LETTERS IN BIOMATHEMATICS
An International Journal

RESEARCH ARTICLE

OPEN ACCESS

Quadratic Dynamics on Finite Fields and GAP

Yaulema Castañeda Jorge Luis[1], Héctor Méndez-Gómez[2], Velasteguí López Efraín[3]

[1]Escuela Superior Politécnica de Chimborazo Ecuador; [2]Universidad de Costa Rica, Sede del Pacífico Costa Rica; [3]Universidad Bolivariana del Ecuador

ABSTRACT

This study examines the dynamics of quadratic functions over finite fields Fq, where q = p^n, p is an odd prime, and n is a positive integer, within a theoretical, analytical, and non-experimental framework. The analysis integrates concepts from number theory, group theory, and graph theory to characterize the iterative behavior of quadratic functions of the form phi_c(x) = x^2 + c, where c is an element of Fq. Initially, the dynamics of the mapping phi(x) = x^2 over the finite field Fp are analyzed to establish fundamental structural properties. The study focuses on functional graphs in which vertices represent elements of the finite field and directed edges correspond to successive iterations of the function. Key concepts, including orbits, periodic and preperiodic points, cycle lengths, and tail lengths, are formally described and examined. The results indicate that the structure of these functional graphs is strongly influenced by the arithmetic properties of the multiplicative group of nonzero elements of Fp, particularly the factorization of p - 1, which determines the distribution and lengths of cycles and associated tails for the squaring map. The functional graphs exhibit cycles with attached inverse trees, reflecting the quadratic nature of the mappings and the algebraic structure of finite fields. Computational validation using GAP supports the theoretical findings, while an illustrative example over the finite field with nine elements (F9) demonstrates the applicability of the analytical framework. Overall, the study provides a systematic mathematical characterization of quadratic dynamical systems over finite fields and contributes to understanding the relationship between algebraic structures, iterative mappings, and functional graph configurations.

ARTICLE HISTORY
Received April 8, 2026
Accepted May 27, 2026

KEYWORDS
Quadratic Dynamics,
Finite Fields,
Functional Graphs,
Multiplicative Order,
Discrete Dynamical Systems

1. Introduction

The field of dynamical systems has gained significant relevance in the analysis of discrete phenomena, particularly when these phenomena are approached from an algebraic perspective. In this context, the arithmetic theory of dynamical systems makes it possible to observe the iterative behavior of functions defined over finite algebraic structures, incorporating tools from graph theory, number theory, abstract algebra, and group theory (Bondy & Murty, 2008; Ireland & Rosen, 1990; Jacobson, 2009; Lang, 2002; Peinado et al., 2001; Rotman, 1995; Silverman, 2007). This type of approach is especially useful in the case of polynomial applications defined over finite fields, as these structures provide a controlled and well-defined framework for mathematical analysis (Jacobson, 2009; Lang, 2002).

Finite fields Fq, where $q = pn$, with p being a prime number and n a positive integer, constitute a fundamental basis in various areas of mathematics and its applications, such as cryptography and coding theory (Ireland & Rosen, 1990; Lang, 2002). The algebraic structure of these fields allows for the analysis of properties such as quadratic residues, multiplicative orders, and primitive roots, which are of central importance in the study of iterative functions (Ireland & Rosen, 1990). Quadratic functions of the form $\varphi c(x) = x2 + c$, where $c \in Fq$, have been extensively studied due to the complexity and richness of their dynamical patterns.

Within the context of discrete dynamical systems, it is observed that the iteration of functions over finite sets leads to the definition of characteristic concepts such as orbits, periodic points, and preperiodic points. All these entities can be represented through graph theory by means of directed functional graphs, where vertices correspond to elements of the set and edges represent the application of the iterated function. Consequently, graph theory provides an appropriate conceptual framework for describing and studying these entities, as it enables the characterization of connectivity, cycles, and tree-like structures derived from the system's dynamics (Bondy & Murty, 2008).

In the case of the function $\varphi(x) = x^2$ over the finite field Fp, it has been demonstrated that the structure of the functional graphs associated with such functions is closely related to arithmetic properties of the multiplicative group $Fp*$,

CONTACT Yaulema Castañeda Jorge Luis: jorge.yaulema@espoch.edu.ec

particularly the order of its elements and their prime factorization (Rotman, 1995). Previous results have shown that the lengths of tails and cycles can be determined through valuation functions and multiplicative orders, allowing for an exact description of the iterative dynamics (Vasiga & Shallit, 2004).

Similarly, recent studies have produced essential results concerning the iteration of quadratic functions over finite fields, through which formulas have been established to describe the computation of the number of cycles, their lengths, and the distribution of elements within functional graphs (Vasiga & Shallit, 2004). Alternatively, the maximal periods of quadratic functions in Fq have also been investigated, which are of particular interest in cryptographic and computational applications (Peinado et al., 2001).

This framework leads to the study of the dynamics of quadratic functions over finite fields, detailing (first) the description of their functional graphs and (second) the typical structure of cycles and preimages. The objective is to integrate theoretical results from different areas of fundamental mathematics to provide a formal and concise description of the iterative behavior of these functions, and to contribute to strengthening the algebraic approach in discrete dynamical systems (Chatterjee & Chakraborty, 2023).

2. Materials and Methods

The present research was conducted within a theoretical–analytical framework, of a non-experimental nature, aimed at studying the dynamics of quadratic functions over finite fields. The methodological design is based on the integration of methods from abstract algebra, number theory, and graph theory, with the objective of providing a characterization of the iterative behavior of quadratic functions through finite structures.

Initially, a systematic review of the specialized literature on algebraic dynamical systems, finite fields, and iterative applications was carried out, including both classical texts and contemporary works in algebraic theory and discrete dynamics (Bondy & Murty, 2008; Ireland & Rosen, 1990; Jacobson, 2009; Lang, 2002; Peinado et al., 2001; Rotman, 1995; Silverman, 2007). This review provided the required conceptual framework, which includes formal definitions of finite fields, multiplicative orders, quadratic residues, functional graphs, and discrete dynamical systems.

Subsequently, the mathematical formalization of the problem was undertaken by defining the quadratic functions under study as $\varphi c(x)=x2+c$ over the finite field Fq, where $q = pn$ and $p > 2$. Within this formulation, structural properties such as orbits, periodic points, preperiodic points, cycle lengths, and tail lengths were introduced, making use of existing theoretical results from the relevant literature, particularly those concerning the decomposition of multiplicative order and valuation functions (Ireland & Rosen, 1990; Rotman, 1995; Vasiga & Shallit, 2004).

