Dynamical System Proof of Infinitude of Primes

Harikrishnan NB

March 11, 2021

1 Introduction

This is a replication of the dynamical system proof of infinitude of primes by Dr. Kishor G Bhat, Post Doctoral Fellow, St. John's Research Institute (Alumnus of NIAS). I thank Dr. Nithin Nagaraj (Associate professor, NIAS) and Harikumar K for helping me understand the proof.

2 Definitions

Definition 1: A **map** is a function whose domain and range are the same. Let $T(\cdot)$ be a map, the orbit (trajectory) of x under the map $T(\cdot)$ is denoted as $x \to T(x) \to T^2(x) \to \ldots T^k(x)$, where x is the initial value of the map $T(\cdot)$ [1].

Example of a Map: We consider a map $T_k(x_{n-1}) = kx_{n-1} \mod (1) = kx_{n-1} - [kx_{n-1}]$, $[0, 1) \to [0, 1)$, k is a positive integer greater than 1 ($[kx_{n-1}]$ represents the integer part of kx_{n-1}).

For $k = 2$, we get the following map: $T_2(x_{n-1}) = 2x_{n-1} - [2x_{n-1}]$. The pictorial representation of the map is provided in Figure 1. This is a piece wise

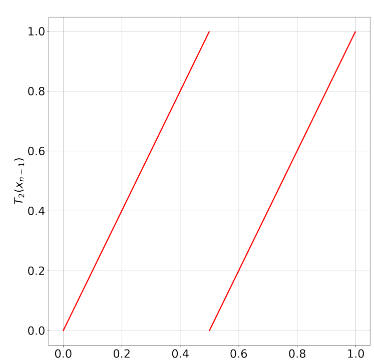

Figure 1: $T_2(x_{n-1}) = 2x_{n-1} - [2x_{n-1}]$.

linear map where $0 \leq x_{n-1} < 1$ and $0 \leq T_2(x_{n-1}) < 1$. The trajectory starting from x_0 is provided as follows:

$$x_0 \rightarrow x_1 \rightarrow \ldots \rightarrow x_n \rightarrow \ldots \tag{1}$$

An example of the trajectory starting from $x_0 = 0.01$ for the $T_2(x_{n-1}) = 2x_{n-1} - [2x_{n-1}]$ map is provided in Figure 2.

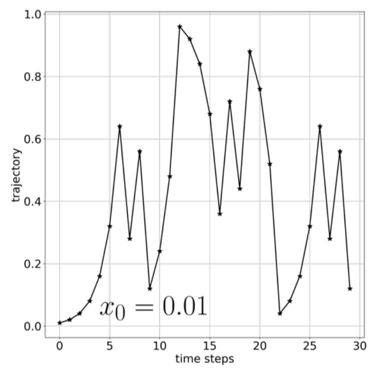

Figure 2: Trajectory starting from $x_0 = 0.01$ for the $T_2(x_{n-1}) = 2x_{n-1} - [2x_{n-1}]$ map.

What are the possible patterns in the trajectory of $T_2(x_{n-1})$ map ?

- Periodic with period-1 ($x_0 = 0$).
- Periodic with period-k ($x_0 = 0.8$, k = 3).
- Eventually periodic ($x_0 = 0.05$).
- Eventually terminating to zero ($x_0 = 0.125$).
- Non-periodic ($x_0 = \frac{\sqrt{2}}{10}$).

We will formally define the definition of period-1/fixed points and eventually periodic points of a map.

Definition-2: **Fixed Point or Period-1 point of a map**: A point p is a fixed point or period 1 point of a map ($T(\cdot)$) if $T(p) = p$.

Definition-3: **Eventually Periodic Point**: A point x is an eventually periodic point with period $l > 0$ of a map $T(\cdot)$, if $T^{n+l}(x) = T^n(x), \forall n \geq N$ and $N \in Z^+$, and l is the smallest such positive number.

Definition-4: **Fundamental Theorem of Arithmetic**: The fundamental theorem of arithmetic states that every positive integer (except the number 1) can be represented in exactly one way apart from rearrangements as a product of one or more primes [2].

3 Lemma

Lemma 1: Given that the map $T_n(x) = nx \mod (1) = nx - [nx]$, $x \in [0, 1)$, $n > 1$ and $n \in \mathbf{Z}^+$, where $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$, then $T_n(x) \in [0, 1)$.

Proof: By definition of a number (nx), we have

$$nx = [nx] + d, 0 \leq d < 1, \tag{2}$$

$$\begin{aligned} nx - [nx] &= d, 0 \leq d < 1, && (3)\\ 0 \leq nx - [nx] &< 1, && (4)\\ 0 \leq T_n(x) &< 1. && (5)\\ & && (6) \end{aligned}$$

Hence proved.

Lemma 2: If $x = \frac{p}{q}$, where $p \in \mathbf{Z}^+ \cup \{0\}$, $q \in \mathbf{Z}^+$, $gcd(p, q) = 1$ and $p < q$, then $T_n^k(x) : [0, 1) \to [0, 1)$ is eventually periodic.

