5-14-2019

Finite Field Dynamics: Exploring Isomorphic Graphs and Cycles of Length p

Catlain McCarthy
Bridgewater State University

Finite Field Dynamics: Exploring Isomorphic Graphs and Cycles of Length p

Catlain McCarthy

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

Bridgewater State University

May 14, 2019

Dr. Jacqueline Anderson, Thesis Advisor
Dr. Irina Seceleanu, Committee Member
Dr. Uma Shama, Committee Member

FINITE FIELD DYNAMICS: EXPLORING ISOMORPHIC GRAPHS AND CYCLES OF LENGTH P

CATLAIN MCCARTHY

Abstract. For this project, we explore finite field dynamics and the various patterns of cycles of elements that emerge from the manipulation of a function and field. Given a function $f : \mathbb{F}_p \longrightarrow \mathbb{F}_p$, we can create a directed graph with an edge from c to $f(c)$ for all $c \in \mathbb{F}_p$. We specifically consider polynomials of the form $f(x) = x^d + c$ and investigate how varying the values of d and c affect the cycles in a given finite field, $\mathbb{F}_p$. We analyze data to look for graphs that result in cycles of length p. We also identify functions whose graphs have the same structure. We prove three main theorems. The first theorem states that for p prime, if $d_1 d_2 \equiv 1 (\text{mod } p-1)$, then the functions $f_1(x) = x^{d_1} + c$ and $f_2(x) = x^{d_2} - c$ have isomorphic graphs for any $c \in \mathbb{Z}_p$. The second theorem states that if $p \equiv 3 \pmod 4$ and $p+1 = 2^k$ then there are exactly $\frac{p+1}{2}$ choices for c in which the graph of $f(x) = x^{p-2} + c$ has one cycle of length p. The third theorem states that for $c \in \mathbb{Z}_p$ if $d = p-2$ and $p+1 = 4q$ where q is a prime, then there are $\frac{p-3}{2}$ choices for c in which the graph of $f(x) = x^d + c$ has one cycle of length p.

1. Background

Dynamical systems have many applications ranging from understanding the spread of disease, the weather, and studying population growth. They play a crucial role in modeling systems which have predictable and repeatable data, as they enable us to understand the behavior of the system. While dynamical systems have many important applications, in my thesis I will study the theoretical aspects of this field through the lens of pure mathematics. In particular, I will focus on the area of dynamics over finite fields which is a topic of current research interest by mathematicians who study arithmetic dynamics. Among the benefits to researching and studying dynamics in a finite setting is that the results about cycle lengths

Date: May 7, 2019.

for a finite dynamical system can allow us to draw various conclusions, such as possible periods, in more complicated and infinite dynamical systems.

Finite field dynamics is a relatively new branch of mathematics that was developed in the 1990s and fits within the broader area of arithmetic dynamics. Going back to the 1920s, the foundation to to the field of complex dynamics was established by Fatou and Julia. These two mathematicians studied the behavior of complex numbers under the repeated iteration of simple polynomials. It is their work that inspired arithmetic dynamicists to attempt to answer some of these same questions in a new setting. Within the field of arithmetic dynamics, mathematicians study similar types of questions, not over the field of complex numbers, but over other sets such as finite field or the field of rational numbers. While this represented the starting point of the field of arithmetic dynamics, since the 1990s mathematicians have taken this branch into different directions, and today we encounter numerous research topics in this broad area of study.

2. Introduction

In my thesis, I will address two major questions that relate to the graphs of finite fields and iterations of polynomials of the form $x^d + c$ over the field $\mathbb{F}_p$, where p is a prime number. In particular, we will study how varying the values of d, c, and p influence the outcome of the dynamical systems in two different ways. First, we will determine the conditions on our function will result in a cycle of length p. Our second question will focus on directed graphs of these graphs and determine when those directed graphs are isomorphic. This thesis builds on the work of another Honors undergraduate research student. From the previous research, we have several results that can help us answer our two questions. We can form a directed graph for $f : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ where $f(x) = x^d + c$ by creating edge from c to $f(c)$ for every $c \in \mathbb{F}_p$. We know that if a bijection exists, then the directed graph of the function will consist entirely of cycles. This implies then that all of the points of the function are periodic. We can also describe when an even or odd number of cycles will occur and therefore, we know some conditions under which there will not be one cycle of length p.