In the third phase, a structural analysis of the functional graphs associated with the iterative functions was conducted. The dynamics were modeled using directed graphs in which the elements of the finite field represent vertices, and edges connect vertices through the application of the function under consideration. This analysis enabled the identification of structural patterns such as cycles, inverse binary trees, and distributions of preimages, based on principles from graph theory (Bondy & Murty, 2008).

In a fourth phase, a computational approach was employed through the implementation of the GAP system (Groups, Algorithms, and Programming) as a means of validating theoretical results, performing calculations on iterations, cycle lengths, and tail lengths, as well as implementing algorithms to simulate the dynamics of quadratic functions. This allowed for the empirical verification of the results obtained across different finite fields.

Finally, in a phase of comparative analysis and interpretation of results, theoretical findings were contrasted with computational results, enabling a comprehensive characterization of the dynamics of quadratic functions through the identification of structural regularities, validation of existing theorems, and interpretation of the results in terms of their mathematical significance, as well as their potential applicability in areas such as cryptography and computational analysis (Peinado et al., 2001; Vasiga & Shallit, 2004).

The methodology employed allowed the research problem to be addressed from a rigorous and multidisciplinary perspective, ensuring coherence between theoretical development, structural analysis, and computational validation of the results.

3. Results

3.1 Preliminaries

This first section will establish the notation, definitions, and important theorems that will assist us throughout the present work. We will introduce concepts from finite field theory and mention significant results from Group Theory, Number Theory, and Graph Theory. Finally, we will outline the basic concepts of the dynamical systems we intend to study. It should be noted that most theorems in this first section will not include a proof, as the results mentioned here are

assumed to be known.

3.1.1 Concepts from Finite Field Theory

Definition 1. Let $(R, +, \cdot)$ be a commutative ring with unity. We say that *R* is a field if for every $x \in R^*$ there exists $x^{-1} \in R$.

Example 2. The sets Q, R, C, and $Z_p = Z/pZ$, with *p* a prime, are well-known examples of fields. We denote the field Z_p by F_p, and we call it the finite field of p elements. It is always possible to construct a field *K* from the maximal ideals, which we define below, of a ring.

Definition 3. Let (*R*, +, ·) be a commutative ring with unity. We say that $I \subseteq R$ is an ideal if
$(I, +)$ is a subgroup of $(R, +)$,

$$if\ r \in R\ and\ x \in I\ then\ rx \in I\ and\ xr \in I.$$

Definition 4. We say that I is a maximal ideal of R if $I/= R$ and the only ideal of R that strictly contains I is R itself.

Theorem 5. *If* I is a maximal ideal of R, the quotient ring R/I is a field. Finite fields can be constructed by virtue of the preceding theorem by following these steps:

1. We consider the commutative ring $Zp[x]$ of polynomials with coefficients in Zp.
2. We take an irreducible polynomial $f(x)$ of degree *n* in $Zp[x]$, which is a factor of the polynomial $xp\ n - 1$ over Z.
3. We consider the ideal $I = \langle f(x)\rangle = \{p(x) \cdot f(x) : p(x) \in Zp[x]\}$. This ideal is maximal because $f(x)$ is an irreducible polynomial.
4. We take the quotient ring $K = Zp[x]/I$.
5. K is a field with p^n elements.

The previous construction scheme establishes the following theorem.

Theorem 6. For any prime p and $n > 0$, there exists a field with $\mathrm{q} = \mathrm{pn}$ elements. Moreover, two fields with $\mathrm{p^n}$ elements are isomorphic.

Theorem 7. If K is a field with q elements, then $\mathrm{q} = \mathrm{pn}$ with p a prime and n a positive integer. In this case, we write $\mathrm{K} = \mathrm{Fq}$. If K is a field of $\mathrm{q} = \mathrm{pn}$ elements, then

$$\underbrace{1 + \cdots + 1}_{p\text{-times}} = 0 \text{ and } \underbrace{m + \cdots + m}_{p\text{-times}} = pm = 0, \forall m \in K.$$

Definition 8. If $q = pn$, we say that Fq is a field of characteristic p. Further details can be found in any text on field theory or Galois theory such as (Jacobson, 2009; Lang, 2002).

3.1.2 Concepts from Group Theory

We will assume that many of the basic concepts of group theory are known, and we will establish some notation for a few important definitions. For more details on group theory, one may consult (Rotman, 1995). For any field *K*, we denote by $U = K^*$ the set of its units (invertible elements), which forms a multiplicative group. In the case where the field is F_q, we write Uq. If p is a prime number, the cardinality or order of the group U_q is given by $|Up| = \varphi(p) = p - 1$, where φ is Euler's φ function.

Definition 9. Let G be a group, and let $m \in N$ be the smallest integer such that $g^m = e$ for $g \in G$, where e is the identity element of the group G. We say that m is the order of g in G, and we write $m = ord_p Gg$. In the case where $x \in U_p$, we denote the order of x in U_p by $ord_p x$.

3.1.3 Concepts from Number Theory

We will mention some results from Number Theory that are considered important throughout the present text. Recall that number theory plays a very important role in various areas of mathematics, such as group theory and field theory; furthermore, applications of this rich branch of mathematics can be seen in cryptography.

Definition 10. Let p be a prime and n a positive integer. We denote by $V_p(n)$ the exponent of the largest power of p that divide n. By convention $V_p(0) = \infty$.

Example 11. If $n = 100$, we see that $n = 22 \cdot 52$, so $v2(100) = 2$ and $v5(100) = 2$. If $n = 84 = 22 \cdot 3 \cdot 7$, then $v2(84) = 2$, $v3(84) = 1$, $v7(84) = 1$ and $v5(84) = 0$.

Definition 12. Given $n \in N$, we say that γ is a primitive root modulo p, if γ generates U_p. That is, for every $\beta \in U_p$. there exists $k \in Z$ such that

$\gamma k \equiv \beta \bmod p.$

Definition 13. We say that *r* is a quadratic residue modulo *n*, if there exists *x* ∈ Z such that

$x2 \equiv r \mod n$.

Otherwise, we say that r is a non-quadratic residue. For Zp, there are a total of $\underline{p+1}$ quadratic residues, including zero, and $\underline{p-1}$ non- quadratic residues, by Euler's criterion. More detailed results on this topic can be found in (Ireland & Rosen, 1990).

