5-3-2018

Exploring Dynamical Systems: Number of Cycle and Cycle Lengths

Christine Marcotte

Exploring Dynamical Systems: Number of Cycle and Cycle Lengths

Christine Marcotte

Submitted in Partial Completion of the
Requirements for Commonwealth Honors in Mathematics

Bridgewater State University

May 3, 2018

Dr. Jacqueline Anderson, Thesis Advisor
Dr. Irina Seceleanu, Committee Member
Dr. Ward Heilman, Committee Member

EXPLORING DYNAMICAL SYSTEMS: NUMBER OF CYCLES AND CYCLE LENGTHS

CHRISTINE MARCOTTE

Abstract. In this project, we observe the number of cycles and cycle lengths that are formed by the periodic points in dynamical systems $f(x) = x^d + c$ over the finite field $\mathbb{F}_p$. We analyze data that suggests which functions would create a cycle of length p and which functions would create an even or odd number of cycles. As a result, we prove some foundational theorems to help further describe the behavior of these dynamical systems. In addition, we perform some statistical analysis to help determine if there are any underlying algebraic structures worth investigating. With the help of both the data analysis and the foundational theorems, we were able to create two major theorems about the number of cycles and cycle lengths by fixing the degree d. The first theorem states that there are only two possible nonisomorphic graphs of the dynamical system when the function is a bijection and $d = \frac{p+1}{2}$. In fact, these two distinct graphs correspond to whether or not the constant c is a quadratic residue modulo p. The second theorem states that if $d = p - 2$, then f has at most two fixed points, and there exists a positive integer $n \geq 2$ such that the cycle containing zero has length $n - 1$ and all remaining cycles (excluding fixed points) have length n.

1. Background

Dynamical systems are systems that can be used to model anything that consistently changes over time. Scientists have been using dynamical systems to describe and predict the spread of diseases, the weather, and changes to the environment. In the 1980s, the development of computer technology allowed people interested in dynamical systems to visualize and analyze more complex dynamical systems. In the 1990s, number theorists brought a new perspective to the field and used new mathematical tools to tackle unsolved problems. Specifically, number theorists study simpler systems and use the knowledge gained to help them understand more complicated systems. This area of studying dynamical systems

Date: May 3, 2018.

from a number theory perspective is called arithmetic dynamics. In this project, we will be using techniques developed by number theorists to solve more dynamical systems problems.

2. Introduction

A dynamical system is a set S and a function $f : S \to S$. In a dynamical system, applying a function f to a point s multiple times forms a set called an orbit. Based on the properties of its orbit, a point is classified as a fixed point, periodic point, preperiodic point, or wandering point. A fixed point is a point $x \in S$ such that $f(x) = x$. A periodic point is a point such that $f^n(x) = x$ for some $n \geq 1$. In other words, periodic points are points that are a part of a cycle. On the other hand, preperiodic points are points such that $f^n(x) = f^m(x)$ for some positive integers $n \neq m$, meaning after an initial set of value sequence they eventually fall into a cycle upon repeated iteration of the function. Note that fixed points are periodic points with $n = 1$, and periodic points are preperiodic points. In addition, preperiodic points have finite orbits. Finally, if a point's orbit is infinite, then it is called a wandering point. However, we note that over finite fields all points are preperiodic.

In this project, we will study dynamical systems over finite fields $\mathbb{F}_p$ and functions of the form $f(x) = x^d + c$ for some $d, c, p \in \mathbb{Z}$ where p is a prime number. The focus of this thesis is analyzing cycles of these functions and so we will primarily study periodic points which generate these cycles. However, we will also expand our analysis to preperiodic points since they help us better understand the behavior of these dynamical systems. Moreover, we will graph these dynamical systems to help investigate their behaviors.

One main goal in this project is to determine which functions of the form $f(x) = x^d + c$ over $\mathbb{F}_p$ create one cycle of length p. The other main goal is to be able to predict the number of cycles and the cycle length each function of this form $f(x) = x^d + c$ over $\mathbb{F}_p$ created by restricting the value of the parameter d. After a brief layout of the important definitions and theorems in section 3 and some basic examples in section 4, we demonstrate some foundational theorems in section 5 that will allow us to make progress towards the overall goals. Moreover, in section 6 we perform some permutation statistics and use them to determine if there are

any underlying algebraic structures in these dynamical systems. Lastly, in section 7 we prove two theorems about the number of cycles and cycle lengths of these dynamical systems.

3. Important Definitions and Theorems

Definition 3.1. A *finite field* $\mathbb{F}$ is a finite set together with two binary operations, addition and multiplication, that satisfy the following properties for all $a, b, c \in \mathbb{F}$:

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. There is an additive identity 0 such that $a + 0 = a$
4. There is an inverse element $-a$ such that $a + (-a) = 0$
5. $ab = ba$
6. $a(bc) = (ab)c$
7. There is a multiplicative identity 1 such that $a1 = a$, where $a \neq 0$
8. There is an inverse element a^{-1} such that $a(a^{-1}) = 1$, where $a \neq 0$
9. $a(b + c) = ab + ac$

Definition 3.2. We denote the finite field with p number of elements as $\mathbb{F}_p$.

Definition 3.3. The number of elements in a field is called the *order*. We denote this as $|\mathbb{F}_p| = p$.

Definition 3.4. A *dynamical system* is a set S and a function $f : S \to S$.

Definition 3.5. In a dynamical system $f : \mathbb{F}_p \to \mathbb{F}_p$, applies a function f to a point s multiple times forming a set of numbers called an *orbit*. We denote the orbit of a point $s \in \mathbb{F}_p$ as $\mathcal{O}_f(s) = \{s, f(s), f^2(s), ...\}$.

Definition 3.6. A point $s \in \mathbb{F}_p$ under the map of f is called a *fixed point* if $f(s) = s$. In other words, a point is *fixed* if the orbit $\mathcal{O}_f(s) = \{s\}$.

Definition 3.7. A point $a \in \mathbb{F}_p$ is *periodic* under the map f if $f^n(a) = a$ for some positive integer n. The orbit created by a periodic point $a \in \mathbb{F}_p$ forms a *cycle* and the *cycle length* is the number of periodic points in the cycle. The cycle length is also known as the *period*.

Definition 3.8. *Preperiodic points* are points with finite orbits, but are not necessarily periodic.

Definition 3.9. We represent the behavior of the dynamical system with a *directed graph* that consists of points and arrows. The points represent the numbers in $\mathbb{F}_p$ and the arrows represent where each number is being mapped to by f.

Definition 3.10. A function is a *bijection* if the function is both one-to-one and onto.

Definition 3.11. A nonzero number that is congruent to a square modulo p is called a *quadratic residue modulo p*. In contrast, a number that is not congruent to a square modulo p is called a *nonresidue modulo p*.

Definition 3.12. A *Legendre symbol* of a modulo p is $(\frac{a}{p}) = 1$ if a is a quadratic residue modulo p and $(\frac{a}{p}) = -1$ if a is a nonresidue modulo p.

Definition 3.13. Two graphs are *isomorphic* if they both have the same number of vertices and are connected in the same way. Moreover, they have the same number of edges, same number of cycles, and cycle structure.

