N° d'ordre: 135/2022-C/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE
Houari Boumediene
FACULTÉ DE MATHÉMATIQUES

THÈSE DE DOCTORAT
Pour l'obtention du grade de Docteur
En : MATHÉMATIQUES
Spécialité: Algèbre et théorie des nombres

Présentée par: SALHI Celia

Intitulée:

Etude des périodes de suites récurrentes bi-périodiques et courbes elliptiques

Soutenue publiquement, le 22/12/2022, devant le jury composé de:

M. Boualem BENSEBA	Professeur à l'USTHB	Président.
M. Hacène BELBACHIR	Professeur à l'USTHB	Directeur de thèse.
M. Mohand Ouamar HERNANE	Professeur à l'USTHB	Examinateur.
M. Rachid BOUMAHDI	Maître de conférences/A à l'ESI	Examinateur.
M. Salah Eddine RIHANE	Maître de conférences/A à l'ENSMath	Examinateur.

N°: 135/2022-C/MT

THE DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF SCIENCES AND TECHNOLOGY HOUARI BOUMEDIENE
FACULTY OF MATHEMATICS

DOCTORAL THESIS

Presented for the obtaining of the grade of a **DOCTOR IN MATHEMATICS**

Domain: Algebra and Number Theory

By: Celia SALHI

Title

Study of the periods of bi-periodic recurrence sequences and elliptic curves

Publicly defended, on 22/12/2022, in front of the jury composed by:

Mr. Boualem BENSEBA	Professor	at USTHB	Chairman.
Mr. Hacène BELBACHIR	Professor	at USTHB	Thesis Supervisor.
Mr. Mohand Ouamar HERNANE	Professor	at USTHB	Examiner.
Mr. Rachid BOUMAHDI	Assoc. Professor	at ESI	Examiner.
Mr. Salah Eddine RIHANE	Assoc. Professor	at ENSMath	Examiner.

ACKNOWLEDGMENT

All praise and thanks to god, the almighty, for granting me strength, courage and patience to accomplish this thesis.

First and foremost, I am extremely grateful to my supervisor Professor **BELBACHIR Hacène**, for his continuous support, assistance, and patience. The words are certainly not enough to express my gratitude to him, for all his efforts. I admire his immense knowledge and his remarkable humility, it was great privilege and honor to achieve this project under his guidance.

I would like to express my deep and sincere gratitude to Professor **TAN Elif** and Professor **SAHIN Murat** from Ankara University.

I would like to express my deepest gratitude to Pr. **BENSEBA Boualem** for giving me honor by agreeing to preside the jury.

I also express my sincere thanks to the honorable jury members: Pr. **HERNANE Mohand Ouamar** from USTHB, Dr. **BOUMAHDI Rachid** from ESI, and Dr. **RIHANE Salah Eddine** from ENSMath.

My deepest gratitude goes to my family and friends for their care and help. Without their advice and continuous support, I would not be able to complete this work.

Finally, I warmly thank SADOUN Mohamed and JAMOUS Abdelillah for their invaluable support, as well as their sage advice and observations.

ABSTRACT

In recent years, several work investigated the periodicity of linear recurrence sequences over elliptic curves. This thesis is devoted to the study of the periodicity of some bi-periodic recurrence sequences over elliptic curves.

In part, we investigate the periodicity of some bi-periodic recurrence sequences reduced modulo a given positive integer m. We extend some properties of Fibonacci sequence modulo m to bi-periodic sequences which are: the generalized bi-periodic Fibonacci sequence and the bi-periodic Horadam sequence. Moreover, since the set of points of an elliptic curve defined on a finite field forms a finite abelian group, we define the bi-periodic Horadam sequence and we investigate the periods of the bi-periodic Horadam sequence over a such elliptic curves. We establish the link between the periods of the bi-periodic Fibonacci sequence modulo m and the periods of the Horadam sequence on an elliptic curve.

Keywords: Generalized bi-periodic Fibonacci sequence, bi-periodic Horadam sequence, period, finite fields, elliptic curves.

RESUME

L'étude des points periodiques sur une courbe elliptique régis par la suite de Fibonacci et de ses extensions a fait l'objet de plusieurs papiers récents. Nous nous proposons dans cette thèse d'étudier les points périodiques sur une courbe elliptique régis par certaines suites récurrentes bi-periodiques.

L'objectif de cette thèse est d'une part l'étude des périodes de certaines suites récurrentes bi-périodiques qui sont périodiques lorsqu'elles sont considérées modulo un entier $m > 1$. Notre contribution a été d'étudier la périodicité de ces suites et de généraliser certaines propriétés des suites de Fibonacci modulo m aux suites bi-périodiques qui sont : la suite de Fibonacci bi-périodique généralisée et la suite de Horadam bi-périodique.

D'autre part, puisque l'ensemble des points d'une courbe elliptique définie sur un corps fini forme un groupe abélien fini, nous définissons la suite de Horadam bi-périodique que nous étudions sur de telles courbes elliptiques, ce qui nous donne des suites périodiques. Nous établissons, également, le lien entre les periodes de la suite de Fibonacci bi-périodique modulo un entier $m > 1$ et les periodes de la suite de Horadam bi-périodique sur une courbe elliptique.

Mots-clés : Suite de Fibonacci bi-periodic généralisée, suite de Horadam bi-periodique, periode, corps finis, courbe elliptique.

NOTATIONS

1. $\mathbb{K}$: Field.
2. $\bar{\mathbb{K}}$: Algebraic closure of $\mathbb{K}$.
3. R : Ring.
4. $\mathbb{Z}$: Ring of integers.
5. $\mathbb{Z}_m$: The ring of integers modulo m.
6. $\mathbb{F}_q$: Finite field with q elements.
7. $\mathbb{F}_q^*$: The set of cyclic group of nonzero elements of $\mathbb{F}_q$.
8. $\operatorname{ord}_e(q)$: Multiplicative order of q modulo e.
9. φ : Frobenius automorphism.
10. $\mathbb{K}[x]$: Ring of polynomials with coefficients in $\mathbb{K}$.
11. $\left(\frac{q}{p}\right)$: Legendre Symbol.
12. $\binom{n}{k}$: Binomial coefficient.
13. $\mathrm{Mat}_m(R)$: Ring of matrices of size $m \times m$ with coefficients in R.
14. $\det(A)$: Determinant of square matrix A.
15. $GL_m(R)$: The general linear group of matrices of size $m \times m$ with coefficients in R.
16. $\operatorname{ord}(g)$: Multiplicative order of an element g in the group G.
17. $\lfloor x \rfloor$: Floor function.
18. $\xi(.)$: Parity function.
19. $gcd(a, b)$ or (a, b) : greatest common divisor of a and b.
20. $n!$: n factorial.
21. $(q_n)_n$: Bi-periodic Fibonacci sequence.
22. $(F_n)_n$: Generalized bi-periodic Fibonacci sequence.
23. $(H_n)_n$: Bi-periodic Horadam sequence.

TABLE OF CONTENTS

INTRODUCTION

The study of recurrence sequences is plainly of intrinsic interest and has been a central part of number theory for many years. These sequences appear in many parts of the mathematical sciences in the wide sense (which includes applied mathematics and applied computer science). The study of the behavior of linear recurrence sequences when reduced modulo a positive integer was begun about one hundred years ago. Two important aspects of the modular situation are the periodicity of the sequence and the distribution of the residues in a period. The interest in this topic is the diversity of the fields of application such that cryptography (the generation of pseudo-random numbers), coding theory and electrical engineering.

Wall [52] studied the periodicity of the Fibonacci sequence modulo an arbitrary integer m and established many interesting results. Vinson [48] extended the work of Wall and studied the rank of apparition of m in the Fibonacci sequence. Vince [51] considered the generalized linear recurrence sequence defined over a ring of integer A of an algebraic number field and he studied the properties on the periods of these sequences modulo an ideal of A. Recently, the periodicity of various generalizations of the Fibonacci sequence has been investigated in several papers, see [18, 25, 31, 49, 50].

Moreover, several work establishing links between elliptic curves and linear recurrent sequences have been carried out, mainly with Fibonacci sequence and their generalizations, for example, in [30] Ribenboim provides the points with integral coordinates in certain elliptic curves. Another link is to determine perfect powers in elliptic divisibility sequences, see [33]. Bilu et al. [9] studied the sequence of numbers whose mth term is the number of points of E on $\mathbb{F}_{q^m}$, where E is an elliptic curve over the finite field $\mathbb{F}_q$.

In particular, we are interested in the periodicity of linear recurrence sequence over elliptic curves. Coleman et al. [10] were the first authors that investigated periodicity of classical Fibonacci sequence over elliptic curves. Ait-Amrane et al. [2] made a link between enumerative combinatorics and number theory through elliptic curves by exploring the case of Morgan-Voyce sequence on elliptic curves. This work has been extended to a third order linear recurrence sequence, in particular the Tribonacci sequence [3].

The goal of this thesis is to study of periods of bi-periodic sequences over elliptic curves. We first investigate periods of some bi-periodic sequences reduced modulo a given positive integer m, which are: the generalized bi-periodic Fibonacci sequence and the bi-periodic Horadam sequence. Next, we investigate the periods of the bi-periodic Horadam sequence over an elliptic curve defined over a finite field.

This thesis is structured into the following chapters:

Chapter 1

In the first chapter, we introduce some preliminaries on number theory and abstract algebra that we will use in the rest of the present thesis. We also give some definitions and results on bi-periodic recurrence sequences.

Chapter 2

In this chapter, we consider the generalized bi-periodic Fibonacci sequence defined by a second-order non-linear recurrence relation depending on four positive integers a, b, c, and d, defined by

$$F_0 = 0, \ \ F_1 = 1, \ \text{ and } \ F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + dF_{n-2}, & \text{for } n \text{ odd,} \end{cases} \ (n \geq 2).$$

We investigate the periodicity of the sequence $(F_n)_n$ when reduced modulo $m \geq 2$. We prove that $(F_n \bmod m)_n$ is periodic when m is relatively prime to c and d, i.e., there exists a positive integer r such that $F_{n+r} = F_n$, for all $n \geq 0$. We extend some well-known results on the period and the rank of the classical Fibonacci sequence to the bi-periodic case.

Chapter 3

In this chapter, we use the matrix approach to study the periodicity of the sequence $(F_n)_{n\geq 0}$. Considering a matrix representation C of $(F_n)_{n\geq 0}$, we show that the study of the period of the sequence $(F_n)_{n\geq 0}$, whose elements are in $\mathbb{Z}_m$ is equivalent to the study of the period of the sequence $(C^n \bmod m)_{n\geq 0}$ over the group $GL_2(\mathbb{Z}_m)$. The main purpose is to investigate the behavior of $(F_n)_{n\geq 0}$ over finite fields and show that we can express the period of the sequence $(F_n)_n$ modulo a power of prime p in terms of the period modulo p, which allows us to obtain bounds for the period for each positive integer m.

Chapter 4

In the last chapter, we let a, b, H_0, H_1, and c be positive integers and we consider the bi-periodic Horadam sequence defined by

$$H_n = \begin{cases} aH_{n-1} + cH_{n-2}, & \text{for } n \text{ even;} \\ bH_{n-1} + cH_{n-2}, & \text{for } n \text{ odd,} \end{cases} \ (n \geq 2).$$

with arbitrary initial conditions H_0, H_1. Motivated by papers that study periods of linear recurrence sequences over elliptic curves [10, 2, 3], we extend this idea to the bi-periodic Horadam sequence. We first investigate the period of the bi-periodic Horadam sequence modulo a positive integer m. Next, we define the bi-periodic Horadam sequence associated to an elliptic curve E over the finite field $\mathbb{F}_p$, for an odd prime p, and we investigate periods of the bi-periodic Horadam sequence on the elliptic curve E. Finally, we show that the study of periods of the bi-periodic Horadam sequence on E is closely related to the study of periods of the generalized bi-periodic Fibonacci sequence $(F_n \bmod m)_{n\geq 0}$.

CHAPTER 1

PRELIMINARIES

In this chapter, we introduce some preliminaries that we will use in the rest of the present thesis. The first two section is devoted to the main mathematical notions on number theory and abstract algebra employed in this work.

In the last section, we introduce the bi-periodic sequences that will be studied throughout this thesis. We also gather some results given in [8, 13, 34, 54].

1.1 Some Results on Number Theory

This section contains some definitions and results from number theory and abstract algebra, which can be found in [17, 21, 24, 27].

Definition 1.1. For any two integers $0 \leq n$ and $0 \leq k \leq n$, the binomial coefficient $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Theorem 1.1. (Binomial Theorem) Let x and y be variables, and n be any positive integer. Then

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i. \tag{1.1}$$

Definition 1.2. Let $\phi(n)$ be the number of positive integers less than or equal to n, and relatively prime to n. Also, let $\phi(1) = 1$. The function $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ is called the Euler function.

We can now announce Euler's theorem which is a generalization of Fermat's theorem.

Theorem 1.2. (Euler's Theorem)[17] Let a and n be positive integers, and let $(a, n) = 1$. Then we have

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Corollary 1.1. (Fermat's little theorem) Let p be a prime and let a be an integer.

If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

In particular,

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

Proof. Since $\phi(p) = p - 1$ then the first statement follows from Theorem 1.1. For the second statement there are two cases. If $(a, p) = 1$ multiply by a both sides of

$$a^{p-1} \equiv 1 \pmod{p}.$$

If $(a, p) \neq 1$, then a is a multiple of p so $a \equiv 0 \pmod{p}$. The equation $a^p \equiv a \pmod{p}$ is true as zero equals zero. □

Definition 1.3. For a multiplicative group G, the order of an element $g \in G$, if there exists, is the smallest positive integer k for which $g^k = 1_G$, where 1_G is the identity element of G.

If G is a finite group, the order of G is the number of elements in G. The basic result about orders is the following.

Theorem 1.3. (Lagrange's Theorem) Let G be a finite group.

1. Let $g \in G$. Then the order of g divides the order of G.

2. Let H be a subgroup of G. Then the order of H divides the order of G.

Definition 1.4. Let R be a ring with identity and let $M_m(R)$ be the set of all $m \times m$ matrices with entries in the ring R. We define the general linear group $GL_m(R)$ to be the subset of $M_m(R)$ consisting of all invertible matrices.

Theorem 1.4. The set $GL_m(R)$ forms a group under matrix multiplication; with identity matrix as the identity element of the group.

Over a field $\mathbb{K}$, a matrix is invertible if and only if its determinant is nonzero. Therefore $GL_m(\mathbb{K})$ is the group of matrices with nonzero determinant. Moreover, if $\mathbb{K}$ is a finite field with q elements, the order of $GL_m(\mathbb{K})$ is given by:

$$\prod_{k=0}^{m-1}(q^m - q^k) = (q^m - 1)(q^m - q)(q^m - q^2) \cdots (q^m - q^{m-1}).$$

Let m be a positive integer and let $\mathbb{Z}_m$ be the set of integers modulo m. It is a group with respect to the addition. We can represent the elements of $\mathbb{Z}_m$ by the numbers $\bar{0}, \bar{1}, \ldots, \overline{m-1}$. Let

$$\mathbb{Z}_m^\times = \{a \mid 1 \leq a \leq m, \quad \gcd(a, m) = 1\}.$$

Then $\mathbb{Z}_m^\times$ is a group with respect to the multiplication modulo m. Let $a \in \mathbb{Z}_m^\times$, and let $\mathrm{ord}_m(a)$ denotes the order of a modulo m, i.e., the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. The order of a mod m divides $\phi(m)$.