3.1.4 Concepts from Graph Theory

Graph Theory has a wide variety of applications in computer science, physics, chemistry, social sciences, engineering, among other areas. For more on the mathematical concepts of graph theory, one may consult (Bondy & Murty, 2008). We will use graphs to describe and understand the dynamics in finite fields. One of the key concepts is the following.

Definition 14. A complete binary tree of height h is a directed graph with 2^i nodes at depth $i, 0 \leq i \leq h$, with the property that every node has exactly two children. We denote it by B_h. The graph B_h contains $2h+1-1$ nodes in total.

Definition 15. If $G = (V, E)$ is a directed graph, we denote by G^R the directed graph (V, E^R), where

$$E\,R = \{(x,y): (y,x) \in E\}$$

G^R is the reverse graph.

3.1.5 Concepts from Dynamical Systems

Dynamical systems describe the long-term behavior of certain phenomena; in biology, for instance, dynamical systems are used to describe the growth of populations of certain species over time. The mathematical theory of dynamical systems has experienced great growth in recent decades, having been developed primarily from an analysis and topology perspective. However, these concepts can also be studied from an algebraic viewpoint. This work aims to apply the basic definitions of dynamics to finite fields. A comprehensive development of the arithmetic theory of dynamical systems, from a purely algebraic approach, can be found in the text (Silverman, 2007).

Definition 16. A dynamical system consists of a set S and a function $\phi: S \to S$ which allows us to perform as many iterations as desired:

$$\phi^n = \underbrace{\phi\, o \ldots o\, \phi}_{n-iterations} = n - th\ iterate\ of\ \phi$$

By convention, ϕ^0 denotes the identity map on S. If $\phi: S \longrightarrow S$ is a (discrete) dynamical system over a set S. We say that y is a successor of x if $y = \phi(x)$; we also say that x is a predecessor of y.

Definition 17. For a point $x \in S$, the orbit of x under ϕ is the set

$$O\phi(x) = O(x) = \{\phi n(x): n \geq 0\}$$

Definition 18. A point α is said to be periodic if $\phi^n(x) = x$ for some $n \geq 1$. The smallest such n is called the period of x. The set of periodic points of ϕ in S is denoted by

$$Per(\phi, S) = \{\alpha \in S : \phi n(x) = x, for\ some\ n \geq 0\}.$$

We also say that x is a fixed point if $\phi(x) = x$; the orbit of a fixed-point x consists of the point x itself.

Definition 19. A point x is said to be preperiodic if some iterate $\phi m(x)$ is periodic. The set of preperiodic points of ϕ in S is denoted by

$$\begin{aligned} Per(\phi, S) &= \{\alpha \in S : \phi m + n(x) = \phi m(x), for\ n \geq 0\ and\ m \geq 0\} \\ &= \{\alpha \in S : O\phi(x)\ is\ finite\} \end{aligned}$$

Definition 20. The functional graph of ϕ is the directed graph $G\phi = (V, E)$ whose vertices are the elements of S and the edges are $(x, \phi(x))$, with $x \in S$. The orbit of $x \in S$ under $\phi, O_\phi(x)$, traces the path in G_ϕ starting at x. The main objective of dynamics is to study the behavior of its orbits, $O_\phi(x)$.

Example 21. If S is a finite set and $\phi: S \longrightarrow S$ is a function, then every point in S is preperiodic. A question that may arise in this case is: What is the number of elements in the set of periodic points? The following definitions are key concepts that will help us understand the dynamics of the quadratic maps over finite fields that we will study later.

Definition 22. When S is finite, for every $x \in S$ there exists a positive integer $s = s(x)$ such that $\phi^s(x) \in \{x, \phi(x), \phi^{s-1}(x)\}$. We call the tail of x the smallest non-negative integer $t = t(x)$ such that $\phi s(x) = \phi t(x)$. We call the cycle length of x the integer $c = s - t$, which satisfies $\phi^t(x) = \phi^{t+c}(x)$. Observe that the set of the tails is given explicitly by

$$\{x, \phi(x), \phi 2(x), \ldots, \phi t - 1(x)\},$$

and the set of cycles is

$$\{\phi t(x), \ldots, \phi t + c - 1(x)\}.$$

The following is an example of a discrete dynamical system over the finite field F_p, where p is a prime number. Example 23. Let $\phi 1 : Fp \longrightarrow Fp, \phi 1(z) = zp \; and \; \phi 2 : Fp \longrightarrow Fp, \phi 2(z) = zp - 1$. By Fermat's Little Theorem we have that

$$Per(\phi_1(z), F_p) = F_p, and \; Per(\phi_2(z), F_p) = \{0,1\}$$

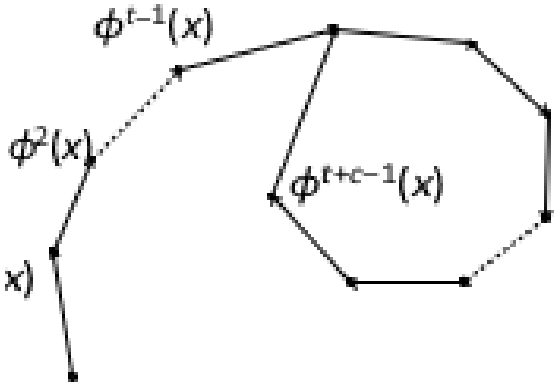


Figure 1: Tails and Cycles of an iteration

3.2 Dynamics of the Mapping $x' \mapsto x^2 \bmod p$

As an introduction, we will focus on the dynamics of the mapping $\phi: F_p \longrightarrow F_p$, where pis a prime, and $\phi(x) = x2$. We will primarily study the behavior of its functional graph, which we denote by $G_{x \longrightarrow x^2}$, and draw several conclusions about these graphs based on the nature of the prime punder consideration. Given $x \in F_p$, we denote by $t_p(x)$ the tail length and $c_p(x)$ as the cycle length in the graph $G_{x \longrightarrow x^2}$. The questions that arise are the following:

1. Given $x \in U_p$, what is the size of its tail? What is the size of its cycle? What is the average size of the cycles and tails?
2. Given a prime number p, what is the structure of the graph $Gx \longrightarrow x2$? If we remove the cycles, is it connected? Disconnected?

These questions are answered in (Vasiga & Shallit, 2004), and we will exhibit the answers in this section, providing examples for certain primes p, and verifying some calculations using the tool provided by GAP (Groups, Algorithms, and Programming).

