ so that $r_{m_0+m_1+m_2,i_2,J_1} = u_2$. So there is a subset A of A_1 for which $T^{m_1+m_2}(A) = [u_2]_{3^{i_2}}$. Setting $k = m_1 + m_2$ yields the desired result. □

Theorem 3. *Let a and b be nonnegative integers, not both 0, and let c be a positive integer such that $c < 2^a 3^b$. Let K be an integer such that $T^K(c) \not\equiv 0 \pmod 3$, and set $M = \max\{a, K\}$. Then:*

(a) *For every integer $i \geq b + s_M(c)$ and every integer u that is a unit modulo 3^i there exists a sequence of positive integers $k_1 < k_2 < \cdots$ and a collection of sets $A_1, A_2, \ldots$ with $[c]_{2^a 3^b} \supseteq A_1 \supseteq A_2 \supseteq \cdots$ such that $T^{k_m}(A_m) = [u]_{3^i}$ for $m = 1, 2, \ldots$.*

(b) *For every $x \in I$, there exists a sequence $k_1 < k_2 < \ldots$ of positive integers and a sequence $\{z_m\} \subseteq [c]_{2^a 3^b}$ such that $T^{k_m}(z_m) = x$ for $m = 1, 2, \ldots$.*

Proof. We have

$$\begin{aligned} T^M([c]_{2^a 3^b}) &\supseteq T^M([c]_{2^M 3^b}) \\ &= T^M\left(\{c + n2^M 3^b : n \in \mathbb{Z}\}\right) \\ &= \{T^M(c) + n3^{b+s_M(c)} : n \in \mathbb{Z}\} \quad \text{by (2)}, \\ &= [T^M(c)]_{3^{b+s_M(c)}}. \end{aligned}$$

So there exists a set $A_0 \subseteq [c]_{2^a 3^b}$ such that

$$T^M(A_0) = [T^M(c)]_{3^{b+s_M(c)}}.$$

Since $M \geq K$, $T^M(c) \not\equiv 0 \pmod 3$, by Lemma 2. Also, since $c < 2^a 3^b$ and $M \geq a$, $T^M(c) < 3^{b+s_M(c)}$. Thus, $T^M(c)$ is a unit modulo $3^{b+s_M(c)}$. By Lemma 3, there exists $B_0 \subseteq [T^M(c)]_{3^{b+s_M(c)}}$ and an integer $m_0 > 0$ such that $T^{m_0}(B_0) = [u]_{3^i}$. Then

$$\begin{aligned} T^{M+m_0}(A_0) &= T^{m_0}\left([T^M(c)]_{3^{b+s_M(c)}}\right) \\ &\supseteq T^{m_0}(B_0) \\ &= [u]_{3^i}. \end{aligned}$$

So there exists $A_1 \subseteq A_0$ such that $T^{k_1}(A_1) = [u]_{3^i}$, where $k_1 = M + m_0 > 0$.

Proceeding inductively, if $T^{k_n}(A_n) = [u]_{3^i}$ for some n, we may reapply Lemma 3 with $i_1 = i_2 = i$ to find that there exists $B_n \subseteq T^{k_n}(A_n)$ and an integer $m_n > 0$ such that $T^{m_n}(B_n) = [u]_{3^i}$. We then have

$$\begin{aligned} T^{k_n+m_n}(A_n) &= T^{m_n}\left(T^{k_n}(A_n)\right) \\ &\supseteq T^{m_n}(B_n) \\ &= [u]_{3^i}. \end{aligned}$$

So there is a subset A_{n+1} of A_n for which $T^{k_n+m_n}(A_{n+1}) = [u]_{3^i}$. Thus, $T^{k_{n+1}}(A_{n+1}) = [u]_{3^i}$, where $k_{n+1} = k_n + m_n > k_n$. Part (a) follows by induction.