1.1.1 Chinese Remainder Theorem

Theorem 1.5. (Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers. Let $a_1, a_2, \ldots, a_k$ be integers, and consider the system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

This system has a unique solution x modulo $M = m_1 m_2 \cdots m_k$.

The unique factorization of an integer is implicit in the statement of many results, such as the Chinese remainder theorem stated above. That is, when the modulus m of a congruence is composite it is sometimes possible to reduce a congruence modulo m to a system of simpler congruences.

Theorem 1.6. (Fundamental Theorem of Arithmetic). Every positive integer can be written as a finite product of prime numbers. This decomposition is unique up to the order.

Another way to state the Chinese Remainder Theorem is to say that for any integer m, we have the factorization

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

where p_i are prime numbers and $e_i > 0$. Then we get

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

An important consequence of Theorem 1.5 is that when studying modular arithmetic in general, we can first study modular arithmetic a prime power and then appeal to the Chinese remainder theorem to generalize any results.

1.1.2 Quadratic Residues

In what follows, we consider $a \in \mathbb{Z}$, and p a prime number. Considering the equation $a = x^2 \pmod{p}$. If a solution of the congruence $a = x^2 \pmod{p}$ with $(a, p) = 1$ exists then a is said to be a quadratic residue modulo p; otherwise a is a quadratic nonresidue modulo p.

Definition 1.5. Let p be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined for all a which are not divisible by p; it is equal to 1 if there exists an x such that $a = x^2 \pmod{p}$; otherwise it is equal to -1. That is,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ a nonzero quadratic residue modulo } p; \\ \\ -1, & \text{if } a \text{ a quadratic nonresidue modulo } p. \end{cases}$$

By convention, if a is a multiple of p the Legendre symbol is defined to be zero.

The Legendre symbol is a very practical tool for studying quadratic residues. We will list some of its properties.

Proposition 1.1. [21] Let p be an odd prime and $a, b \in \mathbb{Z}$. Then

(a) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(c) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(d) $(\frac{-1}{p}) \equiv p \pmod{4}$.

Corollary 1.2. [21] There are as many residues as nonresidues modulo p.

Corollary 1.3. [21] The product of two residues is a residue, the product of two nonresidues is a residue, and the product of a residue and a nonresidue is a nonresidue.

Proposition 1.2. [21] 2 is a quadratic residue of primes of the form $8k+1$ and $8k+7$. 2 is a quadratic nonresidue of primes of the form $8k+3$ and $8k+5$. This information is summarized in the formula

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Theorem 1.7. (Quadratic reciprocity law)[21] Let p and q be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

1.1.3 Finite Fields

The theory of finite fields is a branch of modern algebra that has come to the fore in the last fifty years. Finite fields give rise to particularly useful applications of rings and fields, both in mathematics and in other fields; for example, in communication theory, in computing and in statistics. Technological breakthroughs like space and satellite communications, and guarding the privacy of information in data banks all depend in one way or another on the use of finite fields.

Definition 1.6. A finite field is a field with a finite number of elements.

Example 1.1. For every prime p, the residue class ring

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$$

forms a finite field with p elements, which we denote by $\mathbb{F}_p$.

Remark 1.1. The fact that

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!} \equiv 0 \bmod p$$

for all $i \in \mathbb{Z}$ with $1 \leq i \leq p-1$ along with Fermat's Little Theorem imply that, for any $a, b \in \mathbb{F}_p$, we have $a^p = a$ and

$$\begin{aligned} (a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \\ &= a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p \\ &= a^p + b^p \\ &= a + b. \end{aligned}$$

The prime field $\mathbb{F}_p$, also called the *Galois field* of order p, plays an important role in general field theory, since every field of characteristic p can be thought of as an extension of $\mathbb{F}_p$. We use the notation $\mathbb{F}_q$ for finite fields with q elements.

Theorem 1.8. [24] Let $\mathbb{F}_q$ be a finite field. Then, $\mathbb{F}_q$ has p^n elements, where the prime p is the characteristic of $\mathbb{F}_q$ and n is the degree of $\mathbb{F}_q$ over its prime subfield $\mathbb{F}_p$.

Theorem 1.9. [24] For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.

Proposition 1.3. [24] Let $\mathbb{F}_q$ be a finite field with q elements. Then, every $a \in \mathbb{F}_q$ satisfies $a^q = a$.

Proof. If $a = 0$, then $a^q = a$. On the other hand, the multiplicative group $\mathbb{F}_q^*$ has order $q-1$. Then, $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$, and the multiplication by a yields the desired result. □

1.1.4 Irreducible Polynomials and Splitting Fields

Definition 1.7. Let $f(x) \in \mathbb{F}_q[x]$ of degree $n \geq 1$. We say that $f(x)$ is irreducible over $\mathbb{F}_q$ if $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{F}_q[x]$ implies that either $g(x)$ or $h(x)$ is a constant polynomial.

Theorem 1.10. [24] For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.

Theorem 1.11. [24] Let R be a commutative ring with identity. If R is a principal ideal domain, then $R/(c)$ is a field if and only if c is a prime element of R.

Since $\mathbb{F}_q$ is a field and the commutative ring $\mathbb{F}_q[x]$ is a principal ideal domain, we have the following result.

Theorem 1.12. [24] Let $f(x) \in \mathbb{F}_q[x]$. The residue class ring $\mathbb{F}_q[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over $\mathbb{F}_q$.

Proof. Note that the ring $\mathbb{F}_q[x]$ is a *Euclidean domain*. Therefore, the *Euclidean division* and the *Bézout's identity* for polynomials hold in $\mathbb{F}_q[x]$, i.e., for any nonzero polynomials $g(x), h(x) \in \mathbb{F}_q[x]$, there exist nonzero polynomials $u(x), v(x) \in \mathbb{F}_q[x]$ such that

$$u(x)g(x) + v(x)h(x) = \gcd(g(x), h(x)).$$

If $\mathbb{F}_q[x]/(f(x))$ is a field and $f(x) = g(x)h(x)$ is reducible, with $1 \leq \deg(g(x)), \deg(h(x)) \leq \deg(f(x))$, then both $g(x) + f(x)$ and $h(x) + f(x)$ are nonzero and not invertible in $\mathbb{F}_q[x]/(f(x))$, a contradiction. The other implication is a consequence of the Bézout's identity. □

Remark 1.2. In order to construct $\mathbb{F}_{q^n}$, we need an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then, let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n, Theorem 1.12 implies that

$$\mathbb{F}_q[x]/(f(x)) = \{h(x) \bmod f(x) : h(x) \in \mathbb{F}_q[x] \text{ and } \deg(h) < n\}$$

is a field with q^n elements which we denote by $\mathbb{F}_{q^n}$.

Example 1.2. Consider the irreducible polynomial $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$. Then, the field $\mathbb{F}_4 = \mathbb{F}_{2^2}$ can be represented by the field

$$\mathbb{F}_2[x]/(f(x)) = \{a + bx \mod f(x) : a, b \in \mathbb{F}_2\}.$$

Definition 1.8. If $f(x)$ is irreducible over $\mathbb{F}_q$ of degree n, then the field $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$ is called the *splitting field* of $f(x)$ over $\mathbb{F}_q$.

For $a_1, a_2, \ldots, a_r \in \mathbb{F}_{q^n}$, we denote by $\mathbb{F}_q(a_1, a_2, \ldots, a_r)$ the smallest subfield of $\mathbb{F}_{q^n}$ containing both $\mathbb{F}_q$ and $a_1, a_2, \ldots, a_r$, that is, the extension of $\mathbb{F}_q$ obtained by adjoining $a_1, a_2, \ldots, a_r$ to $\mathbb{F}_q$. In particular, if α is a root of an irreducible polynomial $f(x)$, then we have

$$\mathbb{F}_q(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i \; : \; a_i \in \mathbb{F}_q \right\}.$$

Theorem 1.13. [24] Let $f \in \mathbb{F}_q[x]$ be irreducible of degree n. Then f has a root α in $\mathbb{F}_{q^n}$ and all roots of f in $\mathbb{F}_{q^n}$ are different and given by

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}} \in \mathbb{F}_{q^n}.$$

Proof. the polynomial f splits completely over $\mathbb{F}_{q^n}$ and it has n roots. Let β be some root of f. We now show that β^q is also a root of f. Let $f(x) = \sum_{i=0}^{n} a_i x^i$.

Using the fact that if $a_i \in \mathbb{F}_q$, then $a_i^q = a_i$ and Remark 1.1, we have

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + a_2(\beta^q)^2 + \ldots + a_n(\beta^q)^n \\ &= a_0^q + a_1^q\beta^q + a_2^q\left(\beta^2\right)^q + \ldots + a_n^q(\beta^n)^q \\ &= \left(a_0 + a_1\beta + a_2\beta^2 + \ldots + a_n\beta^n\right)^q \\ &= (f(\beta))^q = 0^q = 0. \end{aligned}$$

This shows that α and α^q are roots and thus also $\alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are roots of $f(x)$. If any two of these powers would coincide, e.g. $\alpha^{q^i} = \alpha^{q^j}$ for some $0 \leq i \leq j \leq n-1$, then we would have

$$\alpha^{q^{n+j-i}} = \alpha^{q^n} = \alpha,$$

and α would satisfy a polynomial of degree $n - j + i \leq n$ which contradicts the definition of α as root of an irreducible polynomial of degree n. □

Corollary 1.4. Let f be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n. Then the splitting field of f over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^n}$.

Corollary 1.5. Any two irreducible polynomials in $\mathbb{F}_q$ of the same degree have isomorphic splitting fields.

1.1.5 The Frobenius Automorphism

Definition 1.9. Let $\mathbb{F}_q$ be a finite field of characteristic p. The *Frobenius automorphism* of $\mathbb{F}_q$ is defined by

$$\begin{aligned} \phi : \mathbb{F}_q &\to \mathbb{F}_q \\ t &\mapsto t^p. \end{aligned} \tag{1.2}$$

We can extend ϕ to the following map :

$$\begin{aligned} \varphi : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ t &\mapsto t^q. \end{aligned}$$

Proposition 1.4. The map φ is an automorphism of $\mathbb{F}_{q^m}$ called, for convenience, the Frobenius automorphism.

Proof. Suppose that $q = p^n$, for some integer $n \geq 1$. For all $a, b \in \mathbb{F}_{q^m}$, we have

$$\begin{aligned} \varphi(a+b) = (a+b)^q &= ((a+b)^p)^{p^{n-1}} \\ &= (a^p + b^p)^{p^{n-1}} \\ &= (a^{p^2} + b^{p^2})^{p^{n-2}} \\ &\vdots \\ &= a^q + b^q \\ &= \varphi(a) + \varphi(b), \end{aligned}$$

and

$$\varphi(ab) = (ab)^q = a^q b^q = \varphi(a)\varphi(b).$$

Therefore, φ is a endomorphism of $\mathbb{F}_{q^m}$. On the other hand, we have

$$\ker(\varphi) = \{c \in \mathbb{F}_{q^m} : c^q = 0\} = \{0\},$$

so φ is injective. Finally, let $c \in \mathbb{F}_{q^m}$, then by Proposition 1.3 we have

$$\left(c^{q^{m-1}}\right)^q = c^{q^m} = c$$

. Hence, φ is surjective and thus φ is an automorphism of $\mathbb{F}_{q^m}$. □

Remark 1.3. Note that, the surjection of φ in the proof above could also be deduced from the fact that $\mathbb{F}_{q^m}$ is finite and φ is injective.

Theorem 1.14. [27] The distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are given by the maps $\varphi_0, \ldots, \varphi_{m-1}$ where

$$\begin{aligned} \varphi_i : \mathbb{F}_{q^m} &\to \mathbb{F}_{q^m} \\ a &\mapsto a^{q^i}. \end{aligned}$$

Remark 1.4. The set of automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ forms a group under composition. This group is called the *Galois group* of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is a cyclic group with generator φ, that is, $\varphi_i = \varphi^i$ for all $0 \leq i \leq m-1$.

1.2 Elliptic Curves

In this section we present the basic concepts from the theory of elliptic curves required for this thesis, which are taken, in large part, from [37] and [53].

1.2.1 Weierstrass Equation

An elliptic curve E is a smooth curve given by the graph of an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.3}$$

where $a_1, \ldots, a_6$ are constants. The Equation (1.3) is called the *generalized Weierstrass equation*. We will need to specify what set $a_1, a_2, a_3, a_4, a_6, x$, and y belong to. Usually, they are elements of a field, for example, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the rational numbers $\mathbb{Q}$, one of the finite fields $\mathbb{F}_p$ for a prime p, or one of the finite fields $\mathbb{F}_q$, where $q = p^n$ with $n \geq 1$. The generalized Weierstrass equation (1.3) is useful when working with fields of characteristic 2 and characteristic 3. If the characteristic of the field is not 2, then we can divide by 2 and complete the square:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

which can be written as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{1.4}$$

with $y_1 = y + a_1\frac{x}{2} + \frac{a_3}{2}$ and with some constants a_2', a_4', a_6'. If the characteristic is also not 3, then we can let $x_1 = x + \frac{a_2'}{3}$, then for some constants A and B we get

$$y_1^2 = x_1^3 + Ax_1 + B. \tag{1.5}$$

This will be referred to as the *Weierstrass equation*. We say that E is defined over $\mathbb{K}$, where $\mathbb{K}$ is a field and $A, B \in \mathbb{K}$. Let O denote the point at infinity that will be defined in Subsection 1.2.3. If we want to consider points with coordinates in some field $\mathbb{L} \supseteq \mathbb{K}$, we write $E(\mathbb{L})$. By definition, this set always contains the point at infinity O:

$$E(\mathbb{L}) = \{O\} \cup \left\{(x, y) \in \mathbb{L} \times \mathbb{L} \mid y^2 = x^3 + Ax + B\right\}.$$

It is not possible to draw meaningful pictures of elliptic curves over most fields. However, it is easy to graph the real locus of a Weierstrass equation. These have two basic forms, represented in Figure 1.1.

The cubic $y^2 = x^3 - 3x + 3$ In the first case and the cubic $y^2 = x^3 + x$ in the second case have only one real root. In the last case, the cubic $y^2 = x^3 - x$ has three distinct real roots.

In the general case, there can be no multiple root. Namely, we assume that

$$4A^3 + 27B^2 \neq 0.$$

If the roots of the cubic are x_1, x_2, x_3, then it can be shown that the discriminant of the cubic is

$$((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 = -(4A^3 + 27B^2).$$

Therefore, the roots of the cubic must be distinct.

