MJFAS MALAYSIAN JOURNAL OF FUNDAMENTAL AND APPLIED SCIENCES
PRINT ISSN: 2289-5981 | ONLINE ISSN: 2289-599X

RESEARCH ARTICLE

# Dynamical system proof of Fermat's little theorem: An alternative approach

Olamide Funmilayo Florence [a], Tahir Bin Ahmad [b], Adaraniwon Amos Olalekan [c,*]

[a] Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia
[b] Centre for Sustainable Nanomaterials, Ibnu Sina Institute for Scientific and Industrial Research, Universiti Teknologi Malaysia, Skudai 81310, Johor, Malaysia
[c] Institute of Mathematical Sciences, Faculty of Science, University of Malaya, 50603 Kuala Lumpur, Malaysia

* Corresponding author: tahir@ibnusina.utm.my

**Article history**
Received 7 February 2018
Revised 20 May 2018
Accepted 11 June 2018
Published Online 3 September 2018

**Abstract**

Fermat's little theorem has been proved using different mathematical approaches, which majority of them are based on number theory. These approaches have only exposed the usability of Fermat's little theorem for logical, linear and structural predictions. Only small numbers of attempts had only been made to proof Fermat's little theorem from other perspectives. This paper exhibits an alternative approach to proof the Fermat's little theorem via dynamical system. Two lemmas are proven with respect to a redefined function, T$_n$ ($x$) in order to achieve the task**.**

***Keywords*****:** Fermat's little theorem, dynamical system approach

© 2018 Penerbit UTM Press. All rights reserved

## INTRODUCTION

Fermat's little theorem is a well-known result in number theory such that when $p$ is prime, then $a^p \equiv a$ (mod $p$) for any natural number $a$. Fermat's little theorem is a theorem regarding prime number in relation to modulo. It is quite a famous theorem by Fermat. It has broadly been proved in so many ways using number theory. However, Iga published a paper titled 'A Dynamical System Proof of Fermat's Little Theorem' in 2003 (Iga, 2003). The proof is totally different than any other researchers have offered before. This paper furnishes in details the proof of Fermat's little theorem offered by Iga (2003). However, two important lemmas are proven with respect to a redefined function, T$_n$ ($x$) in order to achieve the task**.**

## METHODOLOGY

A fixed point of a function is an element of the function's domain that is mapped to its self by the function. A fixed point is a point $a$ such that $f$ ($a$) = $a$ (Holmgren, 2012).

Consider a function T$_n$: [0, 1] → [0, 1] for any $n$, where $n \geq 2$ as

$$\mathrm{T}_n(x) = \begin{cases} (nx), 0 \leq \; x < 1 \\ \quad 1, x \;=\; 1 \end{cases} \qquad (1)$$

Hence, T$_n$ is an example of such a function.

Iga (2003) started with the following lemma to introduce his novel proof of Fermat's little theorem.

**Lemma 1** (Iga, 2003)
Let $n$ be a positive integers greater than 1. Then, the function T$_n$ ($x$) has exactly $n$ fixed point in [0, 1].

**Proof**
Let $a \in \mathbb{Z}^+$ and $0 \leq a < n$-1 with respect to equation (1), $x$ must be in form of $x = \frac{a}{n-1}$ so that $0 \leq \frac{a}{n-1} < \frac{n-1}{n-1}$, i.e. $0 \leq x < 1$ in order to fulfil the first domain condition of equation (1).
Now to obtain the range,
T$_n$ ($x$) = ($n$ $x$) by definition of T$_n$ ($x$)

$$= \frac{na}{n-1} \text{ when } x = \frac{a}{n-1}$$

$$= \frac{na}{n-1}$$

In order to get T$_n$ $\left(\frac{na}{n-1}\right) = \frac{a}{n-1}$, we have to manipulate $\left(\frac{na}{n-1} - a\right) = \left(\frac{na-(n-1)a}{n-1}\right) = \frac{a}{n-1}$ as intended earlier.
In order words we need to redefine T$_n$ ($x$) = ($nx$ – $a$) when $x = \frac{a}{n-1}$.
The second condition of equation (1) is then guaranteed; i.e.
T$_n$ (1) = 1 when $x$ = 1 as $a$ = $n$-1 ■

The fixed points of the function of T$_3$($x$) is illustrated in Figure 1.