It is not difficult to verify that if $\phi: FP \longrightarrow FP$ is given by $\phi(x) = x2 mod p$, then the n-th iteration of ϕ is explicitly given by the formula

$$\phi n(x) = x2n mod p.$$

A function to calculate the n-th iteration of the map $\phi(x) = x^2 mod p$ can be easily programmed in GAP:

```
gap > IterCdr:= function(x, p, n)
> local a, k;
> a:= x mod p;
> for k in [1..n] do
> a:= a^2 mod p;
> od;
> return a;
> end;
> function( x, p, n )... end
```

The function IterCdr takes an integer x, a prime p, and a positive integer n and calculates the n-th iteration, modulo p, of the mapping $\phi(x) = x2$. As an example, we show some calculations for $p = 13$ and $p = 17$.

```
gap > IterCdr(2,13,2); 3
gap > IterCdr(2,13,3); 9
gap > IterCdr(11,13,5); 9
```

gap > IterCdr(10,17,4); 1
gap > IterCdr(3,17,3); 16
gap > IterCdr(12,17,2); 13

The first three calculations tell us that $\phi 2(2) = 3 \bmod 13$, $\phi 3(2) = 9 \bmod 13$, $\phi 5(11) = 9 \bmod 13$, and the other three tell us that $\phi 4(10) = 1 \bmod 17$, $\phi 3(3) = 16 \bmod 17$, $\phi 2(12) = 13 \bmod 17$. We can observe the structure of the functional graphs that describe the iterations of the quadratic map $x \longrightarrow x2 \bmod p$, for $p = 13$ and $p = 17$, in the following figures.

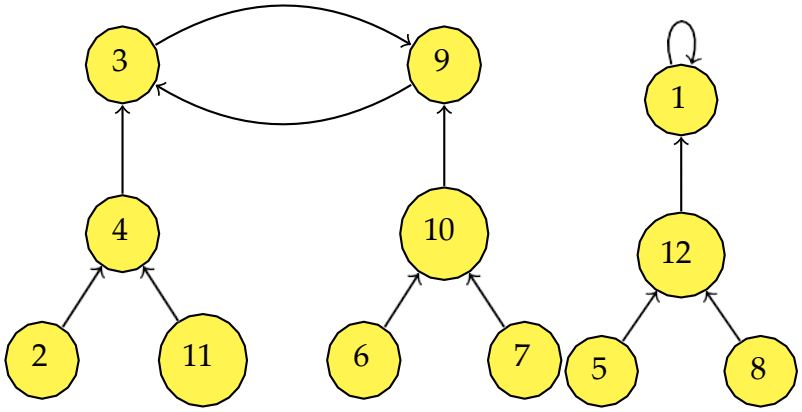


Figure 2: Functional Graph of $\phi(x) = x2$ over F_{13}^*. The node 0 is omitted, as $\phi(0) = 0$ (Fixed Point)

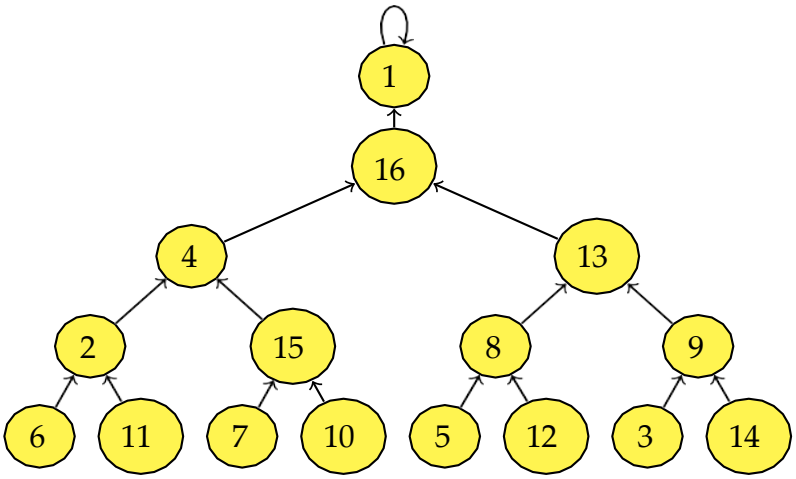


Figure 3: Functional Graph of $\phi(x) = x^2$ over F^*. The Structure is a Complete Binary Tree

rooted at 16, feeding into the fixed point 1. The following theorem describes the length of the tail and the cycle of a point $x \in U_p$ in the graph $G_{x \to x^2}$.

Theorem 24. Let $p > 2$ be a prime and $x \in U_p$. Then the tail length of x, $t_p(x)$, and the cycle length of x, $c_p(x)$, in the functional graph $G_{x \to x^2}$ are given by

$$t_p(x) = v_2(ord_p x),$$
$$c_p(x) = ord_l 2,$$

where $\operatorname{ord} px = 2e \cdot l$ *and* e, l are non-negative integers with l odd.

The proof uses basic techniques from number theory, following the reasoning in (Vasiga & Shallit, 2004). Proof. To simplify the notation in the proof, we write $t = t_p$ and $c = c_p$. Let $\phi: U_p \longrightarrow U_p$ be given by $\phi(x) = x^2 \bmod p$. If $\phi^{t+c}(x) = \phi^t(x)$, then $x^{2^{t+c}} \equiv x^{2^t} \bmod p$, and since $x \in U$, it follows that $x^{2^t(2^c-1)} \equiv 1 \bmod p$. Let $\operatorname{ord} x = 2^e \cdot l$, with e and l non-negative integers, and l odd. Then $2^e \mid 2^t(2^c - 1)$. By the definitions of $t$and c, it follows that $e = t = v_2(\operatorname{ord}_p x)$, and furthermore c is the smallest positive integer such that $2^c \equiv 1 \bmod l$. Therefore, $c = \operatorname{ord}_l 2$. The following functions, programmed in GAP, calculate the tail length $t_p$and the cycle length $c_p$of an integer $x \in U_p$. We use the command P Valuation (n, p) which in GAP calculates the function $v_p(n)$ that we defined in the number theory concepts.

```
gap > Cola:= function(x, p)
> local t;
> t:= PValuation(OrderMod(x, p),2);
> return t;
> end;
function( x, p ) ... end gap > Cola(4,13); 1
gap > Cola(6,13); 2
gap > Cola(13,17); 2
gap > Cola(7,17); 4
```