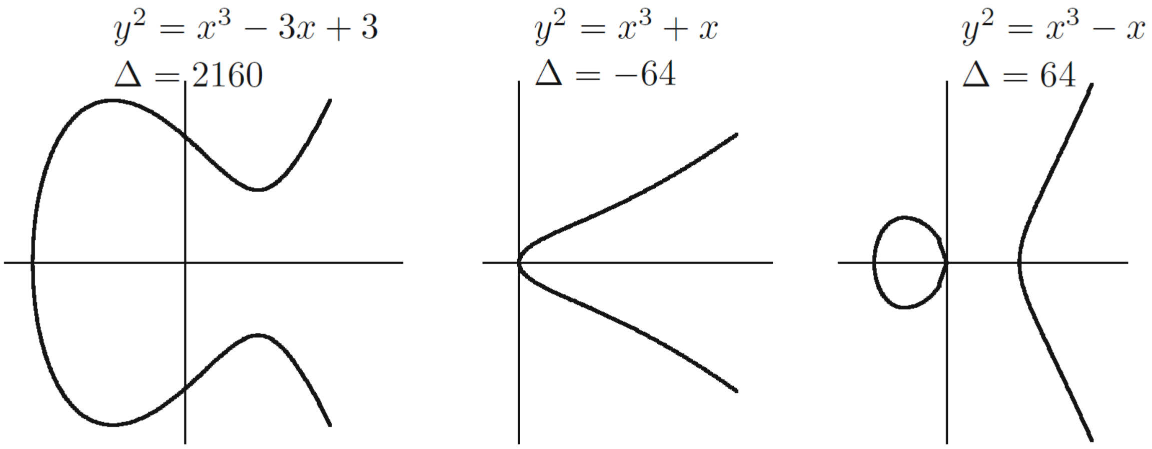

FIGURE 1.1: Three elliptic curves over $\mathbb{R}$

We have seen that in characteristics different from 2 and 3, any elliptic curve is given by the graph of a Weierstrass equation (1.5). However, in characteristic 3, there are also elliptic elliptic curves which are given by a Weierstrass equation (1.5). The two last examples in Figure 1.1 are elliptic curves on $\mathbb{F}_3$.

For technical reasons, it is useful to add a point at infinity to an elliptic curve. In Subsection 1.2.3, this concept will be made rigorous. However, it is easiest to regard it as a point (∞, ∞), usually denoted by O, sitting at the top of the y-axis. For computational purposes, it will be a formal symbol satisfying certain computational rules. For example, a line is said to pass through ∞ exactly when this line is vertical. The point O might seem a little unnatural, but we will see that including it has very useful consequences.

1.2.2 Group Law

Elliptic curves carry an interesting structure, namely their points form a group under a certain addition law that defined by the following rule:

Let $P, Q \in E$ be two points and L be the line connecting P and Q (tangent to E if $P = Q$), and let R be the third point of intersection of L with E. Let L' be the line connecting R and O, and a third point. We denote that third point by $P + Q$.

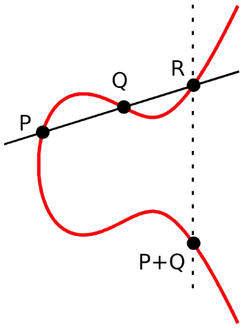

FIGURE 1.2: Addition on an elliptic curve

The addition law $+$ has the following properties:

Theorem 1.15. [37, Proposition 2.2]

1. If a line L intersects E at the (not necessarily distinct) points P, Q, R, then
$$(P+Q)+R=O.$$
2. $P+O=P$, for all $P \in E$.
3. $P+Q=Q+P$, for all $P, Q \in E$.
4. Let $P \in E$. There is a point of E, denoted by $-P$, satisfying
$$P+(-P)=O.$$
5. Let $P, Q, R \in E$. Then
$$(P+Q)+R=P+(Q+R).$$
In other words, the addition law $+$ makes E into an abelian group with identity element O. Further:
6. Suppose that E is defined over $\mathbb{K}$. Then
$$E(\mathbb{K})=\{O\} \cup \left\{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2+a_1 x y+a_3 y=x^3+a_2 x^2+a_4 x+a_6\right\}.$$
is a subgroup of E.

For $m \in \mathbb{Z}$ and $P \in E$, we let

$$[m]P=\underbrace{P+\cdots+P}_{m \text{ terms if } m>0}, \quad [m]P=\underbrace{-P-\cdots-P}_{|m| \text{ terms if } m<0}, \text{ and } \quad [0]P=O. \tag{1.6}$$

Now, we derive explicit formulas for the group operations on E. Let E be an elliptic curve given by the Weierstrass equation

$$F(x, y)=y^2+a_1 x y+a_3 y-x^3-a_2 x^2-a_4 x-a_6=0,$$

and let $P_0=(x_0, y_0) \in E$. In order to calculate $-P_0$, we take the line L through P_0 and O and find its third point of intersection with E. The line L is given by

$$L: x-x_0=0.$$

Substituting this into the equation for E, we see that the quadratic polynomial $F\left(x_0, y\right)$ has roots y_0 and y_0', where $-P=\left(x_0, y_0'\right)$. Writing out

$$F\left(x_0, y\right)=c\left(y-y_0\right)\left(y-y_0'\right),$$

and equating the coefficients of y^2 gives $c = 1$, and similarly equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$. This yields

$$-P_0 = -(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

Next we derive a formula for the addition law. Let

$$P_1 = (x_1, y_1) \quad \text{and} \quad P_2 = (x_2, y_2)$$

be points of E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then we have already shown that $P_1 + P_2 = O$. Otherwise the line L through P_1 and P_2 (or the tangent line to E if $P_1 = P_2$) has an equation of the form

$$L : y = \lambda x + \nu,$$

where the formulas for λ and ν are given below. Substituting the equation of L into the equation of E, we see that $F(x, \lambda x + \nu)$ has roots x_1, x_2, x_3, where $P_3 = (x_3, y_3)$ is the third point of $L \cap E$. Since we have

$$P_1 + P_2 + P_3 = O.$$

We write out

$$F(x, \lambda x + \nu) = x(x - x_1)(x - x_2)(x - x_3)$$

and equate coefficients. The coefficient of x^3 gives $c = -1$, and then the coefficient of x^2 yields

$$x_1 + x_2 + x_3 = \lambda^2 + a_a\lambda - a_2.$$

This gives a formula for x_3, and substituting into the equation of L gives the value of $y_3 = \lambda x_3 + \nu$.

Finally, to find $P_1 + P_2 = -P_3$, we apply the negation formula to P_3. All of this is summarized in the following:

Let E be an elliptic curve given by Equation (1.3), and let $P_1 + P_2 = P_3$, where $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$.

1. Let $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

If P_0 is on the curve described by the Weierstrass equation (1.5), then

$$-P = (x_0, -y_0).$$

2. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then

$$P_1 + P_2 = O.$$

Otherwise, λ and ν are defined by the following formulas:

- If $x_1 = x_2$, then

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},$$

and

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

- If $x_1 \neq x_2$, then λ and ν are given by

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$

and

$$\nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

Then $y = \lambda x + \nu$ is the line through P_1 and P_2, or tangent to E if $P_1 = P_2$.

3. With notation as in part 2, $P_3 = P_1 + P_2$ has coordinates

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

and

$$y_3 = -\left(\lambda + a_1\right)x_3 - \nu - a_3.$$

We have seen that if P is a point on an elliptic curve and k is a positive integer, then $[k]P$ is given by Relation 1.6. However, to compute $[k]P$ for a large integer k, it is inefficient to add P to itself repeatedly. It is much faster to use successive doubling. For example, to compute $[19]P$, we compute $[2]P$,

$$[4]P = [2]P + [2]P, \quad [8]P = [4]P + [4]P, \quad [16]P = [8]P + [8]P, \quad [19]P = [16]P + [2]P + P.$$

This method allows us to compute $[k]P$ for very large k, say of several hundred digits, very quickly. The only difficulty is that the size of the coordinates of the points increases very rapidly if we are working over the rational numbers. However, when we are working over a finite field, for example $\mathbb{F}_p$, this is not a problem because we can continually reduce mod p and thus keep the numbers involved relatively small. Note that the associative law allows us to make these computations without worrying about what order we use to combine the summands.

1.2.3 Projective Space and The Point at Infinity

We know that parallel lines meet at infinity. Projective space allows us to make sense out of this statement and also to interpret the point at infinity on an elliptic curve.

Let $\mathbb{K}$ be a field. Two-dimensional projective space $\mathbf{P}^2_{\mathbb{K}}$ over $\mathbb{K}$ is given by equivalence classes of triples (x, y, z) with $x, y, z \in \mathbb{K}$ and at least one of x, y, z nonzero. Two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are said to be equivalent if there exists a nonzero element $\lambda \in \mathbb{K}$ such that

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2).$$

We write $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. The equivalence class of a triple only depends on the ratios of x to y to z. Therefore, the equivalence class of (x, y, z) is denoted $(x : y : z)$.

If $(x : y : z)$ is a point with $z \neq 0$, then $(x : y : z) = (x/z : y/z : 1)$. These are the "finite" points in $\mathbf{P}^2_K$. However, if $z = 0$ then dividing by z should be thought of as giving infinity in either the x or y coordinate, and therefore the points $(x : y : 0)$ are called *the points at infinity* in $\mathbf{P}^2_{\mathbb{K}}$. The point at infinity on an elliptic curve will soon be identified with one of these points at infinity in $\mathbf{P}^2_{\mathbb{K}}$.

The two-dimensional *affine plane* over $\mathbb{K}$ is often denoted

$$\mathbf{A}^2_{\mathbb{K}} = \{(x, y) \in \mathbb{K} \times \mathbb{K}\}$$

We have an inclusion

$$\mathbf{A}^2_{\mathbb{K}} \hookrightarrow \mathbf{P}^2_K$$

given by

$$(x, y) \mapsto (x : y : 1).$$

In this way, the affine plane is identified with the finite points in $\mathbf{P}^2_{\mathbb{K}}$. Adding the points at infinity to obtain $\mathbf{P}^2_{\mathbb{K}}$ can be viewed as a way of "compactifying" the plane.

A polynomial is homogeneous of degree n if it is a sum of terms of the form $ax^iy^jz^k$ with $a \in \mathbb{K}$ and $i + j + k = n$. For example, $F(x, y, z) = 2x^3 - 5xyz + 7yz^2$ is homogeneous of degree 3 . If a polynomial F is homogeneous of degree n then $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ for all $\lambda \in \mathbb{K}$. It follows that if F is homogeneous of some degree, and $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, then $F(x_1, y_1, z_1) = 0$ if and only if $F(x_2, y_2, z_2) = 0$. Therefore, a zero of F in $\mathbf{P}^2_K$ does not depend on the choice of representative for the equivalence class, so the set of zeros of F in $\mathbf{P}^2_K$ is well defined.

If $F(x, y, z)$ is an arbitrary polynomial in x, y, z, then we cannot talk about a point in $\mathbf{P}^2_K$ where $F(x, y, z) = 0$ since this depends on the representative (x, y, z) of the equivalence class. For example, let $F(x, y, z) = x^2 + 2y - 3z$. Then $F(1, 1, 1) = 0$, so we might be tempted to say that F vanishes at $(1 : 1 : 1)$. But $F(2, 2, 2) = 2$ and $(1 : 1 : 1) = (2 : 2 : 2)$. To avoid this problem, we need to work with homogeneous polynomials.

If $f(x, y)$ is a polynomial in x and y, then we can make it homogeneous by inserting appropriate powers of z. For example, if $f(x, y) = y^2 - x^3 - Ax - B$, then we obtain the homogeneous polynomial $F(x, y) = y^2z - x^3 - Axz^2 - Bz^3$.

If F is homogeneous of degree n then

$$F(x, y, z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$$

and

$$f(x, y) = F(x, y, 1).$$

We can now see what it means for two parallel lines to meet at infinity.

Let

$$y = mx + b_1 \text{ and } y = mx + b_2$$

be two nonvertical parallel lines with $b_1 \neq b_2$. They have respectively the homogeneous forms

$$y = mx + b_1z \text{ and } y = mx + b_2z.$$

When we solve the simultaneous equations to find their intersection, we obtain $z = 0$ and $y = mx$. Since we cannot have all of x, y, z being 0, we must have $x \neq 0$. Therefore, we can rescale by dividing by x and find that the intersection of the two lines is

$$(x : mx : 0) = (1 : m : 0).$$

Similarly, if $x = c_1$ and $x = c_2$ are two vertical lines, they intersect in the point $(0 : 1 : 0)$. This is one of the points at infinity in $\mathbf{P}^2_{\mathbb{K}}$.

Now let us look at the elliptic curve E given by $y^2 = x^3 + Ax + B$. Its homogeneous form is $y^2z = x^3 + Axz^2 + Bz^3$. The points (x, y) on the original curve correspond to the points $(x : y : 1)$ in the projective version. To see what points on E lie at infinity, set $z = 0$ and obtain $0 = x^3$. Therefore $x = 0$, and y can be any nonzero number (recall that $(0 : 0 : 0)$ is not allowed). Rescale by y to find that $(0 : y : 0) = (0 : 1 : 0)$ is the only point at infinity on E. As we saw above, $(0 : 1 : 0)$ lies on every vertical line, so every vertical line intersects E at this point at infinity. Moreover, since $(0 : 1 : 0) = (0 : -1 : 0)$, the "top" and the "bottom" of the y-axis are the same.

1.2.4 Torsion Points

The torsion points, namely those whose orders are finite, play an important role in the study of elliptic curves. We will see in the next subsection for elliptic curves over finite fields, where all points are torsion points.

Let E be an elliptic curve defined over a field $\mathbb{K}$.

Definition 1.10. For a non-negative integer n, the set of n-torsion points of E, denoted by $E[n]$, is defined by

$$E[n] = \{P \in E(\bar{\mathbb{K}}) \mid [n]P = O\},$$

where $\bar{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$.

Notice that $E[n]$ is defined over $E(\bar{\mathbb{K}})$, not $E(\mathbb{K})$. It is easy to see that $E[n]$ is a subgroup of E. By definition, $O \in E[n]$ for all n.

We are interested in the case where the characteristic of $\mathbb{K}$ is not 2. In this case, E can be put in the form $y^2 =$ cubic, (see Equation 1.4) and it is easy to determine $E[2]$. Let

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

with $e_1, e_2, e_3 \in \bar{\mathbb{K}}$. A point P satisfies $[2]P = O$ if and only if the tangent line at P is vertical. It is easy to see that this means that $y = 0$, so

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Proposition 1.5. Let E be an elliptic curve over a field K. If the characteristic of $\mathbb{K}$ is not 2, then

$$E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

If the characteristic of $\mathbb{K}$ is 2, then

$$E[2] \simeq (0) \text{ or } \mathbb{Z}/2\mathbb{Z}.$$

The general situation is given by the following.

Theorem 1.16. Let E be an elliptic curve over a field $\mathbb{K}$ and let n be a positive integer. If the characteristic of $\mathbb{K}$ does not divide n, or is 0, then

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n.$$

If the characteristic of $\mathbb{K}$ is $p > 0$ and $p \mid n$, write $n = p^r n^{'}$ with $p \nmid n^{'}$.