For (b), we note that any positive $x \in I$ is a unit modulo 3^i for sufficiently large i. For negative $x \in I$, we may choose i large enough so that $w = x + 3^i$ is positive. Then w is a unit modulo 3^i and $x \in [w]_{3^i}$. So in either case, we may choose integers i and u such that u is a unit modulo 3^i and $x \in [u]_{3^i}$. The sets A_m and integers k_m from part (1) then have the property that $T^{k_m}(A_m)$ contains x. Thus, there exists $z_m \in A_m$ such that $T^{k_m}(z_m) = x$. □

Remark 1. The statement of Theorem 3(a) encompasses many well-known congruence identities for the $3x + 1$ Problem. For example, the familiar fact that $T^3(4m + 1) = T(m)$ when m is odd is expressible as $T(2n+1) = T^3(8n+5) = T^5(32n+21) = \cdots = 3n+2$, from which $T([1]_{2^1}) = T^3([5]_{2^3}) = T^5([21]_{2^5}) = \cdots = [2]_{3^1}$. This relationship can be identified in Figure 2 from the entries $[2]_{3^1}(1)$ at level $n = 1$, $[2]_{3^1}(5)$ at level $n = 3$, etc. Similar identities can be obtained from further inspection of the CCT periodicities as expressed in Theorem 2. Theorem 3(a), which relies upon these periodicities, shows that such relationships are ubiquitous.

Remark 2. The identification of sufficient sets with the merging property (10) has offered the appealing prospect of being able to address the $3x+1$ Problem by restricting attention to an arbitrarily small subset of the integers. Theorem 3(b), however, diminishes this hope by showing that many sufficient sets of small density are "sufficient" only in a most undesirable way – they simply regenerate the entire invariant set I. It remains an interesting open question as to whether arithmetic progressions with modulus other than 2^a3^b also have this property.

3.2. **Terras' Permutation Function.** We now refer back to the permutation function $\overline{Q}_n(x)$ from (1), which relates a number x to its parity vector $\vec{v}(x)$:

$$\overline{Q}_n(x) = \sum_{i=0}^{n-1} v_i(x)2^i.$$

For $x < 2^n$, the binary bits $b_i(x) \in \{0, 1\}$ are defined by

$$x = \sum_{i=0}^{n-1} b_i(x)2^i,$$

with $b_i(x) = 0$ for $i \geq n$. We also define the k-bit predecessor of x by

$$p_k(x) := x - 2^k \left\lfloor \frac{x}{2^k} \right\rfloor,$$

where $\lfloor x \rfloor$ denotes the floor (or greatest integer) function. So $p_0(x) = 0$ and for $k \geq 1$,

$$p_k(x) = \sum_{i=0}^{k-1} b_i(x)2^i.$$

As described by Lagarias [7], for $n = 1$ and $n = 2$, $\overline{Q}_n(x)$ is the identity map on $\mathbb{Z}_{2^n}$, since in these cases $v_i(x) = b_i(x)$ for $i = 0, \ldots, n - 1$. The first nontrivial permutation occurs for $n = 3$, where $\overline{Q}_3(1) = 5$ and $\overline{Q}_3(5) = 1$. Examination of the CCT in Figure 2 shows that this permutation is due to the odd parity of the residue $r_{2,1,1} = 1$. The next theorem confirms that the permutation function $\overline{Q}_n$ is determined by the parities of the residues at levels $0, 1, \ldots, n - 1$ in the CCT.

Theorem 4. *Let $n \geq 0$ be given. For $1 \leq x < 2^n$, define the $\{0, 1\}$-valued functions $\rho_k(x), b_k(x)$, and $v_k(x)$ for $k = 0, \ldots, n$ by*

$$x = \sum_{k=0}^{n} b_k(x)2^k,$$

$$v_k(x) \equiv T^k(x) \pmod 2, \tag{12}$$

$$\rho_k(x) \equiv T^k(p_k(x)) \pmod 2, \tag{13}$$

where $p_k(x) = x - 2^k \left\lfloor \frac{x}{2^k} \right\rfloor$. *Then*

$$v_k(x) \equiv b_k(x) + \rho_k(x) \pmod 2.$$

Proof. Since $b_0(x) = v_0(x)$ and $\rho_0(x) = 0$, the statement is true for $k = 0$. For $k \geq 1$ we use the fact from Terras [10] that $v_i(y + m2^k) = v_i(y)$ for $i = 0, \ldots, k-1$, from which it follows that $s_k(y + m2^k) = s_k(y)$. In particular,

$$s_k(x) = s_k\left(p_k(x) + \left\lfloor \frac{x}{2^k} \right\rfloor 2^k\right) = s_k(p_k(x)).$$