Definition 3.14. We refer to two non-isomorphic graphs as *distinct graphs*, meaning they do not have the same cycle structure.

Theorem 3.15. *Let a be an element of order n in a group and let k be a positive integer. Then $< a^k >=< a^{gcd(n,k)} >$ and $|a^k| = \frac{n}{gdc(n,k)}$.*

Theorem 3.16. *(Fermat's Little Theorem). Let p be a prime number, and let a be any number with $a \neq 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 3.17. *(Euler's Criterion). Let p be an odd prime. Then $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p}$.*

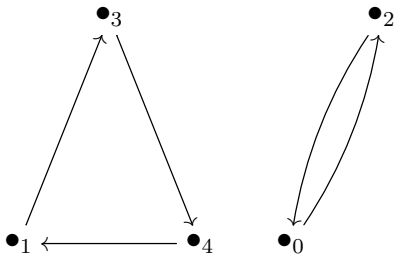


FIGURE 1. $f(x) = x^3 + 2$ over F_5

4. Examples

Example 4.1. To help the reader understand the outlined setting for our research, we begin with an example of a smaller dynamical system of the form $x^d + c$ over $\mathbb{F}_p$. Let $f(x) = x^3 + 2$ be a polynomial defined over $\mathbb{F}_5$.

We will first note that it does not matter which point we begin within the process of iterating since we will eventually map all the points in $\mathbb{F}_5$ to a point in $\mathbb{F}_5$. Let's start by iterating 0. Also, note that we use modular arithmetic so that $f : \mathbb{F}_5 \to \mathbb{F}_5$.

$$f(0) = 0^3 + 2 = 2$$

$$f(2) = 2^3 + 2 = 8 + 2 \equiv 0 \pmod 5$$

Now start with a new point in $\mathbb{F}_5$ to iterate since points 0 and 2 form a cycle of length 2. We can pick any point 1, 3, or 4, so let 1 be our choice.

$$f(1) = 1^3 + 2 = 3$$

$$f(3) = 3^3 + 2 = 27 + 2 \equiv 4 \pmod 5$$

$$f(4) = 4^3 + 2 = 64 + 2 \equiv 1 \pmod 5$$

By Definition 3.7, points 1, 3, and 4 are periodic and form a cycle of length 3. So, $0 \to 2$, $2 \to 0$, and $1 \to 3$, $3 \to 4$, $4 \to 1$. We create the directed graph of the dynamical system. Now let's explore an example of a dynamical system that has one cycle of length p.

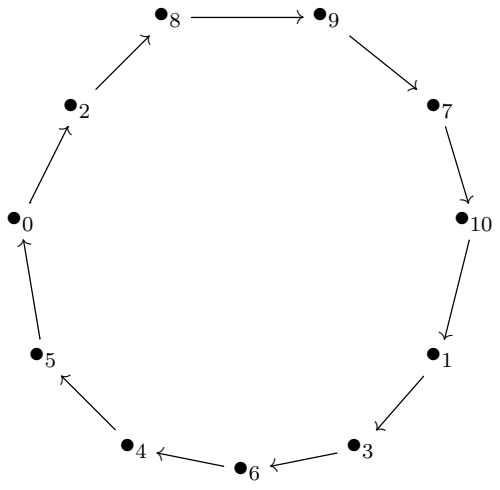


FIGURE 2. Cycle of length 11 for $f(x) = x^9 + 2$ over $\mathbb{F}_{11}$

Example 4.2. Let $f(x) = x^9 + 2$ over $\mathbb{F}_{11}$. We repeat the same process as illustrated in Example 4.1 and pick a point in $\mathbb{F}_{11}$ to iterate.

Starting with 0, we have that

$$f(0) = 0^9 + 2 = 2$$

$$f(2) = 2^9 + 2 = 512 + 2 \equiv 8 \pmod{11}$$

$$f(8) = 8^9 + 2 = 134217728 + 2 \equiv 9 \pmod{11}$$

$$f(9) = 9^9 + 2 = 387420489 + 2 \equiv 7 \pmod{11}$$

$$f(7) = 7^9 + 2 = 40353607 + 2 \equiv 10 \pmod{11}$$

$$f(-1) = (-1)^9 + 2 = -1 + 2 = 1$$

$$f(1) = 1^9 + 2 = 1 + 2 = 3$$

$$f(3) = 3^9 + 2 = 19683 + 2 \equiv 6 \pmod{11}$$

$$f(6) = 6^9 + 2 = 10077696 + 2 \equiv 4 \pmod{11}$$

$$f(4) = 4^9 + 2 = 262144 + 2 \equiv 5 \pmod{11}$$

$$f(5) = 5^9 + 2 = 1953125 + 2 \equiv 0 \pmod{11}$$

Notice that $f^{11}(0) = 0$ which means that iterating 0 produces one cycle of length 11. In fact, every point is periodic and produces a cycle of length 11 since every point in $\mathbb{F}_{11}$ is part of this one cycle. In addition, observe that this function is a bijection since this function is one-to-one and onto. We will explore this fact further in the next section. For now, we explore an example of a function that is not a bijection.

Example 4.3. Let $f(x) = x^6 + 3$ over $\mathbb{F}_7$. The computation below shows that this function is not one-to-one because there are multiple points being in $\mathbb{F}_7$ mapped to the same point. In fact, this function is also not onto because there are no points being mapped to 0,1,2, or 5. When we iterate 0, we notice that it is a preperiodic point because its orbit is finite but $f^n(0) \neq 0$ for any positive n. In this dynamical system, 4 is a fixed point and every other point is preperiodic.

$$f(0) = 0^6 + 3 = 3$$

$$f(3) = 3^6 + 3 = 729 + 3 \equiv 4 \pmod 7$$

$$f(4) = 4^6 + 3 = 4096 + 3 \equiv 4 \pmod 7$$

$$f(1) = 1^6 + 3 = 4$$

$$f(2) = 2^6 + 3 = 64 + 3 \equiv 4 \pmod 7$$

$$f(5) = 5^6 + 3 = 15625 + 3 \equiv 4 \pmod 7$$

$$f(6) = 6^6 + 3 = 46656 + 3 \equiv 4 \pmod 7$$

5. Foundational Theorems

5.1. **Behavior of the Dynamical Systems: Bijections vs Non-Bijections.** Referring back to Definition 3.10, a function is a bijection if the function is both one-to-one and onto. We have observed in Example 4.2 that the function producing one cycle of length p was a

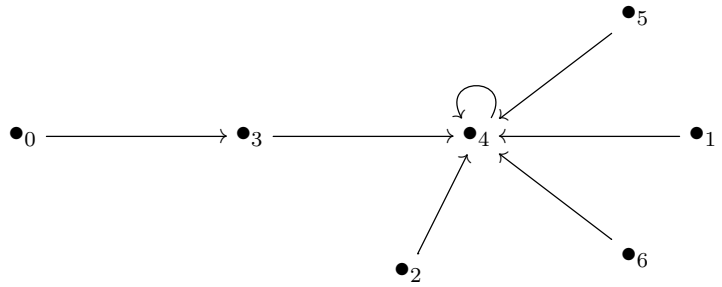


FIGURE 3. $f(x) = x^6 + 3$ over $\mathbb{F}_7$

bijection. In fact, every function of the form $f(x) = x^d + c$ over $\mathbb{F}_p$ producing one cycle of length p is a bijection. This is because every point is periodic, which means that every point in $\mathbb{F}_p$ will be mapped to every point in $\mathbb{F}_p$ exactly once. Since one of our main goals is to figure out which functions of the form $f(x) = x^d + c$ over $\mathbb{F}_p$ create one cycle of length p, we narrow down our search by eliminating functions that are not bijections. In Theorem 5.1, we develop an efficient way to classify a function as a bijection or not a bijection. We set up this conjecture by running simulations in Sage for different values of $d, c, p \in \mathbb{Z}$ and observed that the function is bijective when $\text{GCD}(p-1, d) = 1$. We now prove that this observation is a bi-conditional statement.