Then

$$E[n] \simeq \mathbb{Z}_{n'} \times \mathbb{Z}_{n'} \text{ or } E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_{n'}.$$

1.2.5 Elliptic Curves over Finite Fields

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. The most important arithmetic quantity associated to such a curve is its number of rational points. Since there are only finitely many pairs (x, y) with $x, y \in \mathbb{F}_q$, the group $E(\mathbb{F}_q)$ is finite and then $E(\mathbb{F}_q)$ has approximately q points, with an error of no more than $2\sqrt{q}$. Let $\#E(\mathbb{F}_q)$ denote the order of $E(\mathbb{F}_q)$. The next theorem, which was conjectured by E. Artin and proven by Hasse in the 1930s, states an estimate for the number of points in $E(\mathbb{F}_q)$.

Theorem 1.17. (Hasse's Theorem) Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then

$$\left|\#E(\mathbb{F}_q) - q - 1\right| \leq 2\sqrt{q},$$

Theorem 1.18. [53] Let E be an elliptic curve over the field field $\mathbb{F}_q$. Then

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n,$$

for some integer $n > 1$. Or

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

for some integers $n_1, n_2 > 1$ with $n_1 \mid n_2$.

1.3 Generalized Fibonacci Sequences

In this section we give the definitions of some bi-periodic sequences such as the bi-periodic Fibonacci and Lucas sequences, the generalized bi-periodic Fibonacci sequence and the bi-periodic Horadam sequence. We also give some algebraic properties of these sequences, that will be useful throughout this thesis.

1.3.1 Bi-periodic Fibonacci and Lucas Sequences

The Fibonacci sequence has been generalized in different ways, by preserving the recurrence relation and altering the first two terms of the sequence, while others by preserving the first two terms of the sequence but altering the recurrence relation.

A generalization which has recently increased interest is the bi-periodic Fibonacci sequence introduced by Edson and Yayenie [13], by considering a non-linear recurrence relation depending on two non-zero real parameters defined as follows:

Definition 1.11. For any two nonzero real numbers a and b, the bi-periodic Fibonacci sequence $(q_n)_n$ is defined by

$$q_n = \begin{cases} aq_{n-1} + q_{n-2}, & \text{for } n \text{ even;} \\ bq_{n-1} + q_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad n \geq 2, \tag{1.7}$$

with initial conditions $q_0 = 0$ and $q_1 = 1$.

Many sequences in the literature are special cases of this sequence. The sequence descriptions that follow give reference numbers found in Sloane's On-Line Encyclopedia of Integer Sequences [39].

- The case $a = b = 1$ corresponds to the classical Fibonacci sequence A000045.
- The case $a = b = 2$ gives the Pell sequence A000129.
- For $a = b = k$, with some positive integer k, we obtain the k-Fibonacci sequence [14].

Similarly, Bilgici [8] defined the bi-periodic Lucas sequence using a non-linear recurrence relation depending on two non-zero real parameters defined as follows:

Definition 1.12. For any two nonzero real numbers a and b, the bi-periodic Lucas sequence $(l_n)_n$ is defined by

$$l_n = \begin{cases} bl_{n-1} + l_{n-2}, & \text{for } n \text{ even;} \\ al_{n-1} + l_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad n \geq 2, \tag{1.8}$$

with initial conditions $l_0 = 2$ and $l_1 = a$.

For particular values of a, b, we have some well-known companion sequences.

- If $a = b = 1$, we obtain the classical Lucas sequence A000032.
- If $a = b = 2$ then we have the Pell-Lucas sequence A002203.
- For $a = b = k$, with some positive integer k, we obtain the k-Lucas sequence [16].

Definition 1.13. The parity function of n is defined by

$$\xi_(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \text{ is odd.} \end{cases} \tag{1.9}$$

Here some properties of the parity function (1.9) which will be useful in the sequel.

$$\xi(m+n) = \xi(m) + \xi(n) - 2\xi(m)\xi(n); \tag{1.10}$$

$$\xi(m)\xi(n+1) = \frac{1}{2}\left(\xi(m) + \xi(n+1) - \xi(m+n+1)\right), \tag{1.11}$$

$$\xi(m) = m - 2\left\lfloor \frac{m}{2} \right\rfloor. \tag{1.12}$$

The Binet formula for the bi-periodic Fibonnaci sequence $(q_n)_n$ (see [13]) and the bi-periodic Lucas sequence $(l_n)_n$ (see [8]) are, respectively,

$$q_m = \frac{1}{a^{\lfloor \frac{m-1}{2} \rfloor} b^{\lfloor \frac{m}{2} \rfloor}} \left(\frac{\alpha^m - \beta^m}{\alpha - \beta} \right),$$

and

$$l_m = \frac{1}{a^{\lceil \frac{m}{2} \rceil} b^{\lfloor \frac{m+1}{2} \rfloor}} \left(\alpha^m + \beta^m \right),$$

with $\lfloor . \rfloor$ denotes the floor function and $\alpha = \frac{ab+\sqrt{a^2b^2+4ab}}{2}, \beta = \frac{ab-\sqrt{a^2b^2+4ab}}{2}$ are the roots of the quadratic equation

$$x^2 - abx + ab = 0.$$

The generating function for the bi-periodic Fibonnaci sequence $(q_n)_n$ and the bi-periodic Lucas sequence $(l_n)_n$ are, respectively,

$$\sum_{n\geq 0} q_n x^n = \frac{x(1+ax-x^2)}{1-(ab+2)x^2+x^4},$$

and

$$\sum_{n\geq 0} l_n x^n = \frac{2+ax-(ab+2)x^2+a^3}{1-(ab+2)x^2+x^4}.$$

A further generalization has been introduced in [34, 54] by preserving the initial conditions and modifying the recurrence relation (1.7) in such a way that the resulting sequence (1.13) depends on four real parameters using in a non-linear recurrence relation.

Definition 1.14. For any real numbers a, b, c, and d, the generalized bi-periodic Fibonacci sequence $(F_n)_n$ is defined by initial conditions $F_0 = 0, F_1 = 1$ and the following recurrence relation for $n \geq 2$

$$F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + dF_{n-2}, & \text{for } n \text{ odd.} \end{cases} \tag{1.13}$$

Many sequences in the literature are special cases of this sequence.

- If we take $a = b = p$ and $c = d = q$, we get the generalized Fibonacci sequence [26].
- If we take $a = b = 1$ and $c = d = 2$, we get the Jacobsthal sequence [20].
- If we take $a = b = k$ and $c = d = 2$, we get the k-Jacobsthal sequence [46].

The recurrence (1.13) involve the following relations, which reduce the odd and even subscripted sequences to the kind of generalized Fibonacci sequence studied in [26].

$$F_{2n+1} = (ab + c + d)F_{2n-1} - cdF_{2n-3},$$

and

$$F_{2n} = (ab + c + d)F_{2n-2} - cdF_{2n-4}.$$

The generating function for the sequence $(F_n)_n$ is

$$F(x)=\sum_{n\geq 0}F_nx^n=\frac{x(1+ax-cx^2)}{1-(ab+c+d)x^2+cdx^4}.$$

Binet's formula for even and odd indices of the sequence $(F_n)_n$ is given by

$$\begin{aligned} F_{2n}&=a\frac{\alpha^n-\beta^n}{\alpha-\beta};\\ F_{2n+1}&=\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}-c\frac{\alpha^n-\beta^n}{\alpha-\beta}, \end{aligned} \tag{1.14}$$

here α and β are the roots of the quadratic equation

$$f(x)=x^2-(ab+c+d)x+cd=0. \tag{1.15}$$

That is

$$\alpha=\frac{(ab+c+d)+\sqrt{a^2b^2+c^2+d^2+2abc+2abd-2cd}}{2},$$

and

$$\beta=\frac{(ab+c+d)-\sqrt{a^2b^2+c^2+d^2+2abc+2abd-2cd}}{2}.$$

So that,

$$\alpha+\beta=ab+c+d \text{ and } \alpha\cdot\beta=cd. \tag{1.16}$$

In the following theorem, we list a number of properties including generalizations of Cassini's, Catalan's and d'Ocagne's identities for the classical Fibonacci numbers.

Theorem 1.19. [54] Suppose that $c=d$. Then the sequence $(F_n)_n$ satisfies the following identities:

(a) Cassini's Identity:

$$(a/b)^{\xi(n+1)}F_{n+1}F_{n-1}=(a/b)^{\xi(n)}F_n^2-(a/b)(-c)^{n-1}.$$

(b) Catalan's Identity:

$$(a/b)^{\xi(n+m)-\xi(m)}F_{n+m}F_{n-m}-(b/a)^{\xi(n)-\xi(m)}F_n^2=(-1)^{n-m+1}c^{n-r}F_m^2.$$

(c) d'Ocagne's Identity:

$$a^{\xi(mn+m)}b^{\xi(mn+n)}F_mF_{n+1}-a^{\xi(mn+n)}b^{\xi(mn+m)}F_nF_{m+1}=a^{\xi(m-n)}(-c)^nF_{m-n}. \tag{1.17}$$

(d) Binomial Sum:

$$\sum_{k=0}^{m}\binom{m}{k}a^{\xi(k)}(ab)^{\lfloor\frac{k}{2}\rfloor}c^{m-k}F_k=F_{2m}.$$

The following theorem contain some additional properties of $(F_n)_n$ that will be needed in Chapter 2.

Theorem 1.20. [44] Suppose that $c = d$. Then the sequence $(F_n)_{n\geq 0}$ satisfies the following identities:

(i) $(b/a)^{\xi(ij+i)}F_jF_{i+1} + (b/a)^{\xi(ij+j)}cF_iF_{j-1} = F_{j+i} \qquad (g \geq 1, n \geq 0).$

(ii) $(b/a)^{\xi(ng+n)}F_nF_{g+1} + (b/a)^{\xi(ng+g)}F_{n+1}F_g = (-c)^g F_{n-g} \qquad (g \geq 0, n \geq 0).$

1.3.2 Bi-periodic Horadam Sequence

The second order recurrence sequence has been generalized in two ways mainly, by preserving the initial conditions or by preserving the recurrence relation. In 1965, Horadam [19] gave a sequence generated by the second-order linear homogeneous recurrence relation $h_n = sh_{n-1} + th_{n-2}$ for $n \geq 2$, with arbitrary initial conditions h_0 and h_1. This sequence is now called the Horadam sequence. Similar to the Fibonacci and Lucas sequences that were generalized as the Horadam sequence, the bi-periodic Fibonacci and Lucas sequences were generalized in [13] as follows:

Definition 1.15. Given nonzero real numbers a and b, the sequence $(Q_n)_n$ is defined by the recurrence relation

$$Q_n = \begin{cases} aQ_{n-1} + Q_{n-2}, & \text{for } n \text{ even;} \\ bQ_{n-1} + Q_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad n \geq 2, \tag{1.18}$$

and general initial conditions Q_0 and Q_1, where Q_0 and Q_1 are nonzero values.

Tan and Leung [44] introduced a further generalization of the sequence (1.18) defined as follows:

Definition 1.16. The bi-periodic Horadam sequence $(H_n)_{n\geq 0}$ is defined by

$$H_n = \begin{cases} aH_{n-1} + cH_{n-2}, & \text{for } n \text{ even;} \\ bH_{n-1} + cH_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad n \geq 2, \tag{1.19}$$

with arbitrary initial conditions H_0, H_1, where $H_0, H_1, a, b,$ and c are nonzero real numbers.

Several famous sequences in the literature can be stated in terms of the bi-periodic Horadam sequence. We list some of these sequences in Table 1.1.

Bi-periodic Horadam sequence	$H_n(H_0, H_1; a, b, c)$
Horadam sequence [19]	$H_n(H_0, H_1; a, a, b)$
Bi-periodic Lucas sequence [8]	$H_n(2, b; a, b, 1)$
Bi-periodic Jacobsthal Lucas sequence [47]	$H_n(2, b; a, b, 2)$
Pell-Lucas sequence A002203	$H_n(2, 2; 2, 2, 1)$
Lucas-balancing sequence A001541	$H_n(1, 3; 6, 6, -1)$
k-Fibonacci sequence [14]	$H_n(0, 1; k, k, 1)$
(p, q)-Fibonacci sequence [26]	$H_n(0, 1; p, q, 1)$
Pell sequence A000129	$H_n(0, 1; 2, 2, 1)$
Balancing sequence A001110	$H_n(0, 1; 6, 6, -1)$
Jacobsthal sequence [20]	$H_n(0, 1; 1, 1, 2)$
Bi-periodic Jacobsthal sequence [47]	$H_n(0, 1; a, b, 2)$
Bi-periodic Fibonacci sequence [13]	$H_n(0, 1; a, b, 1)$

TABLE 1.1: Special cases of the sequence $H_n = H_n(H_0, H_1; a, b, c)$.

The bi-periodic Horadam sequence will be studied in Chapter 4. We give in the following theorem an identity relating the terms of the sequence (1.13) for the case $c = d$ and the sequence $(H_n)_{n\geq 0}$, which will be crucial in our study.

Theorem 1.21. [44] Let n and l be any positive integers. Then we have

$$H_{n+l} = (b/a)^{\xi(n+1)\xi(l)} H_{l+1} F_n + c(b/a)^{\xi(n)\xi(l+1)} H_l F_{n-1}. \tag{1.20}$$

For more details on these sequences, we refer the reader to [4, 23, 45].

CHAPTER 2

THE GENERALIZED BI-PERIODIC FIBONACCI SEQUENCE MODULO m

For given positive integers a, b, c, and d, we let $(F_n)_n$ be the generalized bi-periodic Fibonacci sequence defined by the recurrence relation $F_n = aF_{n-1} + cF_{n-2}$ for n even and $F_n = bF_{n-1} + dF_{n-2}$ for n odd, with initial conditions $F_0 = 0$ and $F_1 = 1$. This chapter is devoted to the study the periodicity of $(F_n)_{n\geq 0}$ modulo a given integer $m \geq 2$ relatively prime to c and d. We extend some well-known results on the period and the rank of the classical Fibonacci sequence to the bi-periodic case.

2.1 Periodicity of The Generalized Bi-periodic Fibonacci Sequence Modulo m

We consider the generalized bi-periodic Fibonacci sequence. We assume that a, b, c, and d are positive integers.

$$F_0 = 0, \;\; F_1 = 1, \;\; \text{and} \;\; F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + dF_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad (n \geq 2). \tag{2.1}$$

Notice that for $c = d = 1$, $(F_n)_n$ reduces to the sequence (1.7). For the case $a = b$ and $c = d$, we have the generalized Fibonacci sequence [26].

In this section, we investigate the period of $(F_n)_n$ reduced modulo m. We Assume that m is chosen such that m is relatively prime to c and d, and we prove that $(F_n)_n$ reduced modulo m is periodic, i.e., there exists a positive integer r such that

$$F_{n+r} = F_n, \qquad \text{for all } n \geq 0. \tag{2.2}$$

Since we are dealing with the generalized bi-periodic Fibonacci sequences when reduced modulo m, then the condition $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$ ensures that the considered sequence are actually bi-periodic. For the case where $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the sequence $(F_n \bmod m)$ coincides with the the generalized Fibonacci sequence, see [25, 31, 49].

We show in the next theorem that the sequence $(F_n \bmod m)_n$ is periodic. Our proof follows the proof in the Wall paper [52].