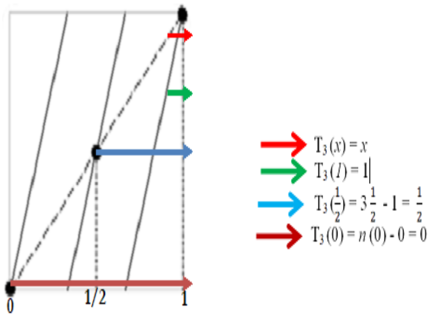

**Figure 1** The graph of T$_3$($x$).

For example, the fixed points of the function $T_3(x)$ are 0, 1/2, and 1. They are indicated by black circles in Figure 1. The function $T_n(x)$ for $n = 3$, $a = 0, 1, 2$ with $0 \leq a < n-1$ are as follow.

When $x = 0$, $T_3(x) = (nx - a)$, where $x = \frac{a}{n-1}$.

Then $x = \frac{a}{n-1} = 0$ which implies $a = 0$

$$\begin{aligned} T_3(0) &= n(0) - 0 \\ &= 0 \end{aligned}$$

Furthermore, when $x = \frac{1}{2}$

$$\begin{aligned} &= \frac{a}{n-1} = \frac{1}{2} \\ &= \frac{a}{3-1} = \frac{1}{2} \text{ when } n = 3 \\ &= \frac{a}{2} = \frac{1}{2} \text{ which implies } a = 1 \end{aligned}$$

Hence, $T_3(x) = (nx - a)$

$$\begin{aligned} &= n(x) - a \\ &= 3\left(\frac{1}{2}\right) - 1 \\ &= \frac{1}{2} \end{aligned}$$

$\therefore\ T_3\left(\frac{1}{2}\right) = \frac{1}{2}$

For the second condition of equation (1), when $x = 1$,

$T_3(x) = (nx - a)$, then $x = \frac{a}{n-1}$

$$\begin{aligned} &= \frac{a}{3-1} \\ &= \frac{a}{2} = 1 \text{ which implies } a = 2 \end{aligned}$$

Hence, $T_3(x) = (nx - a)$

$$\begin{aligned} &= 3(1) - 2 \\ &= 1 \end{aligned}$$

$\therefore\ T_3(1) = 1$

Therefore, the fixed point of $T_3(x) = 0, \frac{1}{2}, 1$ i.e. the number of element of $T_3(x) = 3$

The fixed point for $T_4(x)$ are as follow for $0 \leq a < n$-1 such that $a \in \mathbb{Z}^+$.

When $x = 0$, $T_4(x) = (nx - a)$, where $x = \frac{a}{n-1}$.

Then $x = \frac{a}{n-1} = 0$ which implies $a = 0$.

Therefore, $T_4(0) = n(0) - 0$

$$= 0$$

Furthermore, when $x = 1/3$, them

$$\begin{aligned} x &= \frac{a}{n-1} = \frac{1}{3} \\ &= \frac{a}{3} = \frac{1}{3} \text{ which implies } a = 1 \end{aligned}$$

Hence, $T_4(x) = (nx - a)$

$$\begin{aligned} &= 4\left(\frac{1}{3}\right) - 1 \\ &= \frac{1}{3} \end{aligned}$$

Therefore, $T_4\left(\frac{1}{3}\right) = \frac{1}{3}$.

When $x = \frac{2}{3}$, then $x = \frac{a}{n-1} = \frac{2}{3}$

$$= \frac{a}{3} = \frac{2}{3} \text{ which implies } a = 2.$$

Hence, $T_4(x) = (nx - a)$

$$\begin{aligned} &= 4\left(\frac{2}{3}\right) - 2 \\ &= \frac{2}{3} \end{aligned}$$

Therefore, $T_4\left(\frac{2}{3}\right) = \frac{2}{3}$

For the second condition of equation (1), when $x = 1$,

$$\begin{aligned} T_4(x) &= (nx - a) \\ &= \frac{a}{n-1} \\ &= \frac{a}{4-1} \\ &= \frac{a}{3} = 1 \text{ which implies } a = 3 \end{aligned}$$

$$\begin{aligned} T_4(x) &= (nx - a) \\ &= 4(1) - 3 \\ &= 1 \\ T_4(1) &= 1 \end{aligned}$$

Therefore, the fixed point of $T_4(x) = 0, \frac{1}{3}, \frac{2}{3}, 1$ i.e. the number of element of $T_4(x) = 4$; i.e. $T_4(x)$ has four fixed point as listed earlier.

Now, the question is whether $T_n(x)$ has exactly $n$ fixed points in [0, 1]? In order to answer this question, we introduce our own lemma, called lemma 2.

It was an ordinary statement by Iga (2003) in his paper. He did not supply the proof. However, we prove it as lemma 2 using mathematical induction on our own modified $T_n(x) = nx - a$ function.

