# Dynamical Systems Techniques Applied to Number Theory

**Yunus Emre Kara**

Supervisor: Burak Gürel

**Abstract**

In this study, we are going to use various dynamical systems arguments for proving some number theoretical results. Fixed points, periodicity, number of points of a minimal period and other techniques from dynamical systems can be used for proving some facts about number theory, especially modular arithmetical results and a great theorem in contrast with its name: "Fermat's Little Theorem". Our main reference in relating dynamical systems to number theory is an article of Michael Frame, Brenda Johnson, and Jim Sauerberg, [**4**].

**Özet**

Bu çalışmada, bazı sayılar kuramı sonuçlarını ispatlamak için çeşitli dinamik sistemler argümanlarını kullanacağız. Sabit noktalar, periyodiklik, en küçük periyoda ait periyodik noktaların sayısı ve başka dinamik sistemler teknikleri, bazı sayılar kuramı sonuçlarını, özellikle modüler aritmetik sonuçlarını ve Fermat'nın Küçük Teoremi'ni, ispatlamak için kullanılabilir. Dinamik sistemlerle sayılar kuramı arasındaki ilişkiyi kurarken kullanacağımız ana referansımız Michael Frame, Brenda Johnson, ve Jim Sauerberg'in makalesidir, [**4**].

# Introduction

As its name says, number theory studies numbers, particularly integers. Dynamical systems study the time dependence of a point's position in space. Some number theoretical results are often used for showing dynamical systems facts about fixed and periodic points [**1**], and vice versa. In this study, we use dynamical systems facts for proving number theoretical statements. We begin with giving some definitions, and in the second section we mention about some tools that help us proving Fermat's Little Theorem. At the end, we show some other number theoretical results.
Now, let us give some elementary definitions of dynamical systems, which are needed in our study.

**Definition 1.** The *forward orbit* of $x$ is the set of points $x, f(x), f^2(x), ...$ and is denoted by $O^+(x)$, [**2**, p. 17].

In this text, we use the term *orbit* instead of forward orbit.

**Definition 2.** The point $x$ is a *fixed point for* $f$ if $f(x) = x$, [**2**, p. 18].

**Definition 3.** The point $x$ is a *periodic point of period* $n$ *for* $f$ if $f^n(x) = x$, [**2**, p. 18].

**Definition 4.** The least positive $n$ for which $f^n(x) = x$ is called *the prime(or minimal) period of* $x$, [**2**, p. 18].

We let $\mathscr{N}_n(f)$ denote the number of points of prime period $n$ for the function $f$.

**Definition 5.** The orbit of a periodic point of period $n$ is called an *$n$-cycle*, since it contains at most $n$ distinct elements. The orbit of a periodic point of prime period $n$ is called a *minimal $n$-cycle* or a *periodic orbit with least period $n$*.

*Remark.* It is clear from the definition that a minimal $n$-cycle containts $n$ distinct elements.

The next definition, [**3**], is not a dynamical systems definition, but we use it in relating some dynamical systems facts to each other.

**Definition 6.** Let $\psi(m)$ be an integer-valued function defined on the set of all positive integers. If $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where the $p_i$'s are distinct prime numbers, r and $k_i$'s are positive integers, we let $\Phi_1(1, \psi) = \psi(1)$ and let

$$\begin{aligned}\Phi_1(m, \psi) &= \psi(m) - \sum_{i=1}^{r} \psi(\frac{m}{p_i}) + \sum_{i_1<i_2} \psi(\frac{m}{p_{i_1}p_{i_2}}) - \sum_{i_1<i_2<i_3} \psi(\frac{m}{p_{i_1}p_{i_2}p_{i_3}}) \\ &\quad + \dots + (-1)^r \psi(\frac{m}{p_{i_1}p_{i_2}\dots p_{i_r}}),\end{aligned}$$

where the summation $\sum_{i_1<i_2<\dots<i_j}$ is taken over all integers $i_1, i_2, \dots, i_j$ with $1 \le i_1 < i_2 < \dots < i_j \le r$, [**3**].

# Dynamical Systems Tools

In this section, we are going to introduce some concepts in dynamical systems and prove a few results about these concepts which are needed for our later proofs. Also, we define a function that we use as the main tool in our proofs.