Theorem 2.1. The sequence $(F_n)_n$ is periodic modulo m.

Proof. Since there are only m^2 pairs of integers modulo m, then at least one repetition of a pair must occur within the following m^2+1 pairs of the sequence

$$(F_0, F_1), (F_2, F_3), \ldots, (F_{2m^2}, F_{2m^2+1}).$$

Let i, j and r be integers such that $0 \leq i < j \leq m^2$ and $r = 2j - 2i$. Let $(F_{2i}, F_{2i+1}) \equiv (F_{2j}, F_{2j+1}) \pmod{m}$. It follows by induction that

$$F_{n+r} = F_n, \quad \text{for all } n \geq 2i.$$

Now, since c and d are invertible modulo m, by backward induction, we see that the sequence $(F_n)_n$ is periodic. Indeed, from the recurrence relation (2.1) we have

$$\begin{aligned}
F_{2i-1} &\equiv F_{2j-1} \bmod m,\\
F_{2i-2} &\equiv F_{2j-2} \bmod m,\\
&\vdots\\
F_{2j-2i+1} &\equiv F_{r+1} = F_1 \bmod m,\\
F_{2j-2i} &\equiv F_r = F_0 \bmod m.
\end{aligned}$$

□

Let $k(m)$ denote the period of the sequence $(F_n \bmod m)$, i.e., the least positive integer r that satisfies Property (2.2).

Example 2.1. We consider the generalized bi-periodic Fibonacci sequence generated by $a = 2$ and $b = c = d = 1$ that we find in A048788. The first few terms of this sequence reduced modulo $m = 3$ are

$$0, 1, 2, 0, 2, 2, 0, 2, 1, 0, 1, 1, \ldots.$$

Then we only have repetitions of these terms and $k(3) = 12$.

In [41], the authors investigated the period of the generalized bi-periodic Fibonacci sequences $(F_n)_n$ for the case $c = d = 1$. The period of $(F_n \bmod m)$ is defined to be the least positive integer r such that

$$\begin{cases} F_r \equiv 0 \pmod{m}; \\ \\ F_{r+1} \equiv 1 \pmod{m}. \end{cases}$$

However, unlike the case where $a = b$, the integer r does not necessarily satisfy Relation (2.2). We can see in Example 2.1 that we have $F_9 = 0$ and $F_{10} = 1$, however $r = 9$ is not the period of $(F_n \bmod 3)$ since $F_{r+2} \neq F_2$.

Theorem 2.2. Let r be a positive integer. If $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$, the following assertions are equivalent

(i) $F_{n+r} \equiv F_n$ (mod m) for all $n \geq 0$;

(ii) $(F_r, F_{r+1}, F_{r+2}, F_{r+3}) \equiv (F_0, F_1, F_2, F_3)$ (mod m);

(iii) $(F_r, F_{r+1}) \equiv (F_0, F_1)$ (mod m), and the integer r is even.

In particular, the period $k(m)$ is an even number.

Proof. It is immediate that $(i) \Longrightarrow (ii)$.

Next, let $(F_r, F_{r+1}, F_{r+2}, F_{r+3}) \equiv (F_0, F_1, F_2, F_3)$ (mod m), and suppose that r is an odd number. Then we have the following

$$a = F_2 \equiv F_{r+2} = bF_{r+1} + dF_r \equiv bF_1 + dF_0 = b,$$

and

$$bF_2 + dF_1 = F_3 \equiv F_{r+3} = aF_{r+2} + cF_{r+1} \equiv aF_2 + cF_1.$$

It follows that $a \equiv b$ mod m and $c \equiv d$ mod m, which contradict the assumptions. This shows that $(ii) \Longrightarrow (iii)$.

We now prove that $(iii) \Longrightarrow (i)$. Let $(F_r, F_{r+1}) \equiv (F_0, F_1)$ mod m, with r an even number. We show by induction that

$$F_{n+r} \equiv F_n (\mathrm{mod} m), \text{ for all } n \geq 0$$

For $n = 0$ we have $F_r \equiv F_0 (\mathrm{mod} m)$, and for $n = 1$ we have $F_{r+1} \equiv F_1$ mod m. Assume now that the formula holds for all positive integers up to n, in particular for n and $n - 1$. So, using the recurrence relation (2.1) and the fact that r is an even number, we obtain

$$F_{r+n+1} = \begin{cases} aF_{n+r} + cF_{r+n-1}, & \text{for } n \text{ odd ;} \\ bF_{n+r} + dF_{r+n-1}, & \text{for } n \text{ even .} \end{cases}$$

Now, we consider F_{r+n+1} modulo m. Using the induction hypothesis we obtain the following

$$F_{r+n+1} \equiv F_{n+1} (\mathrm{mod} m), \text{ for all } n \geq 1.$$

This proves that $F_{n+r} \equiv F_n (\mathrm{mod} m)$ for all $n \geq 0$, and complete the proof. □

If $a \not\equiv b$ (mod m) or $c \not\equiv d$ (mod m), then the period $k(m)$ is the smallest integer r satisfying the properties of Theorem 2.2. Furthermore, since any positive integer r that satisfies (2.2) is a multiple of the period $k(m)$. Hence, by Theorem 2.2 the following equivalence holds for any $r \in 2\mathbb{N}$:

$$k(m) \mid r \Longleftrightarrow \begin{cases} F_r \equiv 0 \pmod{m}; \\ \\ F_{r+1} \equiv 1 \pmod{m}. \end{cases} \tag{2.3}$$

The next theorem shows that we can reduce the computation of $k(m)$ to that of $k(p^e)$ for all prime power factor p^e of m. This is an analogue of [52, Theorem.2] for the case of the classical Fibonacci sequence.

Theorem 2.3. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the prime decomposition of m. Then

$$k(m) = \operatorname{lcm}(k(p_1^{e_1}), k(p_2^{e_2}), \ldots, k(p_s^{e_s})).$$

Proof. Our proof is similar to the proof of [52, Theorem. 2]. Let m be a positive integer, and let $m = \prod_{i=1}^{s} p_i^{e_i}$ be its prime factorization. Let $k_i = k(p_i^{e_i})$ denotes the period of $(F_n \bmod p_i^{e_i})$, and k denotes the period of $(F_n \bmod m)$. We prove that

$$k = \operatorname{lcm}(k_1, k_2, \ldots, k_s).$$

Since k is the period of $(F_n \bmod m)$, then we have

$$\begin{cases} F_k \equiv 0 \pmod{m}; \\ \\ F_{k+1} \equiv 1 \pmod{m}. \end{cases}$$

From the Chinese remainder Theorem, we have

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}.$$

Then for all $1 \leqslant i \leqslant s$,

$$\begin{cases} F_{k_i} \equiv 0 \pmod{p_i^{e_i}}; \\ \\ F_{k_i+1} \equiv 1 \pmod{p_i^{e_i}}. \end{cases}$$

For any $r \in \mathbb{N}$ the following congruences hold

$$\begin{cases} F_{rk_i} \equiv 0 \pmod{p_i^{e_i}}; \\ \\ F_{rk_i+1} \equiv 1 \pmod{p_i^{e_i}}. \end{cases}$$

We let $r = k_1 \times \cdots \times k_{i-1} \times k_{i+1} \times \cdots \times k_s$, and let $M = rk_i = \prod_{i=1}^{s} k_i$. We have

$$\begin{cases} F_M \equiv 0 \pmod{p_i^{e_i}}; \\ \\ F_{M+1} \equiv 1 \pmod{p_i^{e_i}}. \end{cases}$$

By the Chinese remainder theorem we obtain

$$\begin{cases} F_M \equiv 0 \pmod{m}; \\ \\ F_{M+1} \equiv 1 \pmod{m}. \end{cases}$$

Since $\operatorname{lcm}(k_i) \mid M$, then we conclude that $k(m) = \operatorname{lcm}(k(p_1^{e_1}), k(p_2^{e_2}), \ldots, k(p_s^{e_s}))$. □

Theorem 2.4. If $m \mid a$, then $k(m) = 2 \cdot \operatorname{ord}_m(d)$, where $\operatorname{ord}_m(d)$ is the order of d in $\mathbb{Z}_m^*$.

Proof. The first few terms of the sequence $(F_n)_n$ are

$$0, 1, a, ab + d, a(ab + d + c), a^2b^2 + 2abd + abc + d^2, \ldots.$$

Assume $a \equiv 0 \pmod{m}$, then following an induction we obtain the formula that gives the terms of the sequence reduced modulo m:

$$F_n \bmod m = \begin{cases} 0, & \text{if } n \text{ is even;} \\ d^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases} \tag{2.4}$$

Let $r = 2 \cdot \operatorname{ord}_m(d)$ be the least positive integer satisfying $F_r \equiv 0 \pmod{m}$ and $F_{r+1} \equiv 1 \pmod{m}$. Furthermore, using Relation (2.4) we obtain the following congruences for all n

$$F_{n+r} \bmod m = \begin{cases} 0, & \text{if } n \text{ is even;} \\ \\ d^{\operatorname{ord}_m(d) + \frac{n-1}{2}} = d^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Since r is the least positive integer such that $F_{n+r} \equiv F_n \bmod m$. Thus, we have $k(m) = 2 \cdot \operatorname{ord}_m(d)$. □

2.2 The Generalized Bi-periodic Fibonacci Sequence Over a Finite Field

Let $\mathbb{F}_q$ denote the finite field of order $q = p^e$ with $e \geq 1$, and p is an odd prime. We assume that $\gcd(c, p) = \gcd(d, p) = 1$ to guarantee that $(F_n)_n$ is periodic over the field $\mathbb{F}_q$. The main tool of our discussion is the Binet formula for even and odd indices given as follows

$$\begin{cases} F_{2n} = a\dfrac{\alpha^n - \beta^n}{\alpha - \beta}; \\ \\ F_{2n+1} = \dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} - c\dfrac{\alpha^n - \beta^n}{\alpha - \beta}. \end{cases} \tag{2.5}$$

Where $\alpha, \beta = \frac{A \pm \sqrt{\Delta}}{2}$ are the roots of the quadratic equation $f(x) = x^2 - Ax + B = 0$ with $A = ab + c + d$, $B = cd$, and Δ is the discriminant of $f(x)$.

In order to prove statements in $\mathbb{F}_q$, we start from $\mathbb{F}_p$, and generalize up to $\mathbb{F}_q$. The most important case to study is therefore $\mathbb{F}_p$. We establish a divisibility relation for $k(p)$ according to the nature of the polynomial f in $\mathbb{F}_p$. However, if $p \mid \Delta$ we obtain an equality statement for $k(p)$ in terms of the order of the zero of equation $f(x) = 0$ in $\mathbb{F}_p^*$. Finally, we consider the case of the period modulo p^e.

In the sequel, we deal only with the cases where $a \not\equiv b \pmod{p}$ or $c \not\equiv d \pmod{p}$. For analogous results in the case $a \equiv b \pmod{p}$ and $c \equiv d \pmod{p}$, see [25, 18, 31]. We also assume that $\gcd(a, p) = 1$, since when $p \mid a$ Theorem 2.4 gives $k(p) = 2 \cdot \mathrm{ord}_p(d)$, where $ord_p(d)$ is the order of d in $\mathbb{F}_p^*$.

Theorem 2.5. Let p be an odd prime. If Δ is a nonzero quadratic residue modulo p, then $k(p) \mid 2(p-1)$. Furthermore, $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right) = 1$ if and only if $k(p) \mid (p-1)$.

Proof. Suppose that Δ is a nonzero quadratic residue modulo p. Then we have $\alpha, \beta \in \mathbb{F}_p$, and by the Fermat little theorem we get

$$\alpha^{p-1} \equiv 1 \pmod{p} \text{ and } \beta^{p-1} \equiv 1 \pmod{p}.$$

Now, using the Binet formula for even and odd indices (2.5), we obtain

$$F_{2(p-1)} = a\frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} \equiv 0 \pmod{p},$$

and

$$F_{2(p-1)+1} = \frac{\alpha^p - \beta^p}{\alpha - \beta} - c\frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} \equiv 1 \pmod{p}.$$

Thus, by Relation (2.3), $k(p) \mid 2(p-1)$.

For the second part, we have the following equivalences:

$$F_{p-1} = a\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 0 \pmod{p} \Longleftrightarrow \alpha^{\frac{p-1}{2}} \equiv \beta^{\frac{p-1}{2}} \pmod{p},$$

and

$$F_p = \frac{\alpha^{\frac{p+1}{2}} - \beta^{\frac{p+1}{2}}}{\alpha - \beta} - c\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 1 \pmod{p} \Longleftrightarrow \alpha^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

So,

$$\alpha^{\frac{p-1}{2}} = \beta^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Longleftrightarrow \begin{cases} F_{p-1} \equiv 0 \pmod{p}; \\ \\ F_p \equiv 1 \pmod{p}. \end{cases}$$

Therefore, from (2.3) we get

$$\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right) = 1 \Longleftrightarrow k(p) \mid p-1.$$

□

Remark 2.1. Suppose that $c = d$, then from (1.16), we have $\alpha + \beta = ab + 2c$ and $\alpha\beta = c^2$. Moreover, since $(c, p) = 1$, then the Fermat little theorem gives $c^{p-1} \equiv 1 \pmod{p}$. Hence

$$(\alpha\beta)^{\frac{p-1}{2}} = c^{p-1} \equiv 1 \pmod{p}.$$

From part (a) and part (b) of Proposition 1.1, we obtain

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right) = (\alpha\beta)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Thus,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right).$$

Now, since $\alpha \in \mathbb{F}_p$ and using the fact that $\alpha\beta = c^2$ and $\alpha + \beta = ab + 2c$, we have

$$ab \equiv \alpha^{-1}(\alpha - c)^2 \pmod{p},$$

where α^{-1} is the inverse of α modulo p. It follows that

$$(ab)^{\frac{p-1}{2}} = (\alpha^{-1}(\alpha - c)^2)^{\frac{p-1}{2}} = \alpha^{\frac{p-1}{2}}(\alpha - c)^{p-1} \equiv \alpha^{\frac{p-1}{2}} \pmod{p}.$$

Thus,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{ab}{p}\right). \tag{2.6}$$

Remark 2.2. We mention that [41, Theorem. 4] is true only if we add the condition ab is also a quadratic residue modulo p. We illustrate this case in Example 2.2.

Now, if Δ is a quadratic nonresidue modulo p, thus the roots α, β are not in $\mathbb{F}_p$. That is, the polynomial $f(x)$ is irreducible over $\mathbb{F}_p$. We construct the splitting field of the polynomial $f(x)$.

$$\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x](f(x)).$$

Since the Frobenius automorphism of $\mathbb{F}_{p^2}$ fixes $\mathbb{F}_p$, it must permute the zeros of any irreducible quadratic polynomial of $\mathbb{F}_p[x]$. Therefore, by applying the Frobenius automorphism to α, a root of the equation $f(x) = 0$, we obtain the other root $\beta = \alpha^p$. Hence,

$$\alpha^{p+1} = \beta^{p+1} = \alpha\beta.$$

Now, we are ready to give a specific bound of $k(p)$ when Δ is a quadratic nonresidue modulo p.