We will first define important definitions in section 3 that will be important to know and understand. Section 4 will cover basic examples of the dynamical systems that we will be working with and section 5 will consist of our three main theorems regarding cycle lengths and isomorphic graphs as well as the various theorems and additional definitions in support of our results.

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 elements as $\mathbb{F}_p$, where p is a prime.

Definition 3.3. A *dynamical system* is a set S and a function $f : S \to S$.

Definition 3.4. A point $s \in \mathbb{F}_p$ under the map of f is called a *fixed point* if $f(s) = s$.

Definition 3.5. We represent the behavior of the dynamical system with a *directed graph* that consists of points and arrows. The points represent the elements of $\mathbb{F}_p$ and the arrows represent where each number is being mapped to by f.

Definition 3.6. A function is a *bijection* if the function is both one-to-one and onto.

Definition 3.7. 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*.

Theorem 3.8. *Let p be an odd prime. Then there are exactly* $\frac{p-1}{2}$ *quadratic residues mod p and exactly* $\frac{p-1}{2}$ *non residues mod p.*

Definition 3.9. 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 3.10. 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 3.11. We refer to two non-isomorphic graphs as *distinct graphs*, meaning they do not have the same cycle structure.

Theorem 3.12. *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* $GCD(p-1, d) = 1$.

Theorem 3.13. *(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 3.14. *(A. Chen, A. Gassert, K. Stange) Let* $f(x) = x^d + c$ *over* $\mathbb{F}_p$. *If* $p \equiv 1$ *(mod 4) and* $d \equiv 3$ *(mod 4), then the dynamical system consists of an even number of cycles. Otherwise, there is an odd number of cycles.* [CGS16]

Definition 3.15. If $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ is a rational map and $f \in \mathrm{PGL}_2(\mathbb{C})$, the linear conjugate of ϕ by f is the map

$$\phi^f = f^{-1} \circ \phi \circ f.$$

Linear conjugation corresponds to a change of variables on $\mathbb{P}^1$. Two rational maps ϕ and ψ are linear conjugate if $\psi = \phi^f$ for some $f \in \mathrm{PGL}_2(\mathbb{C})$ and will have isomorphic graphs.

Theorem 3.16. *(C. Marcotte) If $d = p - 2$ 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. [Mar18]

4. Examples

Example 4.1. We will first give an example of a simple dynamical system over $\mathbb{F}_{11}$. Let $f(x) = x^7 + 3$. In order to understand what the mapping for this function will look like, we first pick any value in $\mathbb{F}_{11}$ and iterate it under the action of f. Since we are working in $\mathbb{F}_{11}$, the arithmetic will be performed mod 11.

Since we can pick any value in F_{11}, let us first start with 0.

$$f(0) = 0^7 + 3 = 3$$

$$f(3) = 3^7 + 3 = 2187 + 3 \equiv 1 \pmod{11}$$

$$f(1) = 1^7 + 3 = 4$$

$$f(4) = 4^7 + 3 = 16384 + 3 \equiv 8 \pmod{11}$$

$$f(8) = 8^7 + 3 = 2097152 + 3 \equiv 5 \pmod{11}$$

$$f(5) = 5^7 + 3 = 78125 + 3 \equiv 6 \pmod{11}$$

$$f(6) = 6^7 + 3 = 279936 + 3 \equiv 0 \pmod{11}$$

These values iterated through our function produce a cycle of length 7. To determine the rest of this dynamical system, we chose another point in $\mathbb{F}_{11}$ outside the seven-cycle.