Proof:

$$T_n\left(\frac{p}{q}\right) = \frac{np}{q} - \left[\frac{np}{q}\right]. \tag{7}$$

From Lemma 1, we have $0 \leq T_n(x) < 1$. This implies $0 \leq T_n\left(\frac{p}{q}\right) < 1$.

$$T_n\left(\frac{p}{q}\right) = \frac{np}{q} - \left[\frac{np}{q}\right]. \tag{8}$$

Let $\left[\frac{np}{q}\right] = t_1$, where $t_1 \in \mathbf{Z}^+ \cup \{0\}$. Now the above equation is of the form :

$$T_n\left(\frac{p}{q}\right) = \frac{np}{q} - t_1 = \frac{np - t_1 q}{q}. \tag{9}$$

From Lemma 1, we have $0 \leq T_n\left(\frac{p}{q}\right) < 1$, this implies $0 \leq \frac{np - t_1 q}{q} < 1$. Therefore, $np - t_1 q < q$. Let us denote $np - t_1 q$ as z_1. Therefore, $T_n\left(\frac{p}{q}\right) = \frac{z_1}{q}$, where $z_1 \in \mathbf{Z}^+ \cup \{0\}$ and $z_1 < q$ (From Lemma 1).

Now,

$$T_n\left(\frac{z_1}{q}\right) = \frac{nz_1}{q} - \left[\frac{nz_1}{q}\right]. \tag{10}$$

Let us denote $\left[\frac{nz_1}{q}\right] = t_2$, this when substituted in the above equation gives the following:

$$T_n\left(\frac{z_1}{q}\right) = \frac{nz_1 - t_2 q}{q}. \tag{11}$$

If we substitute, $nz_1 - tq = z_2$, we have $T_n\Big(\frac{z_1}{q}\Big) = \frac{z_2}{q}$, where $z_2 \in \mathbf{Z}^+ \cup \{0\}$ and $z_2 < q$ (From Lemma 1).

From the above we can conclude that if we iterate the map $T_n(x) = nx - [nx]$ from $x = \frac{p}{q}$, we have the following:

$$\frac{p}{q} \to \frac{z_1}{q} \to \frac{z_2}{q} \to \ldots \to \frac{z_i}{q}. \tag{12}$$

where $\forall i, z_i < q$, which implies $0 \leq z_i < q$ (From Lemma 1). $\forall i, z_i < q$ where $z_i \in \mathbf{Z}^+ \cup \{0\}$ and $q \in \mathbf{Z}^+$ implies that after finite number iterations z_i has to repeat because z_i can take only finite set of values $(0 \leq z_i \leq q-1)$. This repetition of z_i proves that after finite number of iterations $T_n^k\Big(\frac{p}{q}\Big)$ becomes periodic. Hence, the Lemma 2 is proved.

Lemma 3: If $n = p_1 p_2 \ldots p_k$, where $p_i \in \mathbf{P}$ (set of all primes) and $q = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ where $b_i \in \mathbf{Z}^+ \cup \{0\}$ then $T_n\Big(\frac{t}{q}\Big) : [0,1) \to [0,1)$ is eventually terminating to zero where $0 \leq t < q$.

Proof:

$$T_n\Big(\frac{t}{q}\Big) = \frac{nt}{q} - \Big[\frac{nt}{q}\Big], \tag{13}$$

$$T_n\Big(\frac{t}{q}\Big) = \frac{p_1 p_2 \ldots p_k t}{p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}} - \Big[\frac{p_1 p_2 \ldots p_k t}{p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}}\Big], \tag{14}$$

$$\tag{15}$$

We denote $\Big[\frac{p_1 p_2 \ldots p_k t}{p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}}\Big]$ as c_1.

$$T_n\Big(\frac{t}{q}\Big) = \frac{t}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}} - c_1, \tag{16}$$

$$T_n\Big(\frac{t}{q}\Big) = \frac{t - c_1(p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1})}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}}, \tag{17}$$

$$\tag{18}$$

We denote $t - c_1(p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1})$ as z_1.

$$T_n\Big(\frac{t}{q}\Big) = \frac{z_1}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}}, \tag{19}$$

On further iteration, we get the following:

$$T\Big(\frac{z_1}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}}\Big) = \frac{p_1 p_2 \ldots p_k z_1}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}} - \Big[\frac{p_1 p_2 \ldots p_k z_1}{p_1^{b_1-1} p_2^{b_2-1} \ldots p_k^{b_k-1}}\Big], \tag{20}$$

Let $\left[\frac{p_1p_2\ldots p_k z_1}{p_1^{b_1-1}p_2^{b_2-1}\ldots p_k^{b_k-1}}\right]$ be denoted as c_2.