Theorem 2.6. Let p be an odd prime. If Δ is a quadratic nonresidue modulo p, then $k(p) \mid 2 \cdot \mathrm{ord}_p(cd)(p+1)$.

Proof. Suppose that Δ is a quadratic nonresidue modulo p, then $\alpha^{p+1} = \beta^{p+1} = cd$. Using the Binet formula (2.5), we get

$$F_{2\,\mathrm{ord}_p(cd)(p+1)} = a\frac{(\alpha^{p+1})^{\mathrm{ord}_p(cd)} - (\beta^{p+1})^{\mathrm{ord}_p(cd)}}{\alpha - \beta} \equiv 0 \pmod{p},$$

and

$$F_{2\,\mathrm{ord}_p(cd)(p+1)+1} = \frac{\alpha(\alpha^{p+1})^{\mathrm{ord}_p(cd)} - \beta(\beta^{p+1})^{\mathrm{ord}_p(cd)}}{\alpha - \beta} \quad -c\frac{(\alpha^{p+1})^{\mathrm{ord}_p(cd)} - (\beta^{p+1})^{\mathrm{ord}_p(cd)}}{\alpha - \beta}$$

$$\equiv 1 \pmod{p}.$$

Therefore, Relation (2.3) implies that $k(p) \mid 2 \cdot \mathrm{ord}_p(cd)(p+1)$. □

Example 2.2. We take $a = c = d = 1$ and $b = 2$, and then $(F_n 0_n$ corresponds to A002530 in [39], So that, we have $\Delta = 12$.

Let $p = 11$. Then Δ is a nonzero quadratic residue and ab is a quadratic nonresidue. From Theorem 2.5 we have $k(p) \mid 2(p-1)$, with $k(p) \nmid (p-1)$. So, since $F_2 = 1$, we conclude that $k(11) = 20$.

Let $p = 7$, Δ is a quadratic nonresidue modulo p. Then by Theorem 2.6, we have $k(p) \mid 16$. We only have to calculating the first nine terms of the sequence reduced modulo 7

$$0, 1, 1, 3, 4, 4, 1, 6, 0, 6.$$

Thus, $k(7) = 16$.

Example 2.3. Take $a = 3, b = d = 1$, and $c = 4$. For $p = 11$ both Δ and ab are nonzero quadratic residues modulo p, and from Theorem 2.5 we have $k(p) | (p-1)$. Moreover, $k(p)$ is an even integer and F_2 mod $11 = 3$. So the only possible value is $k(11) = 10$.

We consider the case where $\Delta \equiv 0 \pmod{p}$, and investigate the period of the sequence $(F_n)_n$ reduced modulo p. We first need to simplify the Binet formula of F_n for even and odd indices (2.5) as follows:

$$F_{2n} = a\left(\alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \alpha\beta^{n-2} + \beta^{n-1}\right);$$

and

$$F_{2n+1} = \left(\alpha^n + \alpha^{n-1}\beta + \cdots + \alpha\beta^{n-1} + \beta^n\right) - c\left(\alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \alpha\beta^{n-2} + \beta^{n-1}\right).$$

It follows,

$$\begin{cases} F_{2n} = a\sum_{i=1}^{n}\alpha^{n-i}\beta^{i-1}; \\ F_{2n+1} = \alpha^n + \sum_{i=1}^{n}\alpha^{n-(i+1)}\beta^i(\alpha - c). \end{cases} \tag{2.7}$$

Since for the case where $\Delta \equiv 0 \pmod{p}$ the equation $f(x) = 0$ has a repeated root α in $\mathbb{F}_p$, it follows from (2.7) that the terms of the sequence $(F_n)_n$ reduced modulo p have the following form:

$$\begin{cases} F_{2n} \equiv an\alpha^{n-1} \pmod{p}; \\ F_{2n+1} \equiv (n+1)\alpha^n - cn\alpha^{n-1} \pmod{p}. \end{cases} \tag{2.8}$$

The above formula allows us to give an explicit equality statement for $k(p)$ in terms of the order of the root α in $\mathbb{F}_p^*$.

Theorem 2.7. Let p be an odd prime. If $\Delta \equiv 0$ (mod p), then $k(p) = 2p \cdot \mathrm{ord}_p(\alpha)$.

Proof. Assume that $\Delta \equiv 0$ (mod p) and $\gcd(a, p) = 1$. Working modulo p and using Relation (2.8), we obtain the following:

$$\begin{aligned} F_{2n} \equiv 0 \bmod p \text{ and } F_{2n+1} \equiv 1 \bmod p &\iff n\alpha^{n-1} \equiv 0 \bmod p \text{ and } \alpha^n \equiv 1 \bmod p \\ &\iff p \mid n \text{ and } \mathrm{ord}_p(\alpha) \mid n \\ &\iff \mathrm{lcm}(p, \mathrm{ord}_p(\alpha))| \; n \\ &\iff p \cdot \mathrm{ord}_p(\alpha) \mid n. \end{aligned}$$

The last congruence is due to the fact that $(\mathrm{ord}_p(\alpha), p) = 1$ since $\mathrm{ord}_p(\alpha) \mid p - 1$. From (2.3), we know that the period $k(p)$ is the least even integer k such that $F_k \equiv 0 \pmod{p}$ and $F_{k+1} \equiv 1 \pmod{p}$. Therefore, we get $k(p) = 2p \cdot \mathrm{ord}_p(\alpha)$. □

We have seen in Theorem 2.3 that it is easy to compute $k(m)$ once we know $k(p_i^e)$ for all prime power factors p_i^e of m. The corollary of the following theorem is crucial to the investigation of the period modulo p^e.

Theorem 2.8. Let p be a prime number and n be a positive integer. If $a \equiv 1 \pmod{p}$, then we have $a^{p^n} \equiv 1 \pmod{p^{n+1}}$.

Proof. Let $P(n)$ be the proposition

$$a^{p^n} \equiv 1 \pmod{p^{n+1}}.$$

Suppose that $a \equiv 1 \pmod p$, then we have $a = sp + 1$, for some $s \in \mathbb{Z}$.

For $n = 1$, we have

$$\begin{aligned} a^p &= (sp+1)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} (sp)^i \\ &= 1 + p^2 \sum_{i=2}^{p} \binom{p}{i} (sp)^{i-2} \\ &\equiv 1 \bmod p^2. \end{aligned}$$

Thus, $P(1)$ is true.

Assume that $P(n)$ is true up to some n and consider $P(n+1)$:

$$\begin{aligned} a^{p^{n+1}} &= (a^{p^n})^p \\ &= (sp^{n+1}+1)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} (sp^{n+1})^i \\ &= 1 + sp^{n+2} + \sum_{i=2}^{p} \binom{p}{i} (sp^{n+1})^i. \end{aligned}$$

Since $p^{n+2} \mid (sp^{n+1})^i$ for $2 \le i \le p$, it follows

$$a^{p^{n+1}} \equiv 1 \bmod p^{n+2}.$$

Hence $P(n)$ holds by induction. □

Corollary 2.1. Let p be an odd prime such that $\gcd(a, p) = 1$, and let e be a positive integer. Then

$$\alpha^{\frac{k(p)}{2}p^{e-1}} \equiv \beta^{\frac{k(p)}{2}p^{e-1}} \equiv 1 \pmod{p^e}.$$

Proof. Let α and β be the roots of the quadratic equation $f(x) = x^2 - (ab + c + d)x + cd = 0$.

- If $\Delta \equiv 0 \pmod p$, then we have $\alpha \equiv \beta \pmod p$. We know from Theorem 2.7 that $k(p) = 2p \cdot \mathrm{ord}_p(\alpha)$. Thus, it follows

$$\alpha^{\frac{k(p)}{2}} \equiv \beta^{\frac{k(p)}{2}} \equiv 1 \pmod p. \tag{2.9}$$

Thus, applying Theorem 2.8 to Relation 2.9, we get

$$\alpha^{\frac{k(p)}{2}p^{e-1}} \equiv \beta^{\frac{k(p)}{2}p^{e-1}} \equiv 1 \pmod{p^e}.$$

- Suppose that $\Delta \not\equiv 0 \pmod{p}$. We have

$$\begin{cases} F_{k(p)} \equiv 0 \pmod{p}; \\ F_{k(p)+1} \equiv 1 \pmod{p}. \end{cases}$$

Since $k(p)$ is even, then the Binet formula for even indices gives

$$a\frac{\alpha^{\frac{k(p)}{2}} - \beta^{\frac{k(p)}{2}}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Now, since $\gcd(a, p) = 1$ and $\gcd(\Delta, p) = 1$, then we obtain

$$\alpha^{\frac{k(p)}{2}} \equiv \beta^{\frac{k(p)}{2}} \pmod{p}.$$

Now, we use the last congruence in the Binet formula for odd indices

$$\begin{aligned} F_{k(p)+1} &= \frac{\alpha\alpha^{\frac{k(p)}{2}} - \beta\beta^{\frac{k(p)}{2}}}{\alpha - \beta} - c\frac{\alpha^{\frac{k(p)}{2}} - \beta^{\frac{k(p)}{2}}}{\alpha - \beta} \\ &\equiv \alpha^{\frac{k(p)}{2}}. \end{aligned}$$

It follows that $\alpha^{\frac{k(p)}{2}} \equiv \beta^{\frac{k(p)}{2}} \equiv 1 \pmod{p}$.

By applying Theorem 2.8 to $\alpha^{\frac{k(p)}{2}}$ and $\beta^{\frac{k(p)}{2}}$, we obtain the desired result.

□

Now that we have results helping in the calculation of $k(p)$. In Theorem 2.9 we connect $k(p)$ to $k(p^e)$.

Theorem 2.9. Let p be an odd prime such that $\gcd(a, p) = 1$, and let e be a positive integer. Then $k(p^e) \mid p^{e-1}k(p)$.

Proof. Suppose that $(a, p) = 1$. From Corollary 2.1, we have

$$\alpha^{\frac{k(p)}{2}p^{e-1}} \equiv \beta^{\frac{k(p)}{2}p^{e-1}} \equiv 1 \pmod{p^e}. \tag{2.10}$$

- If $\gcd(p, \Delta) = 1$, then using Relation 2.10 we have

$$F_{k(p)p^{e-1}} = a\frac{\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha - \beta} \equiv 0 \pmod{p^e},$$

and

$$F_{k(p)p^{e-1}+1} = \frac{\alpha\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta\beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha-\beta} - c\frac{\alpha^{\frac{k(p)p^{e-1}}{2}} - \beta^{\frac{k(p)p^{e-1}}{2}}}{\alpha-\beta}$$

$$\equiv 1 \pmod{p^e}.$$

- If $p \mid \Delta$, then we work modulo p using Relation 2.8

$$F_{k(p)p^{e-1}} \equiv ap^{e-1}\frac{k(p)}{2}\alpha^{\frac{k(p)p^{e-1}}{2}-1},$$

and

$$F_{k(p)p^{e-1}+1} \equiv \left(\frac{k(p)}{2}p^{e-1}+1\right)\alpha^{\frac{k(p)p^{e-1}}{2}} - cp^{e-1}\frac{k(p)}{2}\alpha^{\frac{k(p)p^{e-1}}{2}-1}.$$

Since from Theorem 2.7, we have $k(p) = 2p \cdot \operatorname{ord}_p(\alpha)$. Then

$$F_{k(p)p^{e-1}} \equiv ap^e \operatorname{ord}_p(\alpha)\alpha^{\frac{k(p)p^{e-1}}{2}-1},$$

and

$$F_{k(p)p^{e-1}+1} \equiv \left(\operatorname{ord}_p(\alpha)p^e+1\right)\alpha^{\frac{k(p)p^{e-1}}{2}} - cp^e \operatorname{ord}_p(\alpha)\alpha^{\frac{k(p)p^{e-1}}{2}-1}.$$

Thus, by (2.10) we obtain

$$\begin{cases} F_{k(p)p^{e-1}} \equiv 0 \pmod{p^e}; \\ \\ F_{k(p)p^{e-1}+1} \equiv 1 \pmod{p^e}. \end{cases}$$

Therefore, by (2.3) we have $k(p^e) \mid p^{e-1}k(p)$.

□

2.3 The Rank of The Generalized Bi-periodic Fibonacci Sequence Modulo m

Let $\gcd(c, m) = 1$. The rank of $(F_n)_n$ modulo m is the least positive integer r such that $F_r \equiv 0 \pmod{m}$. Let $d(m)$ denote the rank of $(F_n \bmod m)$. It is obvious that if $m \mid a$ then $d(m) = 2$. In the rest, we assume that $c = d$, and $m \nmid a$.

Wall [52, Theorem. 3] proved that the indices of the Fibonacci sequence terms that are zero modulo m form an arithmetic progression. In the following theorem we give an analogous result for the bi-periodic case.

Theorem 2.10. Let $\gcd(a, m) = 1$, then the terms for which $F_n \equiv 0 \pmod{m}$ have subscripts that form a simple arithmetic progression, i.e., $n = xl$; for $x = 0, 1, 2, \ldots$. Moreover, $l = d(m)$ gives all n with $F_n \equiv 0 \pmod{m}$.

Proof. Assume that $F_i \equiv 0 \pmod m$ and $F_j \equiv 0 \pmod m$. By setting $m = i$ and $n = j$ in the d'Ocagne identity 1.17, we have

$$a^{\xi(ij+i)}b^{\xi(ij+j)}F_iF_{j+1} - a^{\xi(ij+j)}b^{\xi(ij+i)}F_jF_{i+1} = a^{\xi(i-j)}(-c)^jF_{i-j}.$$

Since $\gcd(c,p) = \gcd(a,m) = 1$, then for $(i \geq j)$ we get

$$F_{i-j} \equiv 0 \pmod m. \tag{2.11}$$

Now, we consider the identity (i) of Theorem 1.20

$$F_{i+j} = (b/a)^{\xi(ij+j)}F_iF_{j+1} + (b/a)^{\xi(ij+i)}cF_jF_{i-1} \qquad (i \geq 1, j \geq 0).$$

It follows that

$$F_{i+j} \equiv 0 \pmod m. \tag{2.12}$$

Let

$$S = \{k \in \mathbb{Z}^* \mid F_k \equiv 0 \pmod m\}.$$

Since $F_{k(m)} \equiv 0 \pmod m$, the set S is not empty. Let d be the smallest integer in S. By using induction and congruence (2.12), we get $F_{ld} \equiv 0 \pmod m$ for $l \in \mathbb{Z}^*$. Now let $\lambda \in S$ and suppose that $d \mid \lambda$. Then there are two positive integers θ and γ such that $\lambda = d\theta + \gamma$ with $0 < \gamma < d$. From (2.11), we have $F_{\lambda-\theta d} = F_\gamma \equiv 0 \pmod m$. A contradiction, since d is the smallest integer in S. Thus, λ is a multiple of d. □

From Theorem 2.10, we have

$$F_n \equiv 0 \pmod m \Longleftrightarrow d(m) \mid n. \tag{2.13}$$

In particular, since $F_{k(m)} \equiv \pmod m$, then $d(m) \mid k(m)$.