**Lemma** 2

The function $T_n(x) = n, \forall n \in \mathbb{N}$

**Proof**: (by mathematical induction)

Let $P(n)$ be the statement

$P(n)$ : $T_n(x) = n, \forall n \in \mathbb{N}$ such that $x = \frac{a}{n-1}$ , $a \in [0, n-1)$

~~$P(1)$~~

$T_1(x) = 1$ since $x = \frac{a}{n-1}$ this implies that $a = 0$ for $0 \leq x < 1$

Hence,

$$\begin{aligned} T_1(x) &= 1x - a \\ &= x - 0 \\ &= x \end{aligned}$$

In order words, $T_1(x)$ has exactly 1 fixed point.

~~$P(n) \Rightarrow P(n+1)$~~

Assume $P(n)$ is true; i.e. $T_n(x) = n$.

Now,

$$\begin{aligned} T_{n+1}(x) &= (n+1)x - a \text{ by redefine of } T_n(x) \\ &= nx + x - a \\ &= nx - a + x \\ &= T_n(x) + x \\ &= n + x \quad \text{by assumption} \\ &= n + T_1(x) \quad \text{since } T_1(x) = x \\ &= n + 1 \end{aligned}$$

Therefore, $T_n(x) = n$ is true, $\forall n \in \mathbb{N}$ ■

In Iga (2003), he produced the following lemma.

**Lemma** 3 (Iga, 2003)

Let $r$ and $s$ be any positive integers for every $x \in [0, 1]$, then $T_r(T_s(x)) = T_{rs}(x)$.

However, in this paper, we will prove the equivalence of Iga's lemma in (2003) as stated in lemma 2 using our own modified $T_n(x)$ as follows.

**Lemma** 4

Let $r, s \in \mathbb{Z}^+$ such that $T_n(x) = (nx - a)$ for some $a \in \mathbb{Z}^+$ and $x \in [0, 1]$. Then $T_r(T_s(x)) = T_{rs}(x)$

### Proof

$$\begin{aligned}
T_r(T_s(x)) &= T_r(sx - a) && \text{by definition of } T_s(x)\\
&= r(sx - a) - a && \text{by definition of } T_r(x)\\
&= r\,sx - ra - a\\
&= r\,sx - a(r+1)\\
&= rsx - a^* && \text{by equating } a^* = a(r+1) \in \mathbb{Z}^+\\
&= T_{rs}(x) && \text{as required.} \qquad \blacksquare
\end{aligned}$$

We are ready to furnish in detail the proof offered by Iga (2003) for Fermat's little theorem using our own redefined $T_n(x)$ (i.e. $T_n(x) = (nx - a)$) and lemmas. We reinstate the theorem as follows.

### Theorem 5

If $p$ is a prime, then $a^p \equiv a \pmod p$, $\forall a \in \mathbb{N}$

### Proof

Consider $T_{a^p}(x)$ as in lemma 1 with $a \geq 2$ and $p$ be any prime.
By lemma 2, $T_a(x)$ has an exact $a$ fixed point. Similarly, $T_{a^p}(x)$ has $a^p$ fixed point. From lemma 4, $T_a(x) = T_a(T_a(\ldots T_a(x)\ldots))$ which means $T_a$ iterated $p$ times, which also implies composition of function with itself repeatedly. These are the $p$ – period point of $T_{a^p}(x)$ which is the fixed point of $T_{a^p}(x)$.
Therefore, any point of $T_a(x)$ is automatically a fixed point of $T_{a^p}(x)$, which means that there is exactly $a$ fixed point of $T_a(x)$ in $T_{a^p}(x)$ . Since $p$ is a prime, the rest of them has least period $p$ or minimal period $p$ under $T_a$ . This implies that there is $a^p - a$ points that have least period $p$.
Each point of least period $p$ lies in an orbit of size $p$. There is $ap - a$ point divisible by $p$ in the orbit of size $p$. Since this is an integer, therefore $a^p - a$ is divisible by $p$.
Hence,
$a^p \equiv a \pmod p$. $\blacksquare$

## CONCLUSION

This paper highlights some important elements of dynamical system approach to proof the Fermat's little theorem. Finally the paper presents an alternative proof of Fermat's little theorem by the method. Some lemmas and manipulation of $T_n(x)$ were provided in order to achieve the task.

## ACKNOWLEDGEMENT

The authors are thankful to Universiti Teknologi Malaysia for providing the necessary environment, technical support and funding (FRGS 4F756) for this research.

## REFERENCES

Iga, K. (2003). A dynamical systems proof of Fermat's's little theorem. Mathematics magazine, 76(1), 48-51.

Holmgren, R. (2012). A first course in discrete dynamical systems. Springer Science & Business Media.