$$f(2) = 2^7 + 3 = 128 + 3 \equiv 10 \pmod{11}$$

$$f(10) = 10^7 + 3 = 10000000 + 3 \equiv 2 \pmod{11}$$

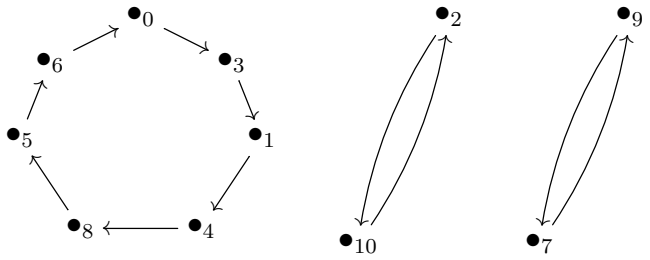


FIGURE 1. $f(x) = x^7 + 3$ over $\mathbb{F}_{11}$

We can see then that 2 and 10 form a two-cycle. We now test the remaining points 7 and 9.

$$f(7) = 7^7 + 3 = 823543 + 3 \equiv 9 \pmod{11}$$

$$f(9) = 9^7 + 3 = 4782969 + 3 \equiv 7 \pmod{11}$$

It is clear that 7 and 9 also result in a two-cycle. From these computations, we get the the directed graph in Figure 1

We also want to consider an example where our function f results in one cycle of length p.

Example 4.2. Let $f(x) = x^5 + 1$ over $\mathbb{F}_7$. We can repeat the iteration process used in Example 4.1 to determine what our directed graph will look like.

Starting with 0, we have

$$f(0) = 0^5 + 1 = 1$$

$$f(1) = 1^5 + 1 = 2$$

$$f(2) = 2^5 + 1 = 32 + 1 \equiv 5 \pmod{7}$$

$$f(5) = 5^5 + 1 = 3125 + 1 \equiv 4 \pmod{7}$$

$$f(4) = 4^5 + 1 = 1024 + 1 \equiv 3 \pmod{7}$$

$$f(3) = 3^5 + 1 = 243 + 1 \equiv 6 \pmod{7}$$

$$f(6) = 6^5 + 1 = 7776 + 1 \equiv 0 \pmod{7}$$

We can see in Figure 2 what this seven-cycle looks like.

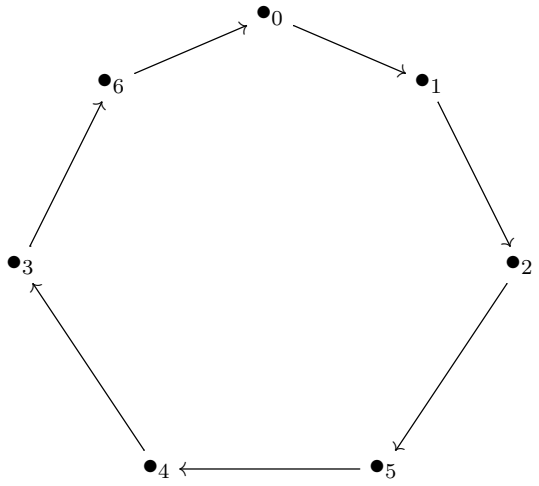


FIGURE 2. Cycle of length 7 for $f(x) = x^5 + 1$ over $\mathbb{F}_7$

5. Main Results

The main goal of this project is to determine when we have a cycle of length p. We gathered data in the form of directed graphs for different functions $f(x) = x^d + c$ over $\mathbb{F}_p$ for different values of c, d, and p. In the process of trying to determine patterns for cycle lengths, a pattern also emerged regarding isomorphic graphs.

5.1. **Isomorphic Graphs.** By Definition 3.10, two graphs are isomorphic if they have the same number of vertices and have edges connecting these vertices in the same way. Isomorphic graphs will have the same number of edges, cycles, and cycle structures.

We found patterns where directed graphs of functions would have the same structure for different d and c values.

In Table 1, we can see that we have pairs of d_1-values and d_2-values where $f(x) = x^{d_1} + c$ and $g(x) = x^{d_2} - c$ result in isomorphic directed graphs. One such instance where two different functions result in the same graph is when you consider $f(x)$ and its inverse $f^{-1}(x)$.