We then have

$$\begin{aligned} T^k(x) &= T^k\left(p_k(x) + 2^k \left\lfloor \frac{x}{2^k} \right\rfloor\right) \\ &= T^k\left(p_k(x)\right) + 3^{s_k(p_k(x))} \left\lfloor \frac{x}{2^k} \right\rfloor \quad \text{by} \quad (2), \end{aligned}$$

so that

$$T^k(x) = T^k\left(p_k(x)\right) + 3^{s_k(x)} \left\lfloor \frac{x}{2^k} \right\rfloor. \tag{14}$$

Since $p_k(x) < 2^k$, $T^k(p_k(x)) < 3^{s_k(x)}$ (as in (2)), so $T^k(p_k(x))$ is the residue of the congruence class mod $3^{s_k(x)}$ that contains $T^k(x)$. We now compare parities of the terms in (14), using (12), (13), and the fact that

$$\left(3^{s_k(x)} \left\lfloor \frac{x}{2^k} \right\rfloor\right) \equiv \left\lfloor \frac{x}{2^k} \right\rfloor \equiv b_k \pmod 2.$$

We then obtain $v_k(x) \equiv \rho_k(x) + b_k(x) \pmod 2$. □

By considering the vectors $\vec{v}(x) = \{v_0(x), v_1(x), \ldots\}$, $\vec{b}(x) = \{b_0(x), b_1(x), \ldots\}$ and $\vec{\rho}(x) = \{\rho_0(x), \rho_1(x), \ldots\}$, the conclusion of Theorem 4 may be written as $\vec{v} = \vec{b} \oplus \vec{\rho}$, where $\oplus$ denotes the bitwise-XOR operator. Note that the $\oplus$ operator has the property that this equation remains true if the vectors $\vec{v}, \vec{b}$, and $\vec{\rho}$ are permuted. This equation gives a concise description of some important features of the $3x+1$ iteration. First, since ρ_i is nonzero precisely when $b_i \neq v_i$, the permutation function $\overline{Q}_n$ is determined by $\vec{\rho}$. Also, if $x < 2^n$, then $b_i = 0$ for $i \geq n$, so that $v_i = \rho_i$ for $i \geq n$, which reflects the known fact that the residues eventually become equal to the iterates themselves, as described by (14) when $2^k > x$. Theorem 4 suggests that greater insight into the nature of $\overline{Q}_n$ may be possible from further investigation of patterns in the parities of the CCT residues.

References

[1] P. Andaloro, *On Total Stopping Times Under* $3x+1$ *Iteration*, The Fibonacci Quarterly, **38.1** (2000), 73–78.

[2] D. J. Bernstein and J. C. Lagarias, *The* $3x+1$ *Conjugacy Map*, Canad. J. Math., **48.6** (1996), 1154–1169.

[3] M. Chamberland, *An Update on the* $3x+1$ *Problem*, Bull. Soc. Catalana Mat., **18.1** (2003), 19–45.

[4] C. J. Everett, *Iteration of the Number-Theoretic Function* $f(2n) = n, f(2n+1) = 3n+2$, Adv. Math., **25.1** (1977), 42–45.

[5] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer-Verlag, London, 1998.

[6] I. Korec and S. Znam, *A Note on the* $3x+1$ *Problem*, Amer. Math. Monthly, **94.8** (1987), 771–772.

[7] J. C. Lagarias, *The* $3x+1$ *Problem and Its Generalizations*, Amer. Math. Monthly, **92.1** (1985), 3–23.

[8] J. C. Lagarias, *The* $3x+1$ *Problem: An Annotated Bibliography (1963-2000)*, `http://www.arxiv.org/abs/math/0309224`.

[9] K. M. Monks, *The Sufficiency of Arithmetic Progressions for the* $3x+1$ *Conjecture*, Proc. Amer. Math. Soc., **134.10** (2006), 2861–2872.

[10] R. Terras, *A Stopping Time Problem on the Positive Integers*, Acta Arith., **30.3** (1976), 241–252.
[11] G. J. Wirsching, *The Dynamical System Generated by the* $3n + 1$ *Function*, Springer-Verlag, Berlin, 1998.

MSC2000: 11B37, 11B83

Department of Mathematics, Angelo State University, San Angelo, TX 76909
E-mail address: roger.zarnowski@angelo.edu