The function Cola (x, p) calculates the tail length of a positive integer in the functional graph of the function $\phi: F_p \longrightarrow F_p, x \longrightarrow x^2 \bmod p$. In Figure 2 we can see that the tail length of $x = 6$ is $t_{13}(6) = 2$ and in Figure 3 we can see that the tail length of $x = 7$ is $t_{17}(7) = 4$. The following GAP commands correspond to the function we call Ciclo and calculate the cycle length of an integer $x \in U_p$. gap > Ciclo:= function(x, p)

```
> local t, l, ci;
> t:= PValuation(OrderMod(x, p),2);
> l:= OrderMod(x, p)/(2^t);
> ci:= OrderMod(2, l);
> return ci;
> end;
function( x, p ) ... end gap > Ciclo(4,13); 2
gap > Ciclo(7,11); 4
gap > Ciclo(8,17); 1
```

It can be seen from the calculations that in the functional graph $G_{x\longrightarrow x^2}$ the cycle length described by $x = 4$, for $p = 13$, is $c_{13}(4) = 2$ (see Figure 2). And that for any element in U_{17}, its cycle length is 1 (see Figure 3). The following theorem specifies the elements that have tail length zero, and tail length equal to $k > 0$ in terms of the primitive root modulo p.

Theorem 25. *Let* $p > 2$ be a prime, and let γ be a primitive root modulo p, then a)

$$a) \quad \{\alpha \epsilon U_p : t_p(\alpha) = 0\} = \{\gamma^i : 0 \le i < p \text{ and } v_2(i) \ge v_2(p-1)\}.$$

$$b) \text{ For } 1 \le k \le v_2(p-1) \text{ we have}$$
$$\{\alpha \epsilon U_p : t_p(\alpha) = k\} = \{\gamma^i : 0 \le i < p \text{ and } v_2(i) = v_2(p-1) - k\}.$$

We will omit the proof of this theorem, which can be found in (Vasiga & Shallit, 2004). The following function in GAP returns the list of those integers in U_p that have a tail of length zero in the functional graph $G_{x\longrightarrow x^2}$; that is, the elements that are in a cycle. gap > Tl0:= function(p)

```
> local T;
> T:= Filtered([1..p − 1], x−> Cola(x, p) = 0);
> return T;
> end;
function( p ) ... end gap > Tl0(13);
$[ 1, 3, 9 ]$
gap > Tl0(17);
$[\ 1\ ]$
```

Note that in this case we use the previously defined function Cola to find the elements whose tail is of length zero. The elements in the cycles can also be calculated using the following function, which utilizes the command Primitive Root to calculate the primitive root modulo n; the drawback is that the result is given in terms of $Z(n)$ defined in GAP. gap > Tl0:= function(p)

```
> local T, P, r;
> r:= PrimitiveRoot(GF(p));
> T:= Filtered([0..p − 1], x−> PValuation(x, 2) >= PValuation(p − 1,2));
> P:= List(T, i−> r ^ i);
> return P;
> end;
function( p ) ... end gap > Tl0(13);
$[\ Z(13)\wedge 0\ ,\ Z(13)\wedge 4\ ,\ Z(13)\wedge 8\ ,\ Z(13)\wedge0\ ]$ gap > Tl0(17);
```

$[\ Z(17)\wedge 0,\ Z(17) \wedge 0\ ]$

The function Tl0, which depends on the previously programmed function Cola, can be modified to calculate those elements whose tail is of length $k > 0$. gap > Tlk:= function(p, k)

> local T;

> T:= Filtered([1..p − 1], x−> Cola(x, p) = k);

> return T;

> end;

function(p) ... end

The function Tlk takes a prime p and an integer $k \geq 0$ and calculates the list of those integers in U_p whose tail length is k. The following corollary further discusses the general structure of the graph $G_{x\to x^2}$. Corollary 26. Let $p > 2$ be a prime with $p - 1 = 2^\tau \cdot \rho, \rho$ odd. For every positive integer d that divides ρ, $G_{x\to x^2}$ contains $\varphi(d)/ord_{d^2}$ cycles of length ord_{d^2}. There are ρ elements in all these cycles combined. Furthermore, from each element in every cycle, a reverse complete binary tree of height $\tau - 1$ hangs, containing $2^\tau - 1$ nodes. Example 27. In Figure 2 we can see that $p - 1 = 12 = 2^2 \cdot 3$. Thus $\tau = 2$ and $\rho = 3$. The divisors of ρ are 1 and 3. Then $G_{x\to x^2}$, in this case, has $\varphi(3)/ord_{3^2} = (3 - 1)/2 = 1$ cycle of length $ord_{3^2} = 2$. There are $\rho = 3$ elements in all these cycles. We can also appreciate that off of the cycle elements (which are 1, 3, 9), reverse binary trees of height $\tau - 1 = 2 - 1 = 1$ hang, and these trees contain $2^\tau - 1$= 4 − 1 = 3 nodes.

3.2.1 Special Cases: Fermat and Mersenne Primes

Two special cases provide specific insights into the structure of the graph $G_{x\to x^2}$. We discuss them in the following theorems. The first relates to Fermat primes.

Theorem 28. The structure of the functional graph $G_{x\to x^2}$ for a prime p of the form $p = 2^{2k} + 1$, a Fermat prime, is a reverse complete binary tree of height $2^{2k} - 1$ rooted at $p - 1$, and it has a cycle of length 1 at the integer 1. Furthermore, the elements x with $t(x) = a$ for $0 \leq a \leq 2^k$ are given by $3^{e22k-a}, 0 \leq e \leq 2^\alpha$, with e odd. In this case, the graph is connected (ignoring the direction of the arrows).

Example 29. The functional graph in Figure 3 satisfies the previous theorem; note that $p = 17 = 2^{22} + 1$ is a Fermat prime. The following theorem gives a complete description of the graph $G_{x\to x^2}$ when $p = 2^q - 1$, a Mersenne prime.

Theorem 30. When $p = 2^q - 1$, a Mersenne prime, the graph $G_{x\to x^2}$ consists of cycles whose lengths divide $q - 1$. Hanging off of each of these cycles is a unique element with a tail length of 1.