Lemma 5.1. *If f is a bijection, $f(x)$ and $f^{-1}(x)$ have isomorphic graphs.*

TABLE 1. Isomorphic Graphs for $p = 23$

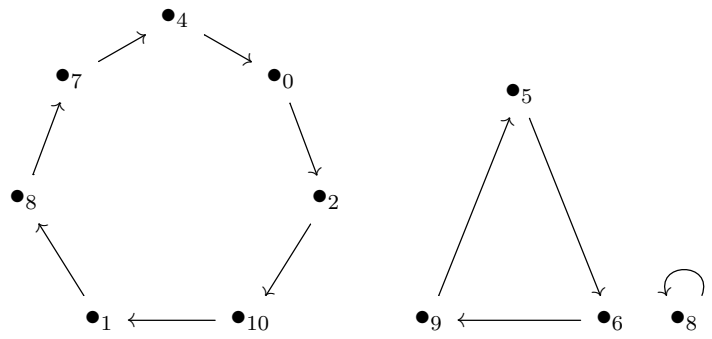
d_1	d_2	Isomorphism classes of graphs by c-value for $f_1(x) = x^{d_1} + c$ and $f_2(x) = x^{d_2} - c$
3	15	$\{\pm1\}, \{\pm2\}, \{\pm3\}, \{\pm4\}, \{\pm5\}, \{\pm6\}, \{\pm7\}, \{\pm8\}, \{\pm9\}, \{\pm10\}, \{\pm11\}$
5	9	$\{\pm1\}, \{\pm2\}, \{\pm3\}, \{\pm4\}, \{\pm5\}, \{\pm6\}, \{\pm7\}, \{\pm8\}, \{\pm9\}, \{\pm10\}, \{\pm11\}$
7	19	$\{\pm1\}, \{\pm2, \pm5\}, \{\pm3\}, \{\pm4\}, \{\pm6, \pm9\}, \{\pm7\}, \{\pm8\}, \{\pm10\}, \{\pm11\}$
13	17	$\{\pm1\}, \{\pm2\}, \{\pm3\}, \{\pm4\}, \{\pm5\}, \{\pm6\}, \{\pm7\}, \{\pm8\}, \{\pm9\}, \{\pm10\}, \{\pm11\}$

A function and its inverse share the same structure, but the inverse function will simply map values in the opposite direction. Using this Lemma and our observations regarding d-values and c-values producing the same graphs, we were able develop the following theorem.

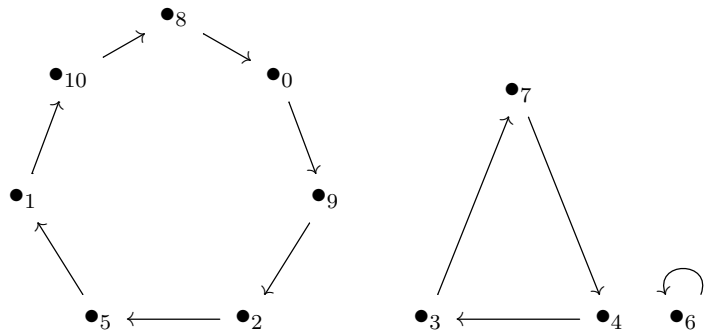
Theorem 5.2. Let p be prime. If $d_1 d_2 \equiv 1 (\text{mod } p-1)$, then the functions $f_1(x) = x^{d_1} + c$ and $f_2(x) = x^{d_2} - c$ have isomorphic graphs for any $c \in \mathbb{Z}_p$.

Example 5.3. To provide an example that shows that this theorem holds true, we consider the two functions $f_1(x) = x^3 + 2$ and $f_2(x) = x^7 + 9$ over $\mathbb{F}_{11}$. The d values for these functions are $d_1 = 3$ and $d_2 = 7$. If we consider $d_1 d_2$, then we get $3(7) = 21 \equiv 1 \pmod{10}$. We can also see that our c values, 2 and 9, are additive inverses of each other in $\mathbb{F}_{11}$ and so the graphs of $f_{1(}x) = x^3 + 2$ and $f_{2(}x) = x^7 + 9$ are isomorphic.