**Lemma 7.**

*(i) If $x_0$ is a point of period $n$ that has minimal period $m$, then $m|n$.*

*(ii) Two minimal $m$-cycles are either disjoint or identical.*

*(iii) For all $m \ge 1$, $m|\mathscr{N}_m$ whenever $\mathscr{N}_m$ is finite. Moreover, $\frac{\mathscr{N}_m}{m}$ is equal to the number of distinct minimal $m$-cycles.*

*Proof.*

(i) If $x_0$ is a point of minimal period $m$, then $f^m(x_0) = x_0$ and also its cycle contains $m$ distinct elements. Therefore only the $(mk)^{th}$ iterations can be equal to $x_0$ which implies period of $x_0$ can only be $mk$ where $k$ is an integer. Therefore $m$ divides any period of $x_0$.

(ii) Assume that we have two minimal $m$-cycles that are not disjoint. Let $x_0, \ldots, x_{m-1}$ be elements of first $m$-cycle and $y_0, \ldots, y_{m-1}$ be elements of second $m$-cycle. Then $x_i = y_j$ for some $i$ and $j$. But $f(x_i) = x_{i+1}$ and $f(y_j) = y_{j+1}$ implies $x_{i+1} = y_{j+1}$. By iterating this we can easily see that the second $m$-cycle is just a reordering of the first. Then two non-disjoint minimal $m$-cycles are identical. Therefore, two minimal $m$-cycles can be either disjoint or identical.

(iii) The points of minimal period $m$ are partitioned into disjoint minimal $m$-cycles(by (ii)). Each minimal $m$-cycle contains $m$ distinct points, so $m|\mathscr{N}_m$ and $\dfrac{\mathscr{N}_m}{m}$ gives the number of distinct minimal $m$-cycles.

■

**Theorem 8.** (Theorem 1 of [**3**]) *Let $S$ be a nonempty set and let $f$ be a map from $S$ into itself such that, for every positive integer $m$, the equation $f^m(x) = x$ has only finitely many distinct solutions. Let $\psi(m)$ denote the number of these solutions. Then, for every positive integer $m$ the number of periodic points of $f$ with least period $m$ is $\Phi_1(m, \psi)$ (i.e. $\mathscr{N}_m(f) = \Phi_1(m, \psi)$). Consequently, $\Phi_1(m, \psi) \equiv 0 \pmod{m}$.*

*Proof.* By inclusion-exclusion principle[**6**, p. 209], we can easily see that if $\psi(m)$ denotes the number of periodic points of period $m$, then $\Phi_1(m, \psi)$ denotes the number of periodic points of minimal period $m$. Then by Lemma

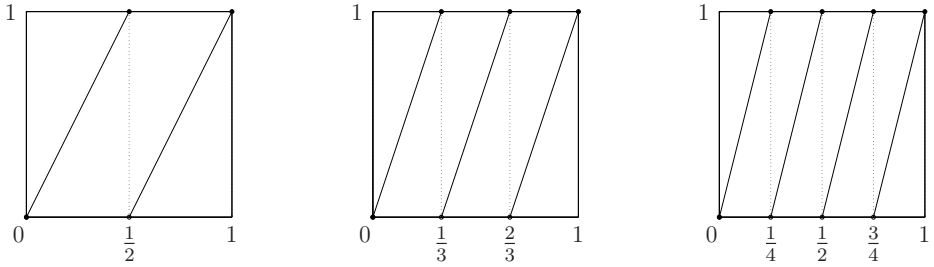
7(iii), $m|\Phi_1(m,\psi)$, which means $\Phi_1(m,\psi) \equiv 0 \pmod{m}$.

■

Now, for each $a \geq 2$, let us define a function $g_a : [0,1] \to [0,1]$ as

$$g_a(x) = \begin{cases} 0 & \text{for } x = 0 \\ a \cdot x - j & \text{for } \dfrac{j}{a} < x \leq \dfrac{j+1}{a} \end{cases}$$

for $0 \leq j \leq a-1$.




(a) The graph of $g_2$ (b) The graph of $g_3$ (c) The graph of $g_4$

Figure 1: The graphs of $g_2$, $g_3$ and $g_4$.

We use some characteristics of $g_a$ for proving most of the number theoretical results in this study. Let us introduce these characteristics and prove some propositions.

**Proposition 9.** *Let $a$ and $b$ be positive integers. Then*

*(i)* $g_{ab} = g_a \circ g_b = g_b \circ g_a$.

*(ii)* ${g_a}^n = g_{a^n}$.