Theorem 5.1. *Let $f(x) = x^d + c$ be a polynomial defined over the finite field $\mathbb{F}_p$, where p is a prime number. Then f is a bijection if and only if GCD$(p-1, d) = 1$.*

Proof. We will first show that if $\text{GCD}(p-1, d) = 1$, then f is a bijection. Let $\text{GCD}(p-1, d) = 1$. We want to show that $f(x) = x^d + c$ is one-to-one. Suppose $x_1^d + c \equiv x_2^d + c \pmod{p}$. We will show that $x_1 = x_2$. By subtracting c, we get $x_1^d \equiv x_2^d \pmod{p}$. We will raise both sides to a u power such that $du \equiv 1 \pmod{p-1}$. Note that such a u exists because $\text{GCD}(p-1, d) = 1$. We obtain that $du - (p-1)v = 1$ which implies $du = 1 + (p-1)v$. Raising both sides to the u, we have $x_1^{du} = x_2^{du} \pmod{p}$ which implies $x_1^{1+(p-1)v} \equiv x_2^{1+(p-1)v} \pmod{p}$. It follows that $x_1 x_1^{(p-1)v} \equiv x_2 x_2^{(p-1)v} \pmod{p}$. By Fermat's Little Theorem, we have shown $x_1 = x_2$. Thus, we obtain that the function is one-to-one. Since $\mathbb{F}_p$ is finite, we have that the function is also

onto. Therefore, if the GCD$(p-1,d)=1$, then $f(x)=x^d+c$ over the finite field $\mathbb{F}_p$ is a bijection.

Next, we will show that if f is a bijection, then GCD$(p-1,d)=1$. We will prove the contrapositive. Let $f(x)=x^d+c\in\mathbb{F}_p$ and let the GCD$(p-1,d)=r$ where $r\neq 1$. We need to show that $f(x)=x^d+c$ is not a bijection. We will do this by showing that f is not onto. Since p is a prime number, we know from group theory that $\mathbb{F}_p^*$ has $p-1$ elements and a generator g. So, $\mathbb{F}_p^*=<g>$ where g is a generator of the multiplicative group $\mathbb{F}_p^*$. We know that if $x=0$, then $f(0)=c$. If $x\neq 0$, then $x=g^k$ for some $k\in\mathbb{Z}$. So we have that $f(x)=g^{kd}+c$. We know from group theory that $<g^d>=\{g^d,g^{2d},g^{3d},...\}$. By Theorem 3.15, we have that $|<g^d>|=\frac{p-1}{GCD(p-1,d)}=\frac{p-1}{r}$. Since we are just adding c to the set of elements generated by g^d, the number of possible outputs is still going to be $\frac{p-1}{r}$ when $x\neq 0$. When we include the $x=0$ case, we have that the number of possible outputs is $\frac{p-1}{r}+1$. In order for f to be onto, the number of outputs must be p. However, $r\neq 1$ so the total number of possible outputs of f is not equal to p. We have shown that f is not onto. Therefore, we can conclude that if GCD$(p-1,d)\neq 1$, then $f(x)=x^d+c\in\mathbb{F}_p$ is not a bijection. $\square$

This theorem is very useful because we can determine if a function is a bijection by looking at GCD$(p-1,d)$ instead of computing the orbits of each element in $\mathbb{F}_p$. In the next section, we will study only those functions that are bijections in order to further investigate which functions have a cycle of length p. For now, we study the behavior of functions that are not bijections.

We already know from Theorem 5.1 that if GCD$(p-1,d)\neq 1$, then f is not a bijection. By observing some of the directed graphs of the dynamical systems indicated by functions that are not bijections, we can see that the value of GCD$(p-1,d)$ predicts the behavior of the mapping. In Example 4.3, we have that GCD$(7-1,6)=6$ and there are 6 points being mapped to one point. This means that the mapping of this function is 6-to-1. There are more examples that suggest this claim may be true and we will prove this conjecture in the following theorem.

Theorem 5.2. *Let $f(x) = x^d + c$ over $\mathbb{F}_p$ for some prime number $p \in \mathbb{Z}$. If GCD$(p-1, d) = r$, then the map f is r-to-1 on the set $\mathbb{F}_p^*$.*

Proof. Let $f(x) = x^d + c$ over $\mathbb{F}_p$ and let $\text{GCD}(p-1, d) = r$. We want to show that for every output value y, there are r input values $x_1, x_2, ..., x_r \in \mathbb{F}_p^*$ such that $f(x_i) = y$. We have that $f(g^k) = y$ for some g^k where g is the generator of $\mathbb{F}_p^*$ and $k \in \mathbb{Z}$. We want to show that $f(g^{k+\frac{(p-1)}{r}m}) = y$ for any $m \in \mathbb{Z}$. We have that $g^{kd} + c = y$. So, $f(g^{k+\frac{(p-1)}{r}m}) = (g^{k+\frac{(p-1)}{r}m})^d + c = g^{kd} \cdot g^{\frac{(p-1)}{r}m \cdot d} + c$. By Fermat's Little Theorem, we know that $g^{p-1} = 1$. Since $m, d, r \in \mathbb{Z}$ and we have that $r|d$ from our assumption that $\text{GCD}(p-1, d) = r$, then $\frac{m \cdot d}{r} \in \mathbb{Z}$. This means that $g^{\frac{(p-1)}{r}m \cdot d} = 1$ which implies that $g^{kd} \cdot g^{\frac{(p-1)}{r}m \cdot d} + c = g^{kd} + c = y$. So we have shown that $f(g^{k+\frac{(p-1)}{r}m}) = y$. We will use this to find the number of inputs that map to y by looking at the set $G = \{g^{k+\frac{(p-1)}{r}m} : m \in \mathbb{Z}\} = \{g^k, g^{k+\frac{p-1}{r}}, g^{k+\frac{2(p-1)}{r}}, ...\}$. Notice that when $m = r$ we have $g^{k+p-1} = g^k \cdot g^{p-1} = g^k$. This means that $|G| = r$. So there are r inputs being mapped to y. In other words, $f^{-1}(y) = \{g^{k+\frac{(p-1)}{r}m} : 0 \leq m \leq r-1\}$. Therefore, we can conclude that if $\text{GCD}(p-1, d) = r$, then the map f is r to 1 on the set $\mathbb{F}_p^*$. □

This theorem is very powerful because we can understand the general dynamical behavior of the function on $\mathbb{F}_p$ without having to iterate points and draw the directed graph. While looking at the graphs of various functions that are not bijections, we observed another pattern for functions that have $d = p - 1$. It seems that every point that does not equal 0 gets mapped to the point $c+1$. Example 4.3 shows this for $p = 7$, $d = 6$, $c = 3$ with every nonzero point mapped to $c + 1 = 4$. We prove this claim using Fermat's Little Theorem.