$f_1(x) = x^3 + 2$ over $\mathbb{F}_{11}$



$f_2(x) = x^7 + 9$ over $\mathbb{F}_{11}$



In order to prove that f_1 and f_2 are isomorphic when $d_1 d_2 \equiv 1 \pmod{p-1}$, we will make use of conjugates. As Definition 3.15 states, linear conjugation will result in a change in variables on $\mathbb{P}^1$. If we have $f^\phi = \phi^{-1} \circ f \circ \phi$ and we consider $(f^\phi(x))^n = (\phi^{-1} \circ f \circ \phi)((\phi^{-1} \circ f \circ \phi)(\phi^{-1} \circ f \circ \phi)...$, then this function will simplify to $(\phi^{-1} \circ f^n \circ \phi(x))$. This matters to us because functions being conjugates of each other will simply mean that their directed graphs will have the same structure with values of the map just shifted. The actual structure of the graph will not change.

Proof of Theorem 5.2. Let p be prime and $d_1 d_2 \equiv 1 \pmod{p-1}$. Let $f_1(x) = (t \circ g)(x) = x^{d_1} + c$, where $g(x) = x^{d_1}$ and $t(x) = x + c$. We can say that x^{d_2} is the inverse of x^{d_1} because $(x^{d_1})^{d_2} = (x^{d_2})^{d_1} = x$ since $d_1 d_2 \equiv 1 (\text{mod } p-1)$ by Theorem 3.13. This means then, that $f_1^{-1}(x) = (g^{-1} \circ T^{-1})(x) = (x-c)^{d_2}$. Let $f_2(x) = (T^{-1} \circ g^{-1})(x) = (g \circ T)^{-1}(x) = x^{d_2} - c$. In order to show that f_1 and f_2 have isomorphic graphs, we need to use the fact that $f_1(x)$ and $f_1^{-1}(x)$ have isomorphic graphs, as stated in Lemma 1, and we need to show that ${f_1}^{-1}$ and f_2 are conjugates. That is, we need to show that:

$$f_2 = T^{-1} \circ f_1^{-1} \circ T$$

where $T(x) = x + c$ and $T^{-1}(x) = x - c$.

Let us consider:

$$\begin{aligned} & T^{-1} \circ f_1^{-1} \circ T \\ &= T^{-1}(f_1^{-1}(T(x))) \\ &= T^{-1}(f_1^{-1}(x + c)) \end{aligned}$$

$$= T^{-1}(x^{d_2})$$
$$= x^{d_2} - c$$
$$= f_2(x)$$

This function is equivalent to our function f_2 and so we have shown that the functions ${f_1}^{-1}$ and f_2 are conjugates and therefore have isomorphic graphs. Therefore by transitivity, f_1 and f_2 have isomorphic graphs. □

Lemma 5.4. *If d is odd, then $f(x) = x^d + c$ and $g(x) = x^d - c$ have isomorphic graphs.*

Proof. Let us consider $g(-x)$. Since d is odd, we will have the following:

$$g(-x) = (-x)^d - c$$
$$= -x^d - c$$
$$= -(x^d + c)$$
$$= -f(x)$$

This then implies that $f(x) = -g(-x)$ which implies that they are conjugates where $\phi(x) = -x$ and so $f(x) = \phi^{-1} \circ g \circ \phi$

Therefore, $f(x)$ and $g(x)$ have isomorphic graphs. □

Corollary 5.5. *As followed from Theorem 5.2 and Lemma 5.4, the graphs of the functions $x^{d_1} + c$, $x^{d_1} - c$, $x^{d_2} + c$, and $x^{d_2} - c$ all have isomorphic graphs .*

5.2. **Cycles of Length *p*.** We also made progress in determining classes of functions that will result in one cycle of length p. In gathering data, we determined which d and c values for a given p value would result in a cycle of length p.