*Proof.* (i) $g_a(x) = \begin{cases} 0 & \text{for } x = 0 \\ ax - j_a & \text{for } \dfrac{j_a}{a} < x \leq \dfrac{j_a+1}{a} \end{cases}$

$$g_a(g_b(x)) = \begin{cases} 0 & \text{for } g_b(x) = 0 \\ ag_b(x) - j_a & \text{for } \dfrac{j_a}{a} < g_b(x) \leq \dfrac{j_a+1}{a} \end{cases}$$

$$= \begin{cases} 0 & \text{for } x = 0 \\ a(bx - j_b) - j_a & \text{for } \dfrac{j_a}{a} < bx - j_b \leq \dfrac{j_a+1}{a} \end{cases}$$

$$= \begin{cases} 0 & \text{for } x = 0 \\ abx - (aj_b + j_a) & \text{for } \dfrac{aj_b+j_a}{ab} < x \leq \dfrac{aj_b+j_a+1}{ab} \end{cases}$$

where $0 \leq j_a \leq a-1$ and $0 \leq j_b \leq b-1$.

Let $k = aj_b + j_a$. Then $k$ runs through all integers between 0 and $ab-1$ (*i.e.* $0 \leq k \leq ab-1$). Therefore, the last step yields

$$g_a(g_b(x)) = \begin{cases} 0 & \text{for } x = 0 \\ abx - k & \text{for } \dfrac{k}{ab} < x \leq \dfrac{k+1}{ab} \end{cases}$$

which is equal to $g_{ab}$. Obviously $g_{ab} = g_{ba}$, since $ab = ba$. Then $g_{ab} = g_a \circ g_b = g_b \circ g_a$.

(ii) This follows from (i), since ${g_a}^n = g_a \circ \cdots \circ g_a$.

■

Now, let us investigate the fixed and periodic points of $g_a$.

**Proposition 10.**

*(i) The function $g_a$ has $a$ many fixed points, which are $j/(a-1)$ for $j = 0, \ldots, a-1$.*

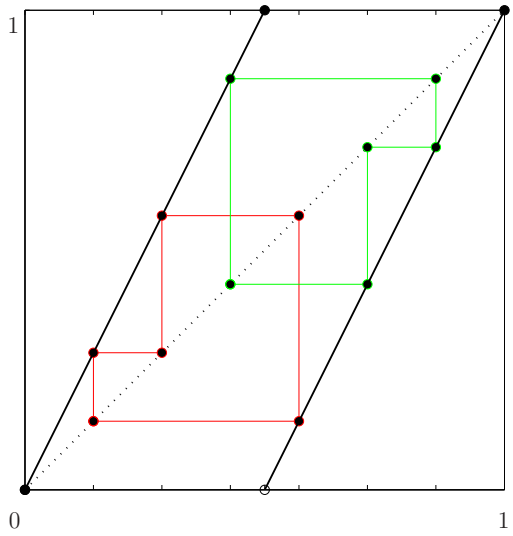
*(ii) The function $g_a$ has $a^n$ many periodic points of period $n$, which are $j/(a^n-1)$ for $j = 0, \ldots, a^n-1$.*

*Proof.*

(i) Fixed points of $g_a$ are those which satisfies $g_a(x) = x$. For the first piece of $g_a$, $x = 0$ is obviously a fixed point. For the second piece, the points which satisfy $ax - j = x$ are fixed points. So $x = j/(a-1)$, for $j = 0, \ldots, a-1$, are fixed points of $g_a$. Since there are $a$ many $j$s, there are exactly $a$ many fixed points of $g_a$.

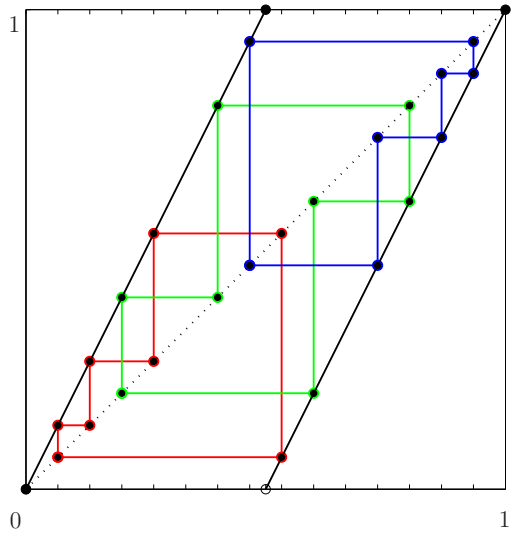
(ii) The function $g_a$'s periodic points of period $n$ are fixed points of $g_{a^n}$ by Proposition 9(ii). Then the result follows from (i).