Let $c = 1$ and $a, b \in \mathbb{F}_2$. Table 2.1 gives the rank of $(F_n \bmod 2)$.

a	b	c	$d(p)$
0	1	1	2
1	0	1	4

TABLE 2.1: p=2

We are now ready to state some fundamental results about the rank of $(F_n \bmod m)$.

Theorem 2.11. Let $m \geq 2$, and p be an odd prime such that $\gcd(a,p) = \gcd(c,p) = 1$. Then

(a) If Δ is a nonzero quadratic residue modulo p, then $d(p) \mid (p-1)$.

(b) If Δ is a quadratic nonresidue modulo p, then $d(p) \mid 2(p+1)$.

(c) If $\Delta \equiv 0 \pmod p$, then if $p \mid b$, $d(p) = 2p$ otherwise, $d(p) = p$.

(d) If $n \mid m$, then $d(n) \mid d(m)$.

(e) Let $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ be the prime decomposition of m. Then

$$d(m) = \operatorname{lcm}(d(p_1^{e_1}), d(p_2^{e_2}), \ldots, d(p_n^{e_n})).$$

Proof. Let p be an odd prime, and let $\gcd(a,p) = 1$.

(a) Suppose that Δ is a nonzero quadratic residue modulo p. Then $\alpha, \beta \in \mathbb{F}_p$ and from Relation 2.6, we have $\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right)$. Hence,

$$F_{p-1} = a\frac{\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Thus, by (2.13), we get $d(p) \mid (p-1)$.

(b) Suppose that Δ is a quadratic nonresidue modulo p. Then, $\alpha^{p+1} = \beta^{p+1} = \alpha\beta$ and we have

$$F_{2(p+1)} {=} a\frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} \equiv 0 \pmod{p}.$$

Thus, from (2.13), we get $d(p) \mid 2\,(p+1)$.

(c) Suppose that $\Delta \equiv 0$ (mod p).

If we assume that $p \mid b$, then we have $\alpha = c$. Using (2.8), we obtain

$$F_{2n} \equiv an(c)^{n-1} \text{ and } F_{2n+1} \equiv (c)^n.$$

Then we have $F_{2n+1} \not\equiv 0 \pmod{p}$, since $\gcd(c,p) = 1$ and $d(p)$ must be even. Note that we have $F_{2n} \equiv 0 \pmod{p}$ if and only if $p \mid n$. Therefore, we obtain $d(p) = 2p$.

Now, if $p \nmid b$ then we have $\alpha = -c$. Then

$$F_{2n} \equiv an(-c)^{n-1} \equiv 0 \pmod{m} \iff p \mid n$$

and

$$F_{2n+1} \equiv (2n+1)(-c)^n \equiv 0 \pmod{m} \iff p \mid (2n+1).$$

Since $d(p)$ is the smallest positive integer n for which $F_n \equiv 0 \pmod{p}$, we obtain $d(p) = p$.

(d) Since $F_{d(m)} \equiv 0$ (mod m) and $n \mid m$, then we have $F_{d(m)} \equiv 0$ (mod n). Thus, by (2.13), it follows that $d(n) \mid d(m)$.

For the proof of (e), see [48, Lemma 2].

□

CHAPTER 3

PERIODICITY OF THE GENERALIZED BI-PERIODIC FIBONACCI SEQUENCE USING MATRIX METHOD

The generalized bi-periodic Fibonacci sequence $(F_n)_{n\geq 0}$ reduced modulo an arbitrary positive integer have been studied in chapter 2 using modular arithmetic on its Binet formula for odd and even indices. In this chapter, we use the matrix approach to study the periodicity of $(F_n)_{n\geq 0}$. For a given positive integer m, we show that $(F_n \bmod m)_{n\geq 0}$ is periodic using matrix method. We investigate the behavior of the sequence $(F_n)_{n\geq 0}$ whose elements are in the finite field $\mathbb{F}_q$, where $q = p^e$ with $e \geq 1$ and p a prime.

3.1 Introduction

Matrix representation has played a very important role in the study of the properties of certain linear recurrent sequences. In [38], Silvester showed that a number of the properties of the Fibonacci sequence can be derived from a matrix representation. For more details, we refer to [22]. This approach, allowed to expressing explicitly the general term of certain linear recurrent sequence and derived many of the basic properties of these sequences, like the Pell sequence and the Stirling sequence; see [5, 15]. Robinson [29] defined the Fibonacci matrix

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

By induction on n, we have $(f_n, f_{n+1}) = (0, 1)U^n$ and the nth power U^n has the following matrix form

$$U^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}.$$

He used the matrix U in a novel approach to prove the results of Wall [52] on the periodicity of the Fibonacci sequence reduced modulo a given positive integer m. He established many other properties of the Fibonacci sequence and showed how the idea can be adapted to the study of more general recurrent linear sequences. The study of the periodicity of the recurrent linear sequences using matrix method has continued in recent years. In [18], the authors hve given alternative proofs of the Robinson results which also use the Fibonacci matrix U. Renault [31] investigated the periodicity of general second-order linear recurrence sequence by matrix method. Our purpose is to deal with the case of bi-periodic recurrence sequence.

Namely, the generalized bi-periodic Fibonacci sequence.

$$F_0 = 0,\ \ F_1 = 1,\ \text{ and }\ F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + dF_{n-2}, & \text{for } n \text{ odd,} \end{cases} \quad (n \geq 2). \tag{3.1}$$

With $a, b, c,$ and d are positive integers.

In Chapter 2, we investigated the periodicity of the sequence $(F_n)_{n\geq 0}$ defined over $\mathbb{Z}_m$, where m is a given positive integer. We established properties on the period and the rank of $(F_n \bmod m)_{n\geq 0}$, using modular arithmetic on the extended Binet formula (2.5).

In this chapter, we use the matrix approach to study the periodicity of the sequence $(F_n)_{n\geq 0}$. Considering an appropriate matrix representation

$$C = \begin{pmatrix} ab+d & bc \\ a & c \end{pmatrix},$$

we show that the study of the period of the sequence $(F_n)_{n\geq 0}$, whose elements are in $\mathbb{Z}_m$ is equivalent to the study of the period of the sequence $(C^n \bmod m)_{n\geq 0}$ over the group $GL_2(\mathbb{Z}_m)$. Then we investigate the behavior of $(F_n)_{n\geq 0}$ over the finite field of order $q = p^e$.

We have seen in Theorem 2.3 that we can simplify the problem of finding the period of $(F_n \bmod m)_{n\geq 0}$ by considering the prime factorization of m. Thus, combining knowledge of $k(p_i^e)$ with the fact that $k(m) = \operatorname{lcm}(k(p_i^{e_i}))$, one can obtain a bound on $k(m)$ for each positive integer m. However, in Theorem 2.9 we have obtained a divisibility relation between $k(p^e)$ and $k(p)$. Here, we complete this result and we show that we can express $k(p^e)$ in terms of $k(p)$.

3.2 Matrix Representation for The Sequence $(F_n)_{n\geq 0}$

Recently, several algebraic and combinatorial properties of the bi-periodic Fibonacci sequence and its generalizations were established by means of matrices; see [4, 36, 43]. In this chapter, we consider the matrix representation of $(F_n)_{n\geq 0}$ given in [43] as follows:

$$C = \begin{pmatrix} ab+d & bc \\ a & c \end{pmatrix}.$$

We have its trace and determinant defined by

$$tr(C) = ab + c + d \ \text{ and }\ \det(C) = cd.$$

Its nth power gives the following matrix:

$$C^n = \begin{pmatrix} F_{2n+1} & \frac{bc}{a}F_{2n} \\ F_{2n} & \frac{c}{a}(F_{2n} - dF_{2n-2}) \end{pmatrix}.$$

Using the above matrix representation, we give in the next lemma an identity which is useful in the computation of the terms of the sequence $(F_n)_n$ for a very large n, as well as for proving properties of this sequence.

Lemma 3.1. Let $C = \begin{pmatrix} ab+d & bc \\ a & c \end{pmatrix}$ be the matrix representation of the sequence $(F_n)_{n\geq 0}$. Set the vector $v_n = \begin{pmatrix} F_{2n+1} \\ F_{2n} \end{pmatrix}$. Then for all $n \geq 0$, we have $v_0 C^n = v_n$.

Proof. Relation (3.1) gives rise to the matrix equation $v_{n+1} = v_n C$, for $n \geq 0$. Thus, inductively we obtain $v_n = v_0 C^n$.

□

3.3 Periodicity by Matrix Method

In this section, we use the matrix approach to prove that the generalized bi-periodic Fibonacci sequence $(F_n)_n$ whose elements are in the ring $\mathbb{Z}_m$ is periodic. The proofs in this section follow those of [29]. Let C be an element of the finite group $GL_2(\mathbb{Z}_m)$. Then the entries of the matrix C^n are elements of the ring $\mathbb{Z}_m$, the desired objective of the study. In fact, the study of the period of sequence $(F_n)_n$ over $\mathbb{Z}_m$ is equivalent to the study of the period of the sequence $(C^n)_n$ over $GL_2(\mathbb{Z}_m)$. In particular, since there are only a finite number of distinct matrices in $GL_2(\mathbb{Z}_m)$, there are positive integers k and n, with $k+n > k > 0$ such that

$$C^{n+k} = C^k.$$

But since C has finite order in this group, this means that for some positive integer n, $C^n \equiv I \pmod{m}$, where I is the identity matrix.

We give in the next theorem the relationship between the period $k(m)$ and the order of C in $GL_2(\mathbb{Z}_m)$.

Theorem 3.1. Let $a \not\equiv b \pmod{m}$ or $c \not\equiv d \pmod{m}$. Let $\operatorname{ord}(C)$ denotes the multiplicative order of C in $GL_2(\mathbb{Z}_m)$. Then $\operatorname{ord}(C) = \frac{k(m)}{2}$, and we have

$$C^n = I \bmod m \text{ if and only if } k(m) \mid 2n. \tag{3.2}$$

Proof. Since $C \in GL_2(\mathbb{Z}_m)$, then there is a positive integer r such that $C^{n+r} = C^n$, for all $n \geq 0$. Then using Lemma 3.1, we get the following

$$\begin{aligned} C^{n+r} = C^n &\iff v_{n+r} = v_n \\ &\iff F_{2(n+r)+1} \equiv F_{2n+1} \pmod{m} \text{ and } F_{2(n+r)} \equiv F_{2n} \pmod{m} \\ &\iff F_{2r+n} \equiv F_n \bmod m, \text{ for all } n \geq 0. \end{aligned}$$

Note that $r = \operatorname{ord}(C)$ is the least integer satisfying $C^{n+r} = C^n$, for all $n \geq 0$. Moreover, the period $k(m)$ is the smallest integer satisfying $F_{n+k(m)} \equiv F_n \pmod{m}$, for all $n \geq 0$. Hence, we conclude that $\operatorname{ord}(c) = \frac{k(m)}{2}$. Indeed, from Theorem 2.2 we know that the period $k(m)$ is an even number, except in the case where $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. It follows that

$$C^n = I \text{ if and only if } k(m) \mid 2n.$$

□

Corollary 3.1. Let $\gcd(cd, m) = 1$, and let $\operatorname{ord}_m(cd)$ denotes the order of cd in $\mathbb{Z}_m^*$. Then

$$\operatorname{ord}_m(cd) \mid k(m).$$

Proof. Since $\det(C) = cd$ and $C^{k(m)} \equiv I \pmod{m}$, then we have

$$(cd)^{k(m)} = \det(C)^{k(m)} = \det(C^{k(m)}) \equiv 1 \pmod{m}.$$

It follows that, $\operatorname{ord}_m(cd) \mid k(m)$. □

3.4 Period of $(F_n)_{n\geq 0}$ Modulo Prime

Let $C \in GL_2(\mathbb{F}_p)$. We formulate a method with the aid of the matrix C for determining upper bound of the period of the sequence $(F_n)_n$ over the finite fields $\mathbb{F}_p$. Let $f_C(x) = \det(C - xI) = x^2 - (ab + c + d)x + cd \in \mathbb{F}_p[x]$ be the characteristic polynomial of the matrix C, and let Δ be its discriminant. If the matrix C is diagonalizable, with λ_1, λ_2 be its eigenvalues. Then we have

$$C = P \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} P^{-1},$$

where $P = \begin{pmatrix} \frac{\lambda_1 - c}{a} & \frac{\lambda_2 - c}{a} \\ 1 & 1 \end{pmatrix}$.
Then

$$C^n = P \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} P^{-1}.$$

Theorem 3.2. Let p be an odd prime. Assume that $p \nmid \Delta$. We have

i) If Δ is a quadratic residue modulo p, then $k(p) \mid 2(p-1)$. Furthermore, if $\left(\frac{\lambda_1}{p}\right) = \left(\frac{\lambda_2}{p}\right) = 1$ then $k(p) \mid p - 1$.

ii) If Δ is a quadratic nonresidue modulo p, then $k(p) \mid 2(p+1)\operatorname{ord}_p(cd)$.

Proof. i) Suppose that the discriminant Δ is a quadratic residue modulo p. So, the eigenvalues λ_1, λ_2 exist in $\mathbb{F}_p$ and are distinct. Then the matrix C is diagonalizable in $\mathbb{F}_p$. Thus, we have

$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \in GL_2(\mathbb{F}_p).$$

Applying the Fermat little theorem, we get $D^{p-1} \equiv I \pmod{p}$. Therefore, we have $C^{p-1} \equiv I \pmod{p}$. Thus, by (3.2), $k(p) \mid (p-1)$.

Now, suppose that $\left(\frac{\lambda_1}{p}\right) = \left(\frac{\lambda_2}{p}\right) = 1$. Using the properties of Legendre symbol, we get

$$D^{\frac{p-1}{2}} = \begin{pmatrix} \lambda_1^{\frac{p-1}{2}} & 0 \\ 0 & \lambda_2^{\frac{p-1}{2}} \end{pmatrix} = I.$$

It follows that $C^{\frac{p-1}{2}} = I$. Thus, by (3.2), we get $k(p) \mid p-1$.

ii) Suppose that Δ is a quadratic nonresidue modulo p. Then the eigenvalues λ_1, λ_2 are not in $\mathbb{F}_p$. Then the matrix C is not diagonalizable over $\mathbb{F}_p$. However, we can work in the field $\mathbb{F}_{p^2}$.

$$\mathbb{F}_{p^2} \simeq \mathbb{F}_p[\sqrt{\Delta}] = \{a_1 + a_2\sqrt{\Delta} \mid a_1, a_2 \in \mathbb{F}_p\}.$$

Since $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}$, then C is diagonalizable over the field $\mathbb{F}_{p^2}$.