In examining Table 2, we can see that when $d = p - 2$, our functions have a large number of c values that result in a p-cycle. This pattern persisted as p values increased. However, this was not true for all p. Since Theorem 3.14 states that when $p \equiv 1 \pmod 4$ and $d \equiv 3 \pmod 3$, then the graph of function $f(x) = x^d + c$ will have an even number of cycles, we get the following lemma.

TABLE 2. Number of p-cycles

p-value	d-value	Number of c-values that result in a p-cycle
23	21	8
29	25	4
31	29	16
37	17	8
43	41	20

Lemma 5.6. *Let p be prime and let $d = p - 2$. We can find c-values such that $f(x) = x^d + c$ will produce directed graphs that have a cycle of length p.*

By Fermat's Little Theorem, we know that $x^{p-1} \equiv 1$. However, since we are considering cases where $d = p - 2$, we can use this theorem to represent x^{p-2} as x^{-1}. Therefore, we will consider cases where our functions are of the form $x^{p-2} + c$ or $x^{-1} + c = \frac{1}{x} + \frac{cx}{x} = \frac{cx+1}{x}$, where $x \neq 0$.

With this equivalent form of our function with $d = p - 1$, we can also think about including ∞ so that we don't need to exclude $x = 0$. Let us consider $\mathbb{P}^1(\mathbb{F}_p) = \{0, 1, ..., p-1, \infty\}$. With this new field, we are now looking for a cycle of length $p + 1$. The only difference between the graph of $x^{p-2} + c$ over $\mathbb{F}_p$ and our equivalent function $\frac{cx+1}{x}$ over $\mathbb{P}^1(\mathbb{F}_p)$ is that the graph of $\frac{cx+1}{x}$ will have ∞ in between 0 and c in the cycle that contains 0.

If $p \equiv 3 \pmod 4$ and $d = p - 2$, then we know we will have a bijection with an odd number of cycles as stated by Theorem 3.14. We also know by Theorem 3.16 that all cycles of length greater than one will all be the same in length. As a consequence, if we can show that there are no fixed points that exist, then we know that $p + 1 = NL$, where L represents the length of one cycle and N represents the number of cycles.

Lemma 5.7. *We can represent $p + 1$ as $p + 1 = LN$ where L represents the length of one cycle and N represents the (odd) number of cycles. By Theorem 3.14, we know N will be odd because $p \equiv 3 \pmod 4$ and $d \equiv 1 \pmod 4$.*

Lemma 5.8. *For $p \equiv 3 \pmod 4$ and $p+1 = 4q$ where q is prime, a four-cycle will map $0 \longmapsto \infty$, $\infty \longmapsto c$, $c \longmapsto \frac{c^2+1}{c}$, $\frac{c^2+1}{c} \longmapsto 0$. So $f^2(c) = 0$.*

Lemma 5.9. *$f^2(c) = 0$ if $c^2 = -2$.*

Proof. As previously stated, we can represent our function $f(x) = x^{-1} + c$ equivalently as $f(x) = \frac{cx+1}{x}$. We can represent this function as $f(x) = \begin{bmatrix} c & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix}$. Using this, we can solve for c by solving:
$\begin{bmatrix} c & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} c \\ 1 \end{bmatrix} = 0 \longrightarrow \begin{bmatrix} c^2+1 & c \\ c & 1 \end{bmatrix} \begin{bmatrix} c \\ 1 \end{bmatrix} = \begin{bmatrix} c^3+2c \\ c^2+1 \end{bmatrix} = 0$. We know then that $c^3 + 2c = 0 \longrightarrow c(c^2+2) = 0$ and therefore $c^2 = -2$. □

With the knowledge that we are seeking to find when we get a directed graph of length p, we know that the graph produced by our function can't have fixed points. As previously stated by Theorem 3.16, we know that we will only get fixed points if $c^2 + 4$ is 0 or produces a quadratic residue. If we know that $c^2 + 4$ is a quadratic residue, then we know that there will be exactly two fixed points. If $c^2 + 4 = 0$, then $f(x)$ will have exactly one fixed point. By determining all $(c^2 + 4)$ values for a given p that are not quadratic residues or equal to 0, we are able to find all c values that can potentially result in a p-cycle.