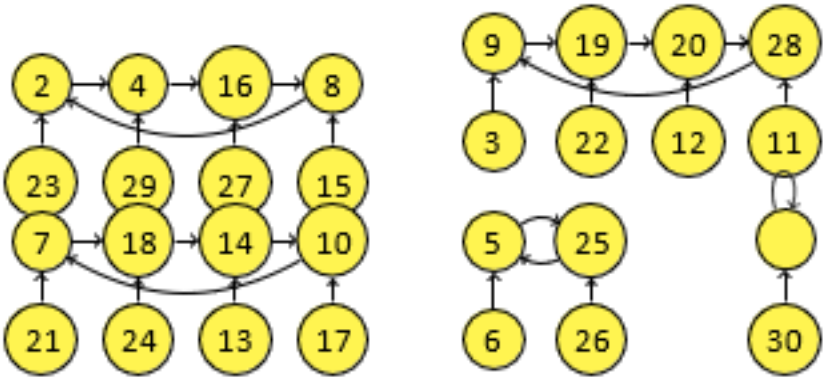


Figure 4: Functional graph $G_{x\to x^2}$ over F^*. This structure, typical of a Mersenne prime $p = 2^q - 1$, shows cycles whose lengths (4, 2, 1) divide $q - 1 = 4$, each with a unique tail of length 1

Figure 4 corresponds to the graph $G_{x\to x^2}$ for $p = 31 = 2^5 - 1$, which is a Mersenne prime. We can see that there are three cycles of length 4, one of length 2, and the cycle of length 1. Clearly, each of these lengths' divides $q - 1 = 5 - 1 = 4$. Furthermore, it can be appreciated that off of each cycle, there is only one node whose tail length is 1, which complies with the description in Theorem 30.

3.2.2 Statistical Measures of the Dynamics

To conclude this section, we will mention some important results concerning the questions posed at the beginning. The two previous theorems answer questions about the graph structure, and the following theorem provides conclusions about the lengths and cycles. First, we adopt the notation used in (Vasiga & Shallit, 2004).

Definition 31. With respect to the iteration $x \longrightarrow x^2 \bmod p$, we define

i. $TC(p)$ = the total number of cycles;
ii. $T_0(p)$ the total number of elements in all cycles;
iii. $AC(p)$ = the average cycle length (based on the number of cycles);
iv. $C(p)$ = the average value of $C_p(a)$ over all $a \in U_p$;
v. $T(p)$ = the average value of $t_p(a)$ over all $a \in U_p$.

Example 32. For $p = 13$, we have $TC(13) = 2$, $T_0(13) = 3$, $AC(13) = 3/2$, $C(13) = 5/3$, $T(13) = 5/4$.

Theorem 33. *Let* $p - 1 = 2^r \cdot \rho$ with ρ odd. With respect to the iteration $x \longrightarrow x^2 \ mod \ p$, we have

i. $TC(p) = \sum_{d|\rho} \frac{\varphi(d)}{\text{ord}_d(2)}$;
ii. $T_0(p) = p$;
iii. $AC(p) = \frac{\rho}{TC(p}$
iv. $C(p) = \frac{1}{\rho} \sum_{d|\rho} \varphi(d) \ \text{ord}_d 2$;
v. $T(p) = \frac{1}{p-1} \sum_{d|p-1} \varphi(d) \ \nu_2(d) = \tau - 1 + 2^{-r}$

The proof of statements $i - iv$ is based on Corollary 26, and the calculations for the proof of *v* can be seen in (Vasiga & Shallit, 2004). The formulas from the preceding theorem can be programmed following the GAP commands below.

i. The total number of cycles is calculated in GAP as follows:

```
gap > TC:= function(p)
> local tau, rho, D, s, d;
> tau:= PValuation(p - 1,2);
> rho:= (p - 1)/(2^(tau));
> D:= DivisorsInt(rho);
> s:= 0;
> for d in D do
> s:= s + Phi(d)/OrderMod(2, d);
> od;
> return s;
> end;
function( p ) ... end
gap > TC(13); TC(17); TC(29);
2
1
3
```

ii. The number of elements in all cycles, which is known to be ρ by Corollary 26, is calculated in GAP as follows:

```
gap > T0:= function(p)
> local tau, rho;
> tau:= PValuation(p - 1,2);
> rho:= (p - 1)/(2^(tau));
> return rho;
> end;
function( p ) ... end
gap > T0(13); T0(17); T0(29); 3
1
7
```

iii. The average cycle length is calculated in GAP using the functions TC and T0:

```
gap > AC:= function(p)
> local ac;
> ac:= T0(p)/TC(p);
> return ac;
> end;
function( p ) ... end
gap > AC(13); AC(17); AC(29);
```

3/2
1
7/3

iv. The average value of the cycle lengths of all elements of $U_p, C(p), is$ calculated in GAP using the following function:

```
gap > C:= function(p)
> local tau, rho, D, s, d, c;
> tau:= PValuation(p − 1,2);
> rho:= (p − 1)/(2^(tau));
> D:= DivisorsInt(rho);
> s:= 0;
> for d in D do
> s:= s + Phi(d) ∗ OrderMod(2, d);
> od;
> c:= (1/rho) ∗ s;
> return c;
> end;
function( p ) ... end gap > C(13); C(17); C(29);
5/3
1
19/7
```

v. Finally, the average value of the tails of all elements of $U_p, T\ (p)$, is calculated in GAP using the following function:

```
gap > T:= function(p)
> local t, tau;
> tau:= PValuation(p − 1,2);
> t:= tau − 1 + 1/(2^(tau));
> return t;
> end;
function( p ) ... end gap > T(13); T(17); T(29);
5/4
49/16
5/4
```

It is worth noting that all these functions can receive an argument that is not nec- essarily a prime number and still perform the calculations. This can be improved by introducing an appropriate if statement that considers the two cases: when p is prime and when p is not prime. Recall that the command Is Prime () tells us whether an integer is prime or not.

3.3 Dynamics of the Mapping $x' \to x^2 + c$ on F_q

From Theorem 6 we know that F_q is a field with $q = p^n$ elements. Furthermore, it is a field of characteristic p according to Definition 8. Let $\phi_c: F_q \longrightarrow F_q$ be defined by $\phi_c(x) = x^2 + c$, where $q = p^n$ with $n \in N$ and $p > 2$ prime. We will examine general aspects of the structure of the functional graph $G_{\phi c}$, focusing mainly on the cycle structure. We will conclude by exhibiting an example in the field with 9 elements.

3.3.1 Number of Predecessors (Preimages)

The following proposition tells us the number of predecessors (preimages) of each element in F_q.