$$T\Big(\frac{z_1}{p_1^{b_1-1}p_2^{b_2-1}\ldots p_k^{b_k-1}}\Big) = \frac{z_1}{p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2}} - c_2, \tag{21}$$

$$T\Big(\frac{z_1}{p_1^{b_1-1}p_2^{b_2-1}\ldots p_k^{b_k-1}}\Big) = \frac{z_1 - c_2(p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2})}{p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2}}, \tag{22}$$

$$\tag{23}$$

We denote $z_1 - c_2(p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2})$ as z_2.

$$T\Big(\frac{z_1}{p_1^{b_1-1}p_2^{b_2-1}\ldots p_k^{b_k-1}}\Big) = \frac{z_2}{p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2}}, \tag{24}$$

The iterates are of the following form:

$$\frac{t}{p_1^{b_1}p_2^{b_2}\ldots p_k^{b_k}} \to \frac{z_1}{p_1^{b_1-1}p_2^{b_2-1}\ldots p_k^{b_k-1}} \to \frac{z_2}{p_1^{b_1-2}p_2^{b_2-2}\ldots p_k^{b_k-2}} \to \ldots \tag{25}$$

Let $b_i = \max(b_1, b_2, \ldots b_k)$. Therefore after $b_i - 1$, we have the following:

$$T_n^{b_i-1}\Big(\frac{t}{p_1^{b_1}p_2^{b_2}\ldots p_k^{b_k}}\Big) = \frac{z_{b_i-1}}{p_i}, \tag{26}$$

On one more iteration, we get the following:

$$T\Big(\frac{z_{b_i-1}}{p_i}\Big) = \frac{nz_{b_i-1}}{p_i} - \Big[\frac{nz_{b_i-1}}{p_i}\Big], \tag{27}$$

$$= \frac{p_1p_2\ldots p_{i-1}p_ip_{i+1}\ldots p_k z_{b_i-1}}{p_i} - \Big[\frac{p_1p_2\ldots p_{i-1}p_ip_{i+1}\ldots p_k z_{b_i-1}}{p_i}\Big], \tag{28}$$

$$= (p_1p_2\ldots p_{i-1}p_{i+1}\ldots p_k z_{b_i-1}) - (p_1p_2\ldots p_{i-1}p_{i+1}\ldots p_k z_{b_i-1}) = 0. \tag{29}$$

We show that after b_i iterations, $T_n(\frac{t}{q})$ is eventually terminating to zero. Hence proved.

Lemma 4: If there is a period - 1 orbit for the map $T(\cdot) : [0, 1) \to [0, 1)$ then the initial value is of the form $\frac{p}{q}$.

Proof: By definition of fixed point or period - 1 point we have the following:

$$T_n(x) = x, \tag{30}$$

$$nx - [nx] = x, \tag{31}$$

$$nx - x = [nx], \tag{32}$$

$$x(n-1) = [nx], \tag{33}$$

$$x = \frac{[nx]}{n-1}. \tag{34}$$

From lemma-2, if $x = \frac{p}{q}$ then $T_n^k(x)$ is eventually periodic. But for the following values of x, iterates of $T_n(x)$ gives period-1 orbit.

$$x = \Big\{0, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, \frac{n-2}{n-1}\Big\}. \tag{35}$$

There are in total '$n-1$' fixed points and all of them are of the form $\frac{p}{q}$. Out of '$n-1$' fixed points, there are '$n-2$' fixed points of the form $\frac{p}{q}$ and which does not terminate to zero.

4 Main Proof

4.1 Proof by Contradiction of Infinitude of Primes

Assumption: Let us assume there are only finite number of primes and the set of finite number of primes be denoted as $P = \{p_1, p_2, \ldots, p_k\}$.

Now consider n as the product of all primes in the set P and q as follows:

$$n = p_1 p_2 p_3 \ldots p_k, \tag{36}$$
$$q = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}. \tag{37}$$

From Lemma 3, $T_n(\frac{t}{q})$ is eventually terminating to zero, $0 \leq t < q$. From Lemma 4, the fixed points of $T_n(x)$ are the form $\frac{k}{n-1}, 0 \leq k \leq n-2$.

Using Fundamental theorem of arithmetic, $n-1$ can be written as follows:

$$n - 1 = p_1^{r_1} p_2^{r_2} .. p_k^{r_k}. \tag{38}$$

From Lemma 3, $T_n\left(\frac{k}{n-1}\right) = T_n\left(\frac{k}{p_1^{r_1} p_2^{r_2} .. p_k^{r_k}}\right)$ should actually terminate to zero. But from Lemma 4, there are '$n-2$' fixed points of the form $\frac{p}{q}$ and not terminating to zero. Therefore the following relation is not true:

$$n - 1 = p_1^{r_1} p_2^{r_2} .. p_k^{r_k}. \tag{39}$$

Hence the assumption that the number of prime numbers are finite is false.

References

[1] Kathleen T Alligood, Tim D Sauer, and James A Yorke. *Chaos*. Springer, 1996.

[2] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.