■




Red colored cycle consists of points $\left\{\frac{1}{7}, \frac{2}{7}, \frac{4}{7}\right\}$.
Green colored cycle consists of points $\left\{\frac{3}{7}, \frac{6}{7}, \frac{5}{7}\right\}$.

Figure 2: 3-cycles of $g_2$.




Red colored cycle consists of points $\left\{\frac{1}{15}, \frac{2}{15}, \frac{4}{15}, \frac{8}{15}\right\}$.
Green colored cycle consists of points $\left\{\frac{3}{15}, \frac{6}{15}, \frac{12}{15}, \frac{9}{15}\right\}$.
Blue colored cycle consists of points $\left\{\frac{7}{15}, \frac{14}{15}, \frac{13}{15}, \frac{11}{15}\right\}$.

Figure 3: 4-cycles of $g_2$.

# Main Results

Now, we are ready to prove Fermat's Little Theorem and some other number theoretical results with the help of $g_a$ and dynamical systems.

**Theorem 11.** (Fermat's Little Theorem) *For all integers $a \geq 2$ and all primes $p$, $a^p \equiv a \pmod{p}$.*

*Proof.* The function $g_a$ satisfies the conditions of $f$ in Theorem 8, since it maps [0,1] into [0,1] and it has $\psi(n) = a^n$ points of period $n$, which is finite.

Let $f$ in Theorem 8 be $g_a$. Then,

$$\begin{aligned} \Phi_1(p,\psi) &\equiv 0 \pmod{p} \\ \psi(p)-\psi(1) &\equiv 0 \pmod{p} \\ a^p - a &\equiv 0 \pmod{p} \end{aligned}$$

Therefore, $a^p \equiv a \pmod{p}$.

■

**Theorem 12.**

*(i) Let $p$ and $q$ be distinct primes and $a \geq 2$. Then $pq|(a^{pq}-a^p-a^q+a)$.*

*(ii) Let $p$ be a prime and $a \geq 2$ be an integer. Then $p^k|a^{p^k}-a^{p^{k-1}}$ for all $k \geq 1$.*

*Proof.*

(i) Similar to the proof of Fermat's Little Theorem, let $f$ in Theorem 8 be $g_a$. Then,

$$\begin{aligned} \Phi_1(pq,\psi) &\equiv 0 \pmod{pq} \\ \psi(pq)-(\psi(p)+\psi(q))+\psi(1) &\equiv 0 \pmod{pq} \\ a^{pq}-a^p-a^q+a &\equiv 0 \pmod{pq} \end{aligned}$$

Therefore, $pq|a^{pq}-a^p-a^q+a$.

(ii) Similar to the proof of Fermat's Little Theorem, let $f$ in Theorem 8 be $g_a$. Then,

$$\begin{aligned} \Phi_1(p^k,\psi) &\equiv 0 \pmod{p^k} \\ \psi(p^k)-\psi(\tfrac{p^k}{p}) &\equiv 0 \pmod{p^k} \\ a^{p^k}-a^{p^{k-1}} &\equiv 0 \pmod{p^k} \end{aligned}$$

Therefore, $p^k|a^{p^k}-a^{p^{k-1}}$.

■

# Some Other Results

In this section, we prove some other number theoretical results which are not required in the proofs of the main results of this study, yet still exciting. We use $g_a$ in this section as well.

**Lemma 13.** *For all integers $a > 1$ and all integers $n \geq 1, a^n = \sum_{m|n} \mathscr{N}_m(g_a)$.*

*Proof.* By Lemma 7(i), we deduce that a point of period $n$ is also a point of minimal period $m$, for some $m|n$. Obviously, the sum of the numbers of the periodic points of these minimal periods is equal to the number of periodic points of period $n$, which is equal to $a^n$ by Proposition 10(ii).