Theorem 5.3. *Let $f : \mathbb{F}_p \to \mathbb{F}_p$ with $f(x) = x^d + c$. If $d = p - 1$, then every nonzero element maps to the same point $c + 1$.*

Proof. Let $k \in \{1, 2, ..., p-1\}$ and let $d = p-1$ such that $f(k) = k^{p-1} + c$. By Fermat's Little Theorem, we have that $k^{p-1} \equiv 1 \pmod{p}$. So $f(k) = k^{p-1} + c \equiv 1 + c \pmod{p}$. Therefore, every nonzero element maps to the point $c + 1$. □

5.2. **Cycle Lengths When the Degree is 1.** When the degree $d = 1$ and the constant $c = 0$, then the dynamical system is $f(x) = x$ over $\mathbb{F}_p$. By Definition 3.6, every $x \in \mathbb{F}_p$ is a fixed point. Thus, there are p points with cycles of length 1. However, when $d = 1$ and c is nonzero, we obtain a dynamical system that contains one cycle of length p. Using some algebraic ideas, we prove this.

Theorem 5.4. *Let $f(x) = x^d + c$ be a polynomial defined over $\mathbb{F}_p$. If $d = 1$ and $1 \leq c \leq p-1$, then every element of $\mathbb{F}_p$ is periodic with period p. (In other words, the graph of the dynamical system consists of a single cycle of length p.)*

Proof. Let $d = 1$ and let c be a nonzero constant. Then $f(x) = x + c \in \mathbb{F}_p$. We have defined the x and c such that both $x, c \in \{0, 1, .., p-1\}$. Without loss of generality, let's consider the orbit of c. So, $f(c) = c + c$. Since we are iterating c, we now plug in $c + c$ to get $f(c + c) = c + c + c$ and repeat this process. By definition, the orbit of c is equivalent to $< c >= \{c, c + c, c + c + c, ...\}$. We know from group theory that $| < c > | = p$ because every nonzero element in $\mathbb{F}_p$ is a generator of the additive group. Since $| < c > | = p$, there will be no repeating values. This means there will be one cycle with p periodic points. Therefore, we can conclude that if $d = 1$ and c is a nonzero constant, $f(x) = x^d + c$ over $\mathbb{F}_p$ has a cycle of length p. □

Theorem 5.5. *(A. Chen, A. Gassert, K. Stange).* Let $f(x) = x^d + c$ over $\mathbb{F}_p$ such that the dynamical system consists of one cycle of length p. If $p \equiv 1 \pmod 4$ and $d \equiv 3 \pmod 4$, then the dynamical system does not consist of one cycle of length p.

The proof for this theorem proves that if $p \equiv 1 \pmod 4$ and $d \equiv 3 \pmod 4$, then these dynamical systems consist of an even number of cycles. This theorem helps us determine which dynamical systems consist of one p-cycle because it allows us to eliminate dynamical systems that have an even number of cycles.

6. Permutation Statistics

Recall by Theorem 5.1 that if $\text{GCD}(p-1, d) = 1$, then the map $f : \mathbb{F}_p \to \mathbb{F}_p$ given by $f(x) = x^d + c$ is a bijection. The mappings of these bijections can be viewed as elements of S_p. In order to better understand these maps and formulate conjectures, we can examine their behavior with respect to various permutation statistics. Examples of permutation statistics include number of cycles, longest cycle length, and number of fixed points. We are interested in determining whether these statistics behave like they are evaluated at permutations sampled uniformly from S_p. If these statistics don't behave like they are evaluated at permutations sampled uniformly from S_p, then we will focus on finding an underlying algebraic structure in $\mathbb{F}_p$ and formulate conjectures.

We will begin to determine this by examining some facts about the cycle structure of random permutations. Let π be a permutation chosen from the uniform distribution on S_n and let $C_n = C(\pi)$ be the number of cycles in π. For example, if π is the permutation of $\{1, 2, .., 6\}$ written in one-line notation as 532146, then π can be expressed in cycle notation as (154)(23)(6). Thus, we have that $C(\pi) = 3$. We observe that the number of permutations of cycle type $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ is given by

$$\frac{n!}{\Pi_{m=1}^{n} m^{\lambda_m} \lambda_m!}$$

where λ_m is the number of m-cycles such that $m = 1, 2, ..., n$. The explanation is that there are $n!$ ways to distribute the n symbols amongst the fixed placement of the parentheses dictated by the cycle type. However, this over-count since we can permute the λ_m m-cycles amongst themselves and we can write each m-cycle in m different ways. Next, we will use the formula for the number of permutations for a given cycle type to find the probability that a permutation is drawn uniformly at random from S_n has cycle type $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$. We can describe this probability as the proportion between the number of permutations for a

given cycle type and the number of elements in S_n. Thus, we obtain

$$\mathbb{P}\{\sigma \sim 1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\} = \frac{\frac{n!}{\Pi_{m=1}^{n} m^{\lambda_m}\lambda_m!}}{n!} = \frac{1}{\Pi_{m=1}^{n} m^{\lambda_m}\lambda_m!}. \tag{1}$$

In the next section, we will use this information to compute the probabilities of certain cycle types occuring in S_{17}.

6.1. **Probabilities of Permutations in S_{17}.** Let us consider functions of the form $x^d + c$ over $\mathbb{F}_{17}$ that are bijections. Given that the following d-values: 3, 5, 7, 9, 11, 13, and 15 form bijections in $\mathbb{F}_{17}$, we have 119 possible graphs of the dynamical system. However, there were only 28 non-isomorphic graphs out of the 119 graphs created by the bijections in $\mathbb{F}_{17}$. We can think of these graphs as cycle types in S_{17}. For example, we have that the cycle lengths created by the function $x^3 + 1$ over $\mathbb{F}_{17}$ is 9,5,2,1. We can think of this as a permutation in S_{17} with cycle type $9^1 5^1 2^1 1^1$. Now, we will compute the probabilities of these 28 different cycle types occurring in S_{17} using formula (1). The probabilities are listed in Table 1.