Proposition 34. Let $\phi_c: F_q \longrightarrow F_q\ \phi_c(x) = x^2 + c$, with $c \in U_q$. Then every element $x \in F_q$

i. has two predecessors if and only if $x - c$ is a quadratic residue,
ii. has no predecessors if and only if $x - c$ is a non-quadratic residue,
iii. has one predecessor if and only if $x = c$.

Proof. The proof is direct from the fact that the function ϕ_c is quadratic. The following graphs are for the functions

$\phi_c(x) = x^2 + c$ mod 7 with $c = 1$ (Figure 5) and $c = 5$ (Figure 6). The non-zero quadratic residues modulo 7 are 1, 2, and 4. The non-quadratic residues modulo 7 are 3, 5, and 6. For Figure 5, we can see that $x = 2, 3, 5$ have two predecessors because in these cases $x - 1$ coincides with the quadratic residues modulo 7; on the other hand, $x = 4$, 6, 0 have no predecessors since $x - 1$ in these cases is a non-quadratic residue modulo 7; and finally, $x = 1$ has a unique predecessor, thus satisfying the previous proposition.

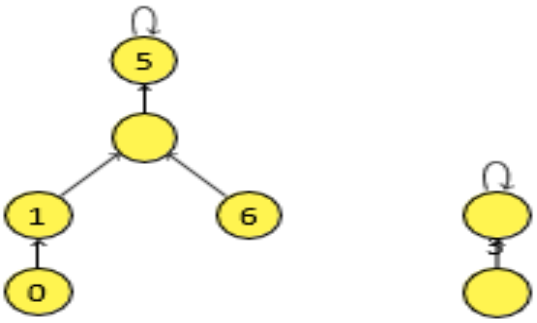


Figure 5: Functional Graph of $\phi_1(x) = x^2 + 1$ over F_7

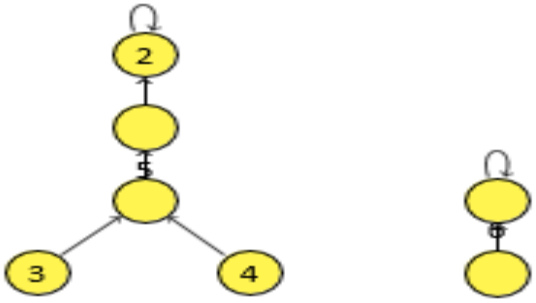


Figure 6: Functional Graph of $\phi_5(x) = x^2 + 5$ over F_7

In Figure 6, it can be seen that $x = 0$, 2, 6 have two predecessors because in these cases $x - 5$ coincides with the quadratic residues modulo 7; on the other hand, $x = 1, 3, 4$ have no predecessors since $x - 1$ in these cases is a non-quadratic residue modulo 7; and finally, $x = 5$ has a unique predecessor. In summary, proposition 34 tells us that $x = c$ has a unique predecessor, and that any other element has two or no predecessors. Since there are a total of $(q - 1)/2$ quadratic residues, the maximum cycle length is bounded by $(q + 1)/2$, and the cardinality of $\phi_c(F_q)$ is $(q + 1)/2$, which means calculating the bound for the maximum cycle length is equivalent to calculating the cardinality $\phi_c(F_q)$ (see (Peinado et al., 2001)). The following proposition guarantees the existence of cycles of length 1 and 2.

Proposition 35. Let $\phi_c: F_q \longrightarrow F_q$, $\phi_c(x) = x^2 + c$, with $c \in U_q$. Then,

i. there exists only one cycle of length 1, if and only if $1 - 4c = 0$,

ii. there exist two cycles of length 1 if and only if $1 - 4c$ is a quadratic residue.

Proposition 36. Let $\phi_c: F_q \longrightarrow F_q$, $\phi_c(x) = x^2 + c$ with $c \in U_q$. Then, there exists a cycle of length 2 if and only if $1 - 4(c + 1)$ is a quadratic residue.

Example 37. If we consider $\phi_4(x) = x^2 + 4$ mod 7, it is not difficult to prove that $1 - 4(c + 1)$ is a quadratic residue modulo 7. We can see in Figure 7 that there is indeed a cycle of length 2.

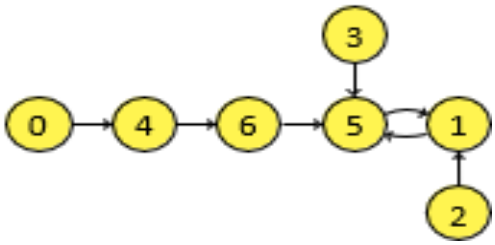


Figure 7: Functional Graph of $\phi_4(x) = x^2 + 4$ over F_7

3.4 Example in F_9

We will exhibit an example in F_9, the field with 9 elements. To construct the field with 9 elements, we start with the

irreducible polynomial $f(x) = x^3 + x^2 + x - 1$ with coefficients in F_3. Then we define $F_9 = F_3[x]/\langle x^3 + x^2 + x - 1\rangle$. The following lemma will help us identify the elements in this field.

Lemma 38. The set of 2 × 2 matrices given by

$$\mathbb{M}_9 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{F}_3 \right\}$$

forms a field of 9 elements isomorphic to F_9.

This set can be explicitly represented by

$$\mathbb{M}_9 = \left\{ \hat{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \hat{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{2} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \hat{3} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \right.$$
$$\left. \hat{4} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \hat{5} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \hat{6} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \hat{7} = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}, \hat{8} = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \right\}.$$

From the previous lemma, we can identify the polynomial $\phi_c(x)$ in $F_9[x]$ as a matrix polynomial in M_9 in the following way

$\phi_c(x) = x^2 + c$,

where C is one of the matrices in M_9.

Example 39. Consider in M_9 the polynomial $\phi(x) = x^2 + \hat{1}$, in matrix form this is

$$f(x) = X^2 + I_2, where\ I_2 = \hat{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

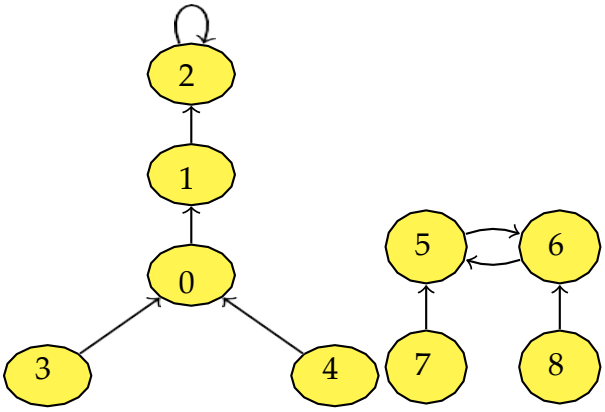


Figure 8: Functional graph of $\phi(X) = X^2 + \hat{1}$ over M_9, isomorphic to F_9

In Figure 8 we can see the functional graph of the function $\phi_1\hat{}(x) = x^2 + 1\hat{}$ in F_9.