■

**Proposition 14.** *If $\gcd(j, a^n-1) = 1$, then $j/(a^n-1)$ is a minimal $n$-periodic point of $g_a$.*

*Proof.* Assume for a contradiction that $\gcd(j, a^n-1) = 1$ but $j/(a^n-1)$ is not a minimal $n$-periodic point of $g_a$. Then, it must be the case that $j/(a^n - 1)$ is a minimal $k$-periodic point of $g_a$, for some $k|n$ (since $j/(a^n - 1)$ is an $n$-periodic point of $g_a$). Let $m > 1$ be an integer such that $(a^n-1) = m(a^k-1)$. Then $\dfrac{j}{(a^n - 1)} = \dfrac{j}{m(a^k - 1)} = \dfrac{j/m}{(a^k - 1)}$. For this being true, $j/m$ should be an integer. But this means $m$ divides both $j$ and $a^n - 1$, which contradicts with our assumption that $\gcd(j, a^n - 1) = 1$. Therefore, if $\gcd(j, a^n - 1) = 1$ then $j/(a^n - 1)$ must be a minimal $n$-periodic point of $g_a$.

■

**Corollary 15.** *Let $m, n, a$ be integers such that $m, n \geq 1$ and $a \geq 2$. Then $m|n$ if and only if $a^m - 1|a^n - 1$.*

*Proof.* Let $x = \dfrac{1}{a^m - 1}$. Then $x$ is a point of minimal period $m$ for the function $g_a$.

If $m|n$, $x$ is also a point of period $n$. So, $x = \dfrac{j}{a^n - 1}$, for some $j$. Then, $x = \dfrac{1}{a^m - 1} = \dfrac{j}{a^n - 1}$. Therefore, $a^m - 1|a^n - 1$.
If $a^m - 1|a^n - 1$, then $(a^n - 1) = k(a^m - 1)$ for some $k$. Then, $x = \dfrac{1}{a^m - 1} = \dfrac{k}{a^n - 1}$. So, $x$ is also a point of period $n$. Therefore, $m|n$.

■

**Proposition 16.** *If $j_1/(a^n - 1)$ and $j_2/(a^n - 1)$ belong to the same $n$-cycle, then* $\gcd(j_1, a^n - 1) = \gcd(j_2, a^n - 1)$.

*Proof.* Let $x = \dfrac{j_1}{(a^n - 1)}$. Then $g_a(x) = a\dfrac{j_1}{(a^n - 1)} - j = \dfrac{aj_1 - j(a^n - 1)}{(a^n - 1)}$, for some $j$. Then, $\gcd(aj_1 - j(a^n - 1), a^n - 1) = \gcd(aj_1, a^n - 1) = \gcd(j_1, a^n - 1)$. So, every iteration gives the same result. Then $\gcd(j_1, a^n - 1) = \gcd(j_2, a^n - 1)$, for any two point $j_1/(a^n - 1)$ and $j_2/(a^n - 1)$ which belong to the same $n$-cycle. ■

**Corollary 17.** *For any integer $a \geq 2$ and $n \geq 1$, $n|\phi(a^n - 1)$.*

*Proof.* Let $A = \{j/(a^n - 1) : 1 \leq j \leq a^n - 1 \text{ with } \gcd(j, a^n - 1) = 1\}$. Then $|A| = \phi(a^n - 1)$. By Proposition 14, the elements of $A$ are minimal $n$-periodic points of $g_a$. By Proposition 16, if $A$ contains an element of a minimal $n$-cycle, then it contains every element of that minimal $n$-cycle. By Lemma 7(ii), these cycles are distinct. Therefore, $n|\phi(a^n - 1)$.

■

# Conclusion

We have shown that we can prove some number theoretical results with the help of fixed and periodic points. We defined a function and by examining its fixed and periodic points, we have shown some of its characteristics. These

characteristics lead us to the path of proving Fermat's Little Theorem and some other number theoretical results. In conclusion, investigation of fixed and periodic points of a function can open the way in the proofs of some number theoretical results.

# References

[1] W.E. Briggs and W.L. Briggs. Anatomy of a Circle Map. *Mathematics Magazine*, 72(2):116–125, Apr 1999.

[2] R.L. Devaney. *An introduction to chaotic dynamical systems*. Addison-Wesley Redwood City, Calif, 1989.

[3] B.S. Du. Congruence identities arising from dynamical systems. *Applied Mathematics Letters*, 12(5):115–119, 1999.

[4] M. Frame, B. Johnson, and J. Sauerberg. Fixed Points and Fermat: A Dynamical Systems Approach to Number Theory. *The American Mathematical Monthly*, 107(5):422–428, May 2000.

[5] K. Iga. A dynamical systems proof of Fermat's little theorem. *Mathematics magazine*, 76(1):48–51, Feb 2003.

[6] I. Niven and H.S. Zuckerman. *An introduction to the theory of numbers*. Wiley New York, 1991.