6.2. **Observed vs. Expected.** In this subsection, we will record the number of each cycle type observed from the functions that are bijections over $\mathbb{F}_{17}$. We will also compute the expected number of each cycle type in a sample of 119 permutations from S_{17}. Let

$$X_k^{\lambda} = \begin{cases} 1 & kth \quad observation \quad type \quad \lambda \\ 0 & otherwise \end{cases}$$

where the observation cycle types were drawn independently and uniformly at random from S_{17}. Then the number of observations in 119 permutations of S_{17} is given by $\mathbb{E}(Y_\lambda) = \mathbb{E}(\sum_{k=1}^{119} X_k) = \sum_{k=1}^{119} \mathbb{E}(X_k)$. Observe that $\mathbb{E}(X_k)$ is the probability of a cycle type λ being drawn randomly from S_{17}. Thus, we obtain $\mathbb{E}(Y_\lambda) = \frac{119}{\Pi_{k=1}^{119} k^{\lambda_k}\lambda_k!}$. Using this formula, the expected values and observed values are listed in Table 2.

TABLE 1. Probabilities of cycle types in S_{17}

cycle lengths	probability in $\mathbf{S}_{17}$
9,5,2,1	$\frac{1}{90}$
11,6	$\frac{1}{66}$
9,8	$\frac{1}{72}$
11,3,2,1	$\frac{1}{66}$
15,2	$\frac{1}{30}$
14,1,1,1	$\frac{1}{84}$
7,5,4,1	$\frac{1}{140}$
6,6,4,1	$\frac{1}{288}$
9,4,2,1,1	$\frac{1}{144}$
14,2,1	$\frac{1}{28}$
17	$\frac{1}{17}$
11,4,2	$\frac{1}{88}$
12,5	$\frac{1}{60}$
10,7	$\frac{1}{70}$
6,6,3,2	$\frac{1}{432}$
4,4,4,3,1,1	$\frac{1}{1152}$
16,1	$\frac{1}{16}$
4,4,2,2,2,1,1,1	$\frac{1}{9216}$
4,4,2,2,1,1,1,1,1	$\frac{1}{30720}$
2,2,2,2,2,2,2,1,1,1	$\frac{1}{3870720}$
2,2,2,2,1,1,1,1,1,1,1,1,1	$\frac{1}{139345920}$

Now, we want to set up a hypothesis test to determine the functions that are bijections over $\mathbb{F}_{17}$ represent a uniform sample from S_{17}. One might think to a chi-squared test, but we suspect that the underlying assumptions are not satisfied in this case. Instead, we will look to run a different test.

6.3. **Hypothesis Testing.** Recall that we let $C_n = C(\pi)$ be the number of cycles in π. We will note that when suitably standardized, C_n is asymptotically normal. To see that this is so, we will construct random permutations using the Chinese Restaurant Process. In a restaurant with many large circular tables, Person 1 enters and sits at a table. Then Person 2 enters and either sits to the right of Person 1 or at a new table with equal probability. In general, when person k enters, they are equally likely to sit to the right of any of the $k-1$ seated customers or to sit at an empty table. We associate the seating arrangement after n people have entered with the permutation whose cycles are the tables with occupants that

TABLE 2. Observed vs. Expected

Cycle Lengths	Observed Value	Expected Value
9,5,2,1	4	$\frac{119}{90} = 1.322$
11,6	6	$\frac{119}{66} = 1.803$
9,8	10	$\frac{119}{72} = 1.653$
11,3,2,1	4	$\frac{119}{66} = 1.803$
15,2	4	$\frac{119}{30} = 3.967$
14,1,1,1	6	$\frac{119}{84} = 1.417$
7,5,4,1	4	$\frac{119}{140} = .85$
6,6,4,1	4	$\frac{119}{288} = .413$
9,4,2,1,1	8	$\frac{119}{144} = .826$
14,2,1	8	$\frac{119}{28} = 4.25$
17	8	$\frac{119}{17} = 7$
11,4,2	8	$\frac{119}{88} = 1.352$
12,5	2	$\frac{119}{60} = 1.983$
10,7	2	$\frac{119}{70} = 1.7$
6,6,3,2	2	$\frac{119}{432} = .275$
9,6,1,1	2	$\frac{119}{108} = 1.102$
10,3,2,2	2	$\frac{119}{240} = .496$
10,5,1,1	2	$\frac{119}{50} = 2.38$
6,4,3,2,2	8	$\frac{119}{576} = .207$
8,4,2,2,1	8	$\frac{119}{256} = .465$
8,7,1,1	4	$\frac{119}{112} = 1.063$
3,3,3,3,3,2	2	$\frac{119}{58320} = .002$
4,4,4,3,1,1	2	$\frac{119}{1152} = .103$
16,1	2	$\frac{119}{16} = 7.438$
4,4,2,2,2,1,1,1	2	$\frac{119}{9216} = .013$
4,4,2,2,1,1,1,1,1	2	$\frac{119}{30720} = .004$
2,2,2,2,2,2,2,1,1,1	2	$\frac{119}{3870720} = .00003$
2,2,2,2,1,1,1,1,1,1,1,1,1	1	$\frac{119}{139345920} = 8.5 \times 10^{-7}$

read off clockwise. Thus, the argument that this generates a permutation from the uniform distribution follows by induction. It's true when $n = 1$, and if we have a seating arrangement corresponding to a uniform permutation of $[n-1]$ before person n sits down, then the rules of the process ensure that we have a uniform permutation of n afterward.

If we let $X_{n,k}$ be the indicator that Person k sits at an unoccupied table, then $C_n = \sum_{k=1}^{n} X_{n,k}$. We obtain

$$\mathbb{E}(C_n) = \sum_{k=1}^{n} \mathbb{E}(X_{n,k}) = \sum_{k=1}^{n} \frac{1}{k}$$

and

$$\mathrm{Var}(C_n) = \sum_{k=1}^{n} \mathrm{Var}(X_{n,k}) = \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k^2}.$$

Now let N be the number of functions that are bijections over $\mathbb{F}_p$. In our case, where $p = 17$, $N = 119$. Then we let $\bar{C}_n = \frac{1}{N}\sum_{i=1}^{N} C(\pi_i)$ be the average number of cycles. Since we have shown the asymptotic normality of C_n, then by the central limit theorem $\bar{C}_n$ is approximately normal with mean $\mu = \sum_{k=1}^{p} \frac{1}{k}$ and standard deviation $\sigma = \sqrt{\frac{\sum_{k=1}^{p} \frac{1}{k} - \frac{1}{k^2}}{N}}$. Thus, we can set up a hypothesis test such that our null hypothesis is that the statistics of the bijections over $\mathbb{F}_{17}$ represent a uniform sample ofS_{17}.

We can compute from Table 2 that the average observed cycle length is $\frac{455}{119}$ which simplifies to $\frac{65}{17}$. Now the probability that a normal random variable with mean $\mu = \sum_{k=1}^{17} \frac{1}{k} \approx 3.4396$ and standard deviation $\sigma = \sqrt{\frac{\sum_{k=1}^{17} \frac{1}{k} - \frac{1}{k^2}}{119}} \approx .1247$ exceeds $\frac{65}{17}$ is equal to the area to the right of $\frac{\frac{65}{17} - 3.4396}{.1247} \approx 3.08$ under the standard normal curve. This area is about .00103 which leads us to reject the hypothesis that the average number of cycles observed is representative of that for uniformly random permutations in favor of the alternative hypothesis that the average is larger at a 5 percent significance level. It is possible that including or excluding other c and d values would change the conclusions slightly, but it looks like the functions that are bijections over $\mathbb{F}_{17}$ don't behave like random permutations from S_{17}. Thus, there is reason to believe that there is an underlying algebraic structure that is causing the behavior of these mappings. We can repeat this process with other bijections over $\mathbb{F}_p$ and explore whether these bijections are worth further analyzing. In the next section, we will analyze data more closely and explore two main theorems.