Lemma 5.10. *Let $p \equiv 3 \pmod 4$ and let $f(x) = x^{p-2} + c$. Then there will be exactly $\frac{p-1}{2}$ choices for $c \in \mathbb{F}_p$ such that $f(x)$ has fixed points.*

Proof. We first will determine the number of c-values where our graph has fixed points. We will use the fact that $\left(\frac{c^2+4}{p}\right) = 1$ as stated by Theorem 3.16. For $f(x) = x^{p-2} + c$, there will be fixed points as long as the property $c^2 + 4 \equiv y^2$ holds for some $y \in \mathbb{F}_p$. Let $c^2 + 4 \equiv y^2 \pmod p$. Then we know that $4 \equiv y^2 - c^2 \equiv (y + c)(y - c)$. Let $m = y + c$. Then we know that $\frac{4}{m} = y - c$. Let us consider $m - \frac{4}{m} = (y + c) - (y - c) = 2c$ which would then imply that $c = \frac{m-\frac{4}{m}}{2} = \frac{m^2-4}{2m}$. We know that m can be anything except for 0 and so there are $p - 1$ choices for m. However, if we consider our equation for c, we can see that every c-value is a

result of 2 different m-values.

Let us suppose that 2 m-values produce the same c-value. Then we have:

$$\frac{m_1^2-4}{2m_1} = \frac{m_2^2-4}{2m_2}$$
$$2m_2m_1^2 - 8m_2 = 2m_1m_2^2 - 8m_1$$
$$0 = m_1m_2^2 + (4 - m_1^2)m_2 - 4m_1$$
$$0 = (m_2 - m_1)(m_1m_2 + 4)$$

As a result, we have that $m_1 = m_2$ or $m_1m_2 = -4$ which implies that $m_2 = \frac{-4}{m_1}$. This means, then, that m_1 and $\frac{-4}{m_1}$ result in the same c-value. Therefore, there are $\frac{p-1}{2}$ choices for c since there are 2 m's for each c-value and there are $p-1$ choices for m. It is important to note that we know that m_1 and $\frac{-4}{m_1}$ can never be the same value because that then would meant that $-4 = m_1^2$ and $(\frac{-4}{p}) = -1$ because $p \equiv 3 \pmod 4$. There will be $\frac{p-1}{2}$ c-values that will correspond to functions which have maps with fixed points and as a consequence $\frac{p+1}{2}$ c-values will correspond to functions which will have maps with no fixed points. □

Theorem 5.11. *If $p \equiv 3$ (mod 4) and $p + 1 = 2^k$ then there are exactly $\frac{p+1}{2}$ choices for c in which the graph of $f(x) = x^{p-2} + c$ has one cycle of length p.*

Proof. Let $p + 1 = 2^k$. By Lemma 5.7, we know that N must be odd. We also know by Theorem 3.16 that we will only get fixed points if $c^2 + 4 = 0$ or produces a quadratic residue. Knowing that $p + 1 = NL = 2^k$, we can conclude then that, as long as there are no fixed points, we will always get a cycle of length $p + 1$ because the only odd factor of of 2^k is 1, so $N = 1$ and $L = p + 1$. □

Example 5.12. Let us consider an example illustrating this theorem. Let us consider $\mathbb{F}_{31}$. Then $p = 31 \equiv 3 \pmod 4$ and $p + 1 = 32 = 2^5$ where $k = 5$. We know then that as long as there are no fixed points, a function where $d = p - 2$ will result in a directed graph with 1 cycle of length p. For $p = 31$, the c-values that do not result in fixed points (meaning c-values for which $c^2 + 4$ is not a quadratic residues or 0) are:

3, 5, 7, 8, 9, 10, 12, 15, 16, 19, 21, 22, 23, 24, 26, 28

Since none of these c-values produce fixed points, then we know that all of these c-values result in a graph with 1 cycle of length p.