We can observe that there is a cycle of length 1 according to Proposition 3.2, since $1 - 4c = \hat{1} - 4 \cdot \hat{1} = -3 \cdot \hat{1} = \hat{0}$ mod 3. It can also be seen that $1 - 4(c + 1) = \hat{1} - 4 \cdot \hat{2} = \hat{2} = \hat{3}^2$. Since $1 - 4(c + 1)$ is a quadratic residue, according to Proposition 3.3, a cycle of length 2 exists.

4. Discussion

The results obtained demonstrate that the dynamics of quadratic functions over finite fields exhibit a highly regular structure, which can be explained through general algebraic properties of the multiplicative group $Fp*$. It has been confirmed that the decomposition of the order of elements into powers of two odd factors becomes a determining component in establishing the length of tails and cycles in functional graphs. These findings are consistent with results reported in studies on quadratic iterations over finite fields (Vasiga & Shallit, 2004).

Regarding the configuration of functional graphs, it is observed that they exhibit structures composed of cycles to which inverse binary trees are attached, confirming the theoretical model derived from graph theory. The existence of these trees reveals the presence of multiple preimages for certain elements, which is directly associated with the quadratic nature of the function. This observation aligns with the principles established in graph theory applied to discrete dynamical systems (Bondy & Murty, 2008).

The configuration allows the dynamics to be addressed from a perspective that extends beyond purely algebraic considerations, incorporating combinatorial aspects. The results also show that the number of cycles, their length, and the distribution of elements within functional graphs depend directly on the factorization of $p - 1$. This behavior supports the assertion that the arithmetic structure of the finite field determines the global dynamics of the system, in accordance with

the foundations of number theory, particularly in relation to multiplicative orders and quadratic residues (Ireland & Rosen, 1990).

In this sense, the relationship established between modular arithmetic and iterative dynamics is consolidated as a central framework for understanding the phenomenon under study. Furthermore, the analysis of particular cases, such as Fermat primes and Mersenne primes, made it possible to identify distinct structural patterns in functional graphs: for Fermat primes, the structure tends to be more compact and connected, typically presenting a single main cycle, whereas for Mersenne primes, multiple cycles are observed with sizes determined by divisors, reflecting greater structural complexity. This reinforces the importance of classifying prime numbers within the dynamic analysis of iterative functions.

With respect to computational validation, the use of the GAP system allowed for precise verification of theoretical results, particularly concerning cycle lengths, tail lengths, and the total number of cycles. The agreement between analytical and computational results confirms the robustness of the methodological approach and the suitability of computational tools for analyzing algebraic dynamical systems. Moreover, these findings are consistent with previous studies that employed computational methods to examine maximal periods and dynamic structures in finite fields (Peinado et al., 2001).

Finally, the results obtained allow us to assert that the dynamics of quadratic functions over finite fields are not arbitrary but rather governed by well-defined structural patterns determined by the algebraic and arithmetic properties of the system. This regularity not only facilitates theoretical characterization but also opens avenues for applications in cryptography, where structural predictability and computational complexity are of particular interest (Silverman, 2007).

The discussion confirms that the results of the present study are coherent with those reported in the literature, while also contributing a clear unification of algebraic theory, graph theory, and computational analysis, thereby strengthening the understanding of iterative dynamics in finite contexts.

5. Final Considerations

First, it was concluded that the dynamics of quadratic functions over finite fields are determined by the algebraic structure of the multiplicative group $Fp*$, particularly by the decomposition of the order of its elements into powers of two and odd components. This relationship enables the precise determination of the lengths of tails and cycles in functional graphs, demonstrating that the observed iterative behavior is not random but instead governed by well-defined arithmetic properties.

Second, it was established that functional graphs derived from quadratic functions are characterized by cycles to which inverse binary trees are attached. This structure allows the dynamics to be described from a combinatorial and graphical perspective, confirming that graph theory provides an effective framework for modeling and analyzing discrete dynamical systems over finite structures.

Third, it was determined that the number of cycles, their lengths, and the distribution of elements within functional graphs depend directly on the factorization of $p - 1$. This finding confirms that modular arithmetic and number theory are fundamental tools for understanding iterative dynamics, thereby consolidating the relationship between different mathematical domains in the study of functions over finite fields.

Fourth, the analysis of cases, such as Fermat primes and Mersenne primes, revealed distinct structural patterns in functional graphs, demonstrating that the nature of the prime number significantly influences the global structure of the dynamical system. This also provides a more concrete and in-depth understanding of the behavior of quadratic functions in these specific cases.

Finally, it was concluded that the integration of theoretical methods with computational tools, such as the GAP system, enables consistent validation of results, thereby enhancing the reliability of the study. Overall, this research contributes to the development of the algebraic approach to discrete dynamical systems, offering a rigorous characterization of the dynamics of quadratic functions over finite fields and opening new directions for future research in cryptography and computational analysis of algebraic systems.

6. References

Bondy, J. A., & Murty, U. S. R. (2008). *Graph theory*. Springer Publishing Company, Incorporated.

Chatterjee, S., & Chakraborty, S. (2023). A Multi-criteria decision making approach for 3D printer nozzle material selection. *Reports in Mechanical Engineering*, *4*(1), 62-79.

Ireland, K., & Rosen, M. I. (1990). *A classical introduction to modern number theory* (Vol. 84). Springer Science & Business Media.

Jacobson, N. (2009). *Basic Algebra I* (Vol. 1). Courier Corporation.

Lang, S. (2002). Algebra. *Graduate Texts in Mathematics*.

Peinado, A., Montoya, F., Munoz, J., & Yuste, A. (2001). Maximal periods of x2+ c in Fq. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (pp. 219-228). Springer.

Rotman, J. J. (1995). An Introduction to the Theory of Groups. *Graduate Texts in Mathematics*.

Silverman, J. H. (2007). The Arithmetic of Dynamical Systems. *Graduate Texts in Mathematics*, *241*.

Vasiga, T., & Shallit, J. (2004). On the iteration of certain quadratic maps over GF (p). *Discrete Mathematics*, *277*(1-3), 219-240.