7. Main Results

Using Sage, we are able to calculate the cycle lengths, the number of cycles, and create the graphs of each dynamical system of the form $f(x) = x^d + c \in \mathbb{F}_p$ for any given $d, c \in \mathbb{Z}$ and prime numbers $p \leq 43$. In Excel, we record all of the data and organize the data into columns based on each dynamical systems' degree, constant, finite field, cycle lengths, number

TABLE 3. Number of distinct graphs when $d = \frac{p+1}{2}$

p-value	d-value	distinct graphs
5	3	2
13	7	2
17	9	2
29	15	2
37	19	2

of cycles, and number of distinct graphs. Using Theorem 5.1, we categorize the data by separating functions that are bijections and functions that are not bijections. Since we are interested in the cycles and cycle lengths, we focus mostly on functions that are bijections and discover some interesting patterns. In the next subsection, we will observe three tables containing data illustrating these patterns. The first two tables will provide evidence for the first main theorem and the third table will provide evidence for the second main theorem. In the second subsection, we will prove these theorems and provide examples.

7.1. **Data Analysis.** We observe in Table 3 that for these specific p-values and d-values, the dynamical systems create only two graphs that are distinct, meaning there are two non-isomorphic graphs. Furthermore, we have that given any nonzero c-value the structure of the graph has only one of two options. Observe that the p-values in the Table 3 are congruent to 1 modulo 4. In addition, observe that the degree of these functions or the d-value is $\frac{p+1}{2}$. Based on more data, these observations are true for more than the illustrated p-values and d-values. In the next section we construct a theorem based on these patterns and prove it. However, we are still interested in finding a relationship between the c-values and which of the two types of graphs are created. We explore this in Table 4.

In Table 4, we observe the different c-values for each given d-value and p-value already illustrated in Table 3. For example, when $p = 5, d = 3$, and $c = 1, 4$, we observe in Table 2 one of the two structures of the graphs formed by $f(x) = x^3 + c$ over $\mathbb{F}_5$. The other cycle

TABLE 4. Cycle structures when $d = \frac{p+1}{2}$

p-value	d-value	c-value	cycle lengths
5	3	1, 4	4, 1
5	3	2, 3	2, 3
13	7	1, 3, 4, 9, 10, 12	6, 4, 2, 1
13	7	2, 5, 6, 7, 8, 11	5, 4, 2, 2
17	9	1, 2, 4, 8, 9, 13, 15, 16	6, 4, 3, 2, 2
17	9	3, 5, 6, 7, 10, 11, 12, 14	8, 4, 2, 2, 1

structure occurs when $c = 2$ and $c = 3$. Notice that 1 and 4 are squares modulo 5 and that 2 and 3 are not squares modulo 5. After analyzing these c-values, it is evident that the two non-isomorphic graphs are determined by whether the c-value is a quadratic residue modulo p. More specifically, Table 4 suggests that if the c-value is a quadratic residue (3.11) modulo p, then one of the two graphical structures is formed. Additionally, if the c-value is a nonresidue (3.11) modulo p, then the other graphical structure is formed. Using both the data and observations from Tables 3 and 4, we create and prove the first main theorem in the next subsection.

Table 5 illustrates dynamical systems where the degree is $p-2$ and the constant is nonzero. As shown below, there are no more than two fixed points in each dynamical system of this form. In addition, there seems to be a pattern with the cycles when we eliminate the fixed points. In the first row of the table, we observe that the cycle lengths are all the same except for the last cycle length, which is one less than the others. We also notice this same pattern in rows 2 and 5 when the fixed points are eliminated. Another observation worth noting is that when there is only 1 fixed point, the remaining cycle is of length $p-1$. In the next subsection we will use these observations to create and prove the second main theorem.

TABLE 5. Cycle structures for $d = p - 2$

p-value	d-value	c-value	cycle lengths	number of fixed points
19	17	6, 13	4, 4, 4, 4, 3	0
23	21	4, 17	8, 8, 7	0
29	27	3, 26	7, 7, 7, 6, 1, 1	2
29	27	5, 24	28, 1	1
31	29	4, 27	10, 10, 9, 1, 1	2
37	35	1, 36	19, 18	0
41	39	5, 36	7, 7, 7, 7, 7, 6	0
41	39	7, 8, 33, 34	21, 20	0
43	41	7, 19, 20, 23, 24, 36	14, 14, 13, 1, 1	2
43	41	13, 30	6, 6, 6, 6, 6, 6, 5, 1, 1	2
45	43	1, 4, 11, 18, 29, 36, 43, 46	16, 16, 15	0
53	51	4, 10, 14, 39, 43, 49	9, 9, 9, 9, 9, 8	0

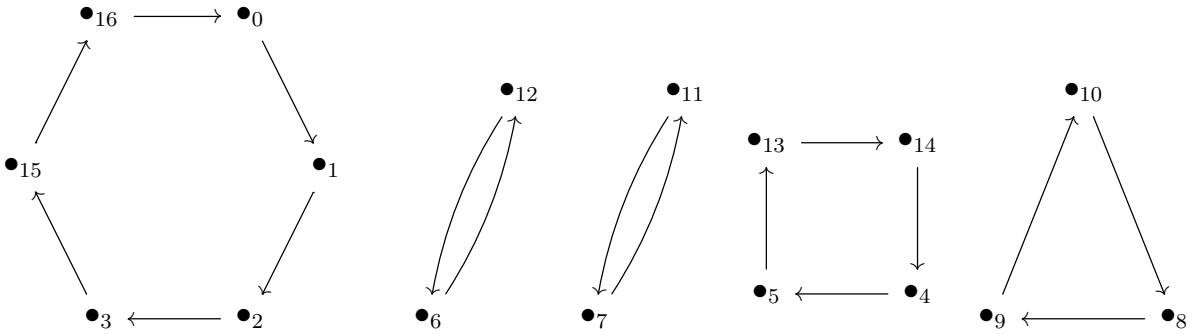
7.2. **Main Theorems.** In this section we use the observations made in the last section and introduce the two main theorems. In addition, we illustrate each of them with an example and formally prove both of these theorems. In order to prove Theorem 6.1, we show that $f(x) = x^d + c$ over $\mathbb{F}_p$ is a bijection when $p \equiv 1 \pmod 4$ and $d = \frac{p+1}{2}$. Then, we use Euler's Criterion to reduce the polynomial using quadratic reciprocity. Lastly, using our knowledge of dynamical systems and quadratic reciprocity, we find the cycle lengths and number of cycles to show there are two distinct graphs. The main idea behind the second main theorem is that we represent the functions of the form $x^{p-2} + c$ over $\mathbb{F}_p$ using matrices. Then we find the fixed points by finding the eigenvalues. Also, we find the cycle lengths by iterating the matrix until we reach the identity. Let us first state Theorem 6.1.