We can also consider the case where $p+1 = 4q$, where q is prime. With this particular case, we have the potential to have 1 cycle of length $p+1$ or q cycles of length 4, as implied by Lemma 5.7.

Theorem 5.13. *Let $c \in \mathbb{Z}_p$ and $p \equiv 3$ (mod 4) and $p+1 = 4q$ where q is a prime. Then there are $\frac{p-3}{2}$ choices for c in which the graph of $f(x) = x^{p-2} + c$ has one cycle of length p.*

Proof of Theorem 5.13. We now consider the case where p is a prime where $p \equiv 3 \pmod 4$ and $p+1 = 4q$ where q is a prime number. If there are no fixed points, by Lemma 5.7, we know that we will have a directed graph of either one cycle of length $p+1$ or q cycles of length 4. We also know by Lemma 5.8, what a four cycle will look like. Finally, Lemma 5.9, tells us that

$$f^2(c) = 0 \longrightarrow c^2 = -2$$

If -2 is a square mod p, then we know that there are two c-values such that $c^2 = -2$ and that these c-values don't result in one cycle of length $p+1$ (since they are a part of the four-cycle). We can verify this. We know that $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$. Since p is $p \equiv 3 \pmod 4$, then we know that $(\frac{-1}{p}) = -1$ and so $(\frac{-1}{p})(\frac{2}{p}) = -(\frac{2}{p})$. We can determine the value of $-(\frac{2}{p})$ with the following:

$$-(\frac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

since

$$(\frac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

If $(\frac{-2}{p}) = 1$, then there exists c_1 and c_2 such that $(c_1)^2 = -2$ and $(c_2)^2 = -2$. This then means that c_1 and c_2 will not result in a $p+1$ cycle and would no longer be part of the

list of c-values that have the potential to produce p-cycles. In particular, we are only considering when $p+1 = 4q$. If $p \neq 7$, then $p = 3 \pmod 8$ since q is an odd number and so $4q = 4 \pmod 8$. As a result, we will have two c values for which our graph consists of q 4-cycles.

We have shown that there are $\frac{p+1}{2}$ c-values that result in no fixed points and therefore will produce either a cycle of length p or q cycles of length 4. Then we know that there are $\frac{p-3}{2}$ c-values that will produce a p-cycle.

□

Example 5.14. Let us consider our third theorem by considering the following example
Let us consider $\mathbb{F}_{67}$. Then we have $p = 67 \equiv 3 \pmod 4$ and $p + 1 = 4(17)$, where $q = 17$. From this, we know that for a function where $d = p - 2$, that there is the potential to have 1 cycle of length 68 or 17 cycles of length 4 (if there are no fixed points).
We were able to determine that the list of possible c-values that do not produce fixed points (meaning that $c^2 + 4$ is not a quadratic residue or 0) are:
1, 2, 3, 4, 7, 9, 11, 14, 15, 19, 20, 21, 24, 27, 28, 29, 31, 26, 28, 39, 40, 43, 46, 47, 48, 52, 53, 56, 58, 60, 63, 64, 65, 66
Since we know that the four cycle maps $0 \longmapsto \infty$ and $\infty \longmapsto c$, we know that $f^2(c) = 0$. By verifying then that $(\frac{-2}{67}) = 1$, we know then that that there are two c-values that will produce a four-cycle.
Since $67 \equiv 3 \pmod 8$, then we know that $(\frac{-2}{67}) = 1$ and that -2 is a square. So there are two c-values, 20 and 47, such that $c^2 = -2$. These c-values will produce a graph consisting of four-cycles and so we are left with $\frac{p-3}{2} = 32$ c-values that will result in a cycle of length p.

References

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

[Sil12] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, 4th ed., Pearson, New Jersey, 2012. ↑

[CGS16] Annie S. Chen, T. Alden Gassert, and Katherine E. Stange, *Index Divisibility in Dynamical Sequences and Cyclic Orbits Modulo p* (2016). ↑4

[Mar18] Christine Marcotte, *Exploring Dynamical Systems: Number of Cycle and Cycle Lengths* (2018). ↑5