Theorem 7.1. If $f(x) = x^d + c \in \mathbb{F}_p$ such that $p \equiv 1 \pmod 4$, $d = \frac{p+1}{2}$, and $c \neq 0$, then there are exactly two non-isomorphic graphs of the dynamical system, corresponding to whether c is a quadratic residue or nonresidue modulo p.

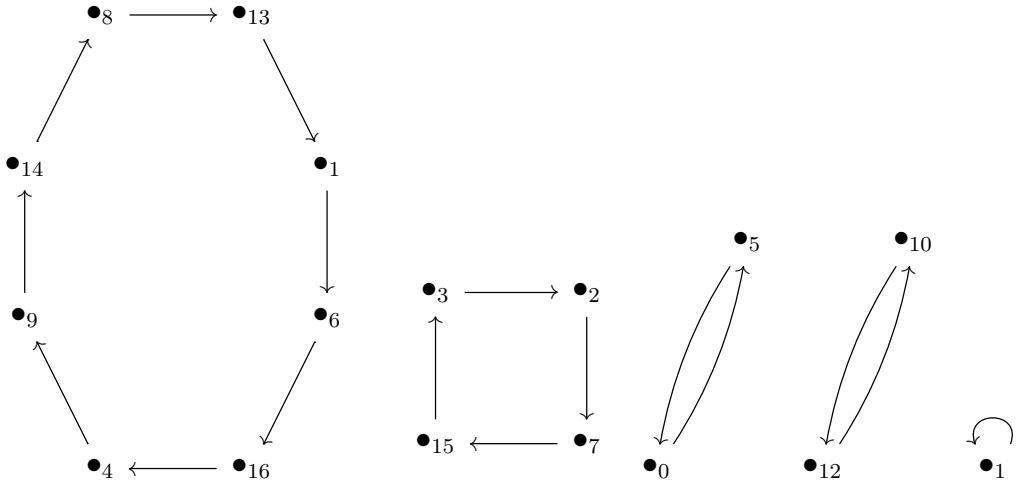
Example 7.2. To illustrate this theorem with an example, we consider $f(x) = x^9 + c$ over $\mathbb{F}_{17}$. The values $c = 1, 4, 8, 9, 13, 15, 16$, which are quadratic residues mod 17, all create a dynamical system of cycle lengths $6, 4, 3, 2, 2$. Thus, all of these graphs created by the quadratic residues are isomorphic to each other. In contrast, the c-values that are nonresidues

modulo 17 create cycle lengths $8, 4, 2, 2, 1$. Similarly, all of these graphs created by the nonresidues are isomorphic to each other. The graphs of the dynamical systems when the c-values are 1 and 5 are shown below.

$f(x) = x^9 + 1$ over $\mathbb{F}_{17}$



$f(x) = x^9 + 5$ over $\mathbb{F}_{17}$



Proof of Theorem 7.1. Suppose that $f(x) = x^d + c \in \mathbb{F}_p$ such that $p \equiv 1 \pmod 4$ and $d = \frac{p+1}{2}$. We will show that $f(x)$ is a bijection. More specifically, we will use Theorem 5.1 to show that the $\text{GCD}(p-1, d) = 1$. Let us consider $\text{GCD}(p-1, \frac{p+1}{2})$ when $p \equiv 1 \pmod 4$. We note that factors of $\frac{p+1}{2}$ are also factors of $p+1$. Next, let us observe that $p+1$ and $p-1$ can only have a common factor of 2 because they are two units apart. However, $\frac{p+1}{2}$ is odd since we have that $p \equiv 1 \pmod 4$ so $p+1$ and $p-1$ do not share a common factor of 2. Thus, $\text{GCD}(p-1, \frac{p+1}{2}) = 1$ and so $f(x)$ is a bijection.

Next, since $f(x)$ is a bijection, we have that every point is periodic. In other words, every point is part of a cycle. Now, we will show that there are exactly two distinct graphs of the dynamical system where one is created when c is a quadratic residue and the other is created when c is a nonresidue modulo p. First, we will reduce the degree of the polynomial by observing that if $d = \frac{p+1}{2}$, then $f(x) = x^{\frac{p+1}{2}} + c = x \cdot x^{\frac{p-1}{2}} + c$. By Euler's Criterion (Theorem 3.17), we have that $f(x) = x + c$ if x is a quadratic residue modulo p and $f(x) = -x + c$ if x is a nonresidue modulo p. Without loss of generality, we will list the finite sets of quadratic residues and nonresidues in increasing order. We have that the quadratic residues are $\{q_1, q_2, \ldots, q_{\frac{p-1}{4}}, -q_{\frac{p-1}{4}}, \ldots, -q_2, -q_1\}$ and the nonresidues are $\{n_1, n_2, \ldots, n_{\frac{p-1}{4}}, -n_{\frac{p-1}{4}}, \ldots, -n_2, -n_1\}$. Note that we know $-q_1$ is a quadratic residue because -1 is a quadratic residue modulo p and a quadratic residue multiplied by a quadratic residue is a quadratic residue. A similar argument can be made for $-n_1$. Next, we will explore the two cases: c is a quadratic residue or c is a nonresidue.

Suppose c is a quadratic residue. We will iterate each point until we reach the first nonresidue. We will start by iterating 0 and obtain $0 \to c \to 2c \to \cdots \to n_1c \to -(n_1-1)c \to -(n_1-2)c \to \cdots \to -c \to 0$. Thus we have that the length of this cycle is $2n_1$ since the number of points in the cycle from 0 to n_1 is n_1 and the number of points in the cycle from n_1 back to 0 is n_1. Next we iterate $(n_1 + 1)c$, since it is not part of the first cycle, until we reach the next nonresidue n_2c. We obtain an orbit that looks like $(n_1 + 1)c, (n_1 + 2)c, \ldots n_2c, -(n_2 - 1)c, -(n_2 - 2)c, \ldots, -(n_1)c$. Then the cycle length is $2(n_2 - n_1)$ since the number of points in the cycle from n_1 to n_2 is $n_2 - n_1$ and the number of points back to n_1 is the same. Continuing this process we have that the cycle lengths when c is a quadratic residue are $\{2n_1, 2(n_2 - n_1), ..., 2(n_{\frac{p-1}{4}} - n_{\frac{p-1}{4}-1}), p - 2n_{\frac{p-1}{4}}\}$. We obtain the last cycle length $p - 2n_{\frac{p-1}{4}}$ by subtracting all the previous cycle lengths from p since there are p points and every point is part of a cycle. Notice, not including the last cycle length, the number of cycles is $\frac{p-1}{4}$. Thus, if we include the last cycle we have that the total number of cycles is $\frac{p-1}{4} + 1$. Therefore, we have shown that the graphs created when $d = \frac{p+1}{2}$ and c is

quadratic residue are all isomorphic. This is because they have the same cycle lengths and number of cycles.

Now, suppose that c is a nonresidue. Similar to the argument made when c was a quadratic residue, we iterate each point until we reach the first quadratic residue. So we iterate 0 and obtain a cycle of length $2q_1$. Then, we start with the next nonresidue that is not contained in the first cycle which is $(q_1+1)c$. Iterating this point, we obtain that the cycle length of this cycle is $2(q_2-q_1)$. Thus, continuing this process we have that the cycle lengths when c is a nonresidue are $\{2q_1, 2(q_2-q_1), ..., 2(q_{\frac{p-1}{4}} - q_{\frac{p-1}{4}-1}), p-2q_{\frac{p-1}{4}}\}$. By similar argument made when c is a quadratic residue, we have that the number of cycles is $\frac{p-1}{4}+1$. Thus, dynamical systems of this form with $d=\frac{p+1}{2}$ and constants that are nonresidues are isomorphic because they have the same number of cycles and the same cycle lengths.

Therefore, by case 1 and case 2 we have shown that there are exactly two distinct graphs of the dynamical systems of the form $f(x)=x^d+c \in \mathbb{F}_p$ for any given $p \equiv 1 \pmod 4$ and $d=\frac{p+1}{2}$. □

Theorem 7.3. *$d=p-2$ and $c \neq 0$, then f has at most two fixed points, and there exists a positive integer $n \geq 2$ such that the cycle containing zero has length $n-1$ and all remaining cycles (excluding fixed points) have length n.*

Moreover, f has two fixed points if c^2+4 is a quadratic residue modulo p, one fixed point if $c^2+4 \equiv 0 \pmod p$, and no fixed points if c^2+4 is a quadratic nonresidue modulo p.

Proof. Suppose $f(x)=x^d+c$ over $\mathbb{F}_p[x]$ and $d=p-2$. Then, $f(x)=x^{p-2}+c$. By Fermat's Little Theorem we have that $f(x)=x^{p-1}\cdot x^{-1}+c=x^{-1}+c$. We can reframe $f(x)=x^{-1}+c$ in $\mathbb{P}^1(\mathbb{F}_p)$. Let us define $g(x)=\dfrac{cx+1}{x}$. Note that $f(x)=g(x)$ as long as $x \neq 0$. We have $f(0)=c$ but $g(0)=\infty$ and $g(\infty)=c$. Thus, $g(x)$ is a dynamical system over $\mathbb{P}^1(\mathbb{F}_p)$.

We can think of $g(x)$ as a fractional linear transformation, which can be represented by a matrix $M=\begin{bmatrix} c & 1 \\ 1 & 0 \end{bmatrix}$. Let $\vec{x}$ be the vector $\begin{bmatrix} x \\ 1 \end{bmatrix}$ so that $g(x)=M\vec{x}$. Then, we have that $g^n(x)=M^n\vec{x}$. So, the cycle length for x is n if n is the smallest positive integer such that

$M^n\vec{x} = \vec{x}$. That can happen if $\vec{x}$ is an eigenvector for M^n, or if M^n is the identity matrix in $PGL_2(\mathbb{F}_p)$. Thus, every $\vec{x}$ that is not an eigenvector is periodic of period n, where n is the order of $M \in \mathrm{PGL}_2(\mathbb{F}_p)$.

We find the eigenvalues by computing the determinant of the matrix $\begin{bmatrix} c-\lambda & 1 \\ 1 & -\lambda \end{bmatrix}$ and setting it equal to zero. The determinant is $\lambda^2 - c \cdot \lambda - 1$. Setting this equal to zero and solving for λ we obtain that the eigenvalues for M are:

$$\lambda = \frac{c \pm \sqrt{c^2+4}}{2}.$$

Let us note that the eigenvalues for M are also the fixed points of $g(x)$ and $f(x)$.

If $c^2 + 4$ is a quadratic residue modulo p, then we have 2 solutions, so M is diagonalizable. In this case, to find the fixed points, we solve $M\vec{x} = \lambda\vec{x}$ for x:

$$M\vec{x} = \begin{bmatrix} cx+1 \\ x \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda \end{bmatrix}$$

The remaining points will have period n.

In the case where $c^2 + 4$ is a nonresidue modulo p, there are no fixed points, and every point has period n.

In the case where $c^2 + 4 = 0$, there is one fixed point. We observe that this case only happens if $p \equiv 1 \pmod 4$ because it requires -4 to be a quadratic residue.

Since we have the extra point at infinity in $g(x)$, we have that $f(x)$ has one less point than $g(x)$. Thus, there will be one cycle of length $n-1$. Additionally, this cycle of length $n-1$ will contain the point zero since $g(0) = \infty$ and we are taking away the point at infinity in $f(x)$. Therefore, $f(x)$ has at most two fixed points, and there exists a positive integer $n \geq 2$ such that the cycle containing zero has length $n-1$ and all remaining cycles (excluding fixed points) have length n. □

Corollary 7.4. *If $d = p-2$, $c \neq 0$, and f has exactly one fixed point, then every remaining point is part of one cycle of length $p-1$.*

Proof. Let $f(x) = x^{p-2} + c$ over $\mathbb{F}_p$ such that $c \neq 0$. Suppose that f has exactly one fixed point. By Theorem 7.3, we have that, including the point at infinity, all non-fixed points have cycles of equal length. Thus, including the point at infinity, we have p points remaining since 1 point is fixed. Since p is prime, p cannot be divided into cycles of equal length. Therefore, every remaining point is part of one cycle of length $p - 1$. □

Example 7.5. Let us further understand the second main theorem by considering the example $f(x) = x^{15} + 2$ over $\mathbb{F}_{17}$. In this case, we have that $p = 17$ and $c = 2$. Recall that we will find the fixed points by evaluating $\lambda = \dfrac{c \pm \sqrt{c^2 + 4}}{2}$ at $c = 2$.

Thus, we obtain that $\lambda = \dfrac{2 \pm \sqrt{2^2 + 4}}{2} = \dfrac{2 + \sqrt{8}}{2}$ or $\dfrac{2 - \sqrt{8}}{2}$. Since $\sqrt{8} \equiv 5 \pmod{17}$, we have that $\lambda = 7, 12$. Thus, the fixed points are $7, 12$.

We can check this by substituting these points back into either $f(x)$ or $g(x)$. Observe that $g(7) = 15/7 = 15 \cdot 5 = 7$, $g(12) = 25/12 = 8/12 = 2/3 = 2 \cdot 6 = 12$. For the rest of the points, we need to look at when M^n is the identity:

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 12 & 5 \\ 5 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 12 & 12 \\ 12 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^8 = \begin{bmatrix} 16 & 0 \\ 0 & 16 \end{bmatrix}$$

We have reached the identity since we are working in $PGL_2(\mathbb{F}_p)$, so any scalar multiple of the identity matrix is the identity in this space.

Thus, the function $f(x) = x^{15} + 2$ over $\mathbb{F}_{17}$ has two fixed points $7, 12$ and two remaining cycles of lengths $8, 7$.

References

[Sil07] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. ↑

[JHS12] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, 4th ed., Pearson, New Jersey, 2012. ↑

[Che16] Annie S. and Gassert Chen T. Alden and Stange, *Index Divisibility in Dynamical Sequences and Cyclic Orbits Modulo p* (2016). ↑