We have

$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \in GL_2(\mathbb{F}_{p^2}).$$

Now, consider the Frobenius automorphism defined by

$$\begin{array}{rcccc} \varphi & : & \mathbb{F}_p[\sqrt{\Delta}] & \to & \mathbb{F}_p[\sqrt{\Delta}] \\ & & t & \mapsto & t^p. \end{array}$$

Under the automorphism φ, $\varphi(\lambda_1)$ and $\varphi(\lambda_2)$ must be roots of $\varphi(f_C(x))$. Since the coefficients of $f_C(x)$ are all in $\mathbb{F}_p$, then by the Fermat little theorem we get $\forall t \in \mathbb{F}_p, t^p = t$. Thus, the Frobenius automorphism φ fixes $f_C(x)$, and $\varphi(\lambda_1)$ and $\varphi(\lambda_2)$ are the roots of $f_C(x)$. However, $\lambda_1, \lambda_2 \notin \mathbb{F}_p$, and the equation $x^p = x$ has only p solutions so $\varphi(\lambda_1) \neq \lambda_1$ and $\varphi(\lambda_2) \neq \lambda_2$, but since $f_C(x)$ has only two roots, $\varphi(\lambda_1) = \lambda_2$ and $\varphi(\lambda_2) = \lambda_1$. Thus, we have

$$\lambda_2 = \lambda_1^p \text{ and } \lambda_1 = \lambda_2^p.$$

It follows that the diagonal matrix D has the following form:

$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^p \end{pmatrix} \in GL_2(\mathbb{F}_{p^2}).$$

Now, let

$$D^{(p+1)\operatorname{ord}_p(cd)} = \begin{pmatrix} \lambda_1^{(p+1)\operatorname{ord}_p(cd)} & 0 \\ 0 & \lambda_1^{p(p+1)\operatorname{ord}_p(cd)} \end{pmatrix}.$$

Since $\det(D) = \det(C) = cd = \lambda_1\lambda_2$, then we have $\lambda_1^{p+1} = cd$ and $\lambda_1^{p(p+1)} = (cd)^p$. Moreover, we have $cd \in \mathbb{F}_p$, then $(cd)^p = cd$. It follows that

$$D^{(p+1)\operatorname{ord}_p(cd)} = I.$$

Therefore, from (3.2) we have $k(p) \mid 2(p+1)\operatorname{ord}_p(cd)$.

□

Now, we consider the case where $p \mid \Delta$. The eigenvalues of the matrix C are not distinct so the matrix C is not diagonalizable. However, we can use the Jordan form of C. We get in the following theorem an explicit statement of the period $k(p)$, depending on the multiplicative order of λ, the eigenvalue of C.

Theorem 3.3. Let p be an odd prime. If $\Delta \equiv 0 \pmod p$, then $k(p) = 2p\operatorname{ord}_p(\lambda)$. In particular, we have $k(p) \mid 2p(p-1)$.

Proof. Suppose that $\Delta \equiv 0 \pmod p$. We consider the Jordan form $C = PJP^{-1}$, for some invertible P. Then we have

$$C = P\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} P^{-1}.$$

The form of the nth power of J is as follows

$$J^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}.$$

Working modulo p, we have $J^n = I$ if and only if $\lambda^n \equiv 1 \bmod p$, and $n\lambda^{n-1} \equiv 0 \bmod p$.

Then,

$$J^n = I \iff \operatorname{lcm}[\operatorname{ord}_p(\lambda), p] \mid n \iff p\operatorname{ord}_p(\lambda) \mid n.$$

The last equivalence is due to the fact that $\gcd(p, \operatorname{ord}_p(\lambda)) = 1$, since $\operatorname{ord}_p(\lambda) \leq p-1$. Moreover, since $C^n = I$ if and only if $J^n = I$, then $n = p\operatorname{ord}_p(\lambda)$ is the least positive integer satisfying $C^n = I$. Thus, from Theorem 3.1, we obtain $k(p) = 2p\operatorname{ord}_p(\lambda)$. □

Theorem 3.2 and Theorem 3.3 are given in Section 2.2 of Chapter 2 using modular arithmetic on the Binet formula of $(F_n)_n$ for even and odd indices (2.5). The most notable side of this section is the proof method.

3.5 On The period of $(F_n)_{n\geq 0}$ Modulo a Prime Power

Let $C \in GL_2(\mathbb{F}_q)$, $q = p^e$. We have seen in Theorem 2.9 that $k(p^e)$ divides $p^{e-1}k(p)$. The main result in this work, Theorem 3.4, shows that we can express $k(p^e)$ in terms of $k(p)$.

In the next lemma, we examine how the period of $(F_n)_{n\geq 0}$ changes as we reduce it modulo higher power of a given prime p.

Lemma 3.2. Let p be a prime. Let e and s be positive integers. Then we have the following:

1. If $p^e | p^s$, then $k(p^e) \mid k(p^s)$.
2. $k(p^{e+1}) = k(p^e)$ or $k(p^{e+1}) = pk(p^e)$.

3. Except for the single case $p = 2$ and $e = 1$, the following holds for any prime p and positive integer e:

$$\text{If } k(p^{e+1}) \neq k(p^e), \text{ then } k(p^{e+1}) \neq k(p^{e+2}).$$

Proof. 1. Let $C \in GL_2(\mathbb{F}_{p^s})$. From Theorem 3.1 we have $\operatorname{ord}(C) = \frac{k(p^s)}{2}$, it follows that $C^{\frac{k(p^s)}{2}} = I \pmod{p^s}$. Since $p^e | p^s$, then $C^{\frac{k(p^s)}{2}} = I \pmod{p^e}$. Thus, using Relation (3.2) we obtain $k(p^e) \mid k(p^s)$.

2. Let $C \in GL_2(\mathbb{F}_{p^e})$. Then $\frac{k(p^e)}{2}$ is the order of C in $GL_2(\mathbb{F}_{p^e})$. Thus, $C^n \equiv I \pmod{p^e}$, and we have $C^{\frac{k(p^e)}{2}} = I + p^e N$, where N is a 2 x 2 matrix with integer entries. Applying the binomial formula, we obtain the following statement:

$$C^{p\frac{k(p^e)}{2}} = \sum_{i=0}^{p} \binom{p}{i} (p^e N)^i. \tag{3.3}$$

Note that all of the terms of (3.3) except the first are congruent to $0 \pmod{p^{e+1}}$, thus $C^{p\frac{k(p^e)}{2}} \equiv I \pmod{p^{e+1}}$. From Theorem 3.1, we get $k(p^{e+1}) \mid pk(p^e)$. Moreover, part (a) gives $k(p^e) \mid k(p^{e+1})$. Thus, $k(p^{e+1})$ is either $pk(p^e)$ or $k(p^e)$.

3. Suppose that $k(p^{e+1}) \neq k(p^e)$. Then we have $C^{\frac{k(p^e)}{2}} = I + p^e M$, for some matrix M with integer entries not all of which are divisible by p. The binomial formula gives

$$C^{p\frac{k(p^e)}{2}} = I + \binom{p}{1} p^e M + \binom{p}{2} p^{2e} M^2 + \cdots + p^{pe} M^p. \tag{3.4}$$

Since $\binom{p}{1} p^e M \not\equiv 0 \pmod{p^{e+2}}$, by way of the nature of the matrix M. Then all the terms of (3.4) except the first two terms are divisible by p^{e+2}. It follows that $C^{p\frac{k(p^e)}{2}} \not\equiv I \pmod{p^{e+2}}$ so, $k(p^{e+2}) \neq pk(p^e)$. Moreover, since $k(p^{e+1}) \neq k(p^e)$, then part (b) gives $k(p^{e+1}) = pk(p^e)$. Therefore, we have $k(p^{e+1}) \neq k(p^{e+2})$.

□

The following theorem is an immediate consequence of Lemma 3.2.

Theorem 3.4. Let p be an odd prime, and let e be a given positive integer. Let e_0 be the largest positive integer such that $k(p^{e_0}) = k(p)$. Then we have for $1 \leq e \leq e_0$, $k(p^e) = k(p)$, and for $e > e_0$, $k(p^e) = p^{e-e_0} k(p)$.

Proof. Let e_0 be the largest positive integer such that $k(p^{e_0}) = k(p)$. In fact, the existence of e_0 is assured because if $C^{\frac{k(p)}{2}} \equiv I \pmod{p^e}$ for $e \geq 1$, then $C^{\frac{k(p)}{2}} = I$, which is impossible.

Since $k(p^{e_0}) = k(p)$, then for $1 \leq e \leq e_0$, part (c) of Lemma 3.2 gives $k(p^e) = k(p)$. From the definition of e_0, we have that $k(p^{e_0+1}) \neq k(p^{e_0})$. Then using part (b) of Lemma 3.2, we obtain $k(p^{e_0+1}) = pk(p^{e_0}) = pk(p)$. Therefore, inductively applying the above procedure gives $k(p^e) = p^{e-e_0} k(p)$, for $e > e_0$. □

In the next example we illustrate the fact that once we know $k(p)$, it is easy to compute the period for all prime power factors p^e.

Example 3.1. Let $b = c = d = 1$, and $a = 2$. The generalized bi-periodic Fibonacci sequence $(F_n)_n$ corresponds to A048788 in [39].

The period of $(F_n)_n$ reduced modulo 3 is $k(3) = 12$. We easily verified that $k(3^2) \neq 12$ then for $p = 3$, the value of e_0 is 1. Hence, by the Theorem 3.4, $k(3^e) = 3^{e-1}k(3)$. For instance, we have $k(9) = 36$ and $k(27) = 108$.

CHAPTER 4

PERIODS OF THE BI-PERIODIC HORADAM SEQUENCE AND ELLIPTIC CURVES

In this chapter, we consider the bi-periodic Horadam sequence $(H_n)_{n\geq 0}$ defined by $H_n = \chi(n)H_{n-1} + cH_{n-2}$, where $\chi(n) = a$ if n is even and $\chi(n) = b$ if n is odd with arbitrary initial conditions H_0 and H_1, where a, b, and c are positive integers. We investigate the periods of the bi-periodic Horadam sequence modulo an integer $m > 1$. Moreover, we investigate the periods of the bi-periodic Horadam sequence associated to an elliptic curve E defined over the finite field $\mathbb{F}_p$, p a prime number.

4.1 Introduction

This work is motivated by papers that studied periods of linear recurrence sequence over elliptic curves. Firstly, Coleman et al. [10] investigated classical Fibonacci sequence on elliptic curves. In [2], the authors explored the case of Morgan-Voyce sequence over elliptic curves, and in [3] they extended the work to the Tribonacci sequence.

In this chapter, we extend this idea to the bi-periodic Horadam sequence over elliptic curves. Let E be a an elliptic curve over the finite field $\mathbb{F}_p$, where p is an odd prime. We define the bi-periodic Horadam sequence associated to the elliptic curve E as follows:

$$\mathbf{H}_n^{(U,V)} = \begin{cases} [a]\mathbf{H}_{n-1}^{(U,V)} + \mathbf{H}_{n-2}^{(U,V)}, & \text{for } n \text{ even;} \\ & \qquad\qquad (n \geq 2). \\ [b]\mathbf{H}_{n-1}^{(U,V)} + \mathbf{H}_{n-2}^{(U,V)}; & \text{for } n \text{ odd,} \end{cases} \tag{4.1}$$

With two points U and V on E as initial conditions.

We investigate the period of the bi-periodic Horadam sequence (4.2) modulo a positive integer m, and periods of the bi-periodic Horadam sequence on the elliptic curve E. We will see that the study of periods of the sequence $(\mathbf{H}_n^{(U,V)})_{n\geq 0}$ is closely related to the study of periods of the generalized bi-periodic Fibonacci sequence $(F_n)_{n\geq 0}$.

4.2 Periods of The Bi-periodic Horadam Sequence Modulo m

Let a, b and c be positive integers. The bi-periodic Horadam sequence is defined by the following recurrence relation:

$$H_n = \begin{cases} aH_{n-1} + cH_{n-2}, & \text{for } n \text{ even;} \\ & \qquad\qquad (n \geq 2) \\ bH_{n-1} + cH_{n-2}, & \text{for } n \text{ odd,} \end{cases} \tag{4.2}$$

with initial conditions $H_0 = u$ and $H_1 = v$, where u, v are integers.

Notice that for particular value $u = 2, v = b$ and $c = 1$, we have the bi-periodic Lucas sequence. If $u = 2, v = b$ and $c = 2$, we get the bi-periodic Jacobsthal Lucas sequence. Suppose that $c = d$. For the initial conditions $u = 0$ and $v = 1$, the sequence $(H_n)_n$ reduces to the generalized bi-periodic Fibonacci sequence:

$$F_0 = 0, \;\; F_1 = 1, \;\; \text{and} \;\; F_n = \begin{cases} aF_{n-1} + cF_{n-2}, & \text{for } n \text{ even;} \\ bF_{n-1} + cF_{n-2}, & \text{for } n \text{ odd.} \end{cases}$$

In the following lemma, we express terms of the sequence $(H_n)_n$ in terms of the sequence $(F_n)_{n\geq 0}$. It holds from the particular case $l = 0$ in Theorem 1.20.

Lemma 4.1. The sequence $(H_n)_{n\geq 0}$ satisfies the following

$$H_n = vF_n + uc(b/a)^{\xi(n)}F_{n-1}. \tag{4.3}$$

Let m be a positive integer such that $\gcd(m, c) = 1$. We investigate the periodicity of the bi-periodic Horadam sequence $(H_n)_n$ reduced modulo m.

Theorem 4.1. For positive integers a, b, c and m, such that $\gcd(c, m) = 1$, the bi-periodic Horadam sequence $(H_n)_{n\geq 0}$ reduced modulo m is periodic.

Proof. The same proof as for the generalized bi-periodic Fibonacci sequence $(F_n)_n$ holds; see the proof of Theorem 2.1. □

Let $k(u, v, m)$ denotes the period of the sequence $(H_n)_n$ reduced modulo m, which is the smallest positive integer l satisfying $H_{n+l} \equiv H_n \pmod{m}$, for all $n \geq 0$. Also, it is clear that every such l is a multiple of the period $k(u, v, m)$. Moreover, if l is an even number then we have

$$k(u, v, m) \mid l \iff \begin{cases} H_l \equiv u \pmod{m}, \\ H_{l+1} \equiv v \pmod{m}. \end{cases} \tag{4.4}$$

Example 4.1. We fix $a = c = 1, b = 2$ in Relation (4.2), and consider the initial conditions $u = 2, v = 3$. We give in Table 4.1 some few terms of the corresponding bi-periodic Horadam sequence reduced modulo 7.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
H_n mod m	2	3	5	6	4	0	4	1	5	4	2	1	3	0	3	6	2	3

TABLE 4.1: Some few terms of $(H_n \bmod 7)_n$.

We have $H_{16} = 2$ and $H_{17} = 3$, which repeats the two initial conditions and then all terms repeat. So, the sequence $(H_n \pmod 7)_n$ is periodic, with $k(2,3,7) = 16$. Note that for $u = 0$ and $v = 1$ we have $k(7) = 16$, so $k(2,3,7) = k(7)$.

We summarize in the next lemma some properties of the period of the sequence $(F_n)_{n\geq 0}$ reduced modulo m given in Chapter 2, which will be needed later.

Lemma 4.2. [6] Let $\Delta = ab(ab + 4c)$ denotes the discriminant of the quadratic polynomial $f(x) = x^2 - (ab + 2c)x + c^2$. Let m be a given positive integer such that $\gcd(m, c) = 1$. Let p be an odd prime, with $p \nmid c$. We have

(a) If $\left(\frac{\Delta}{p}\right) = \left(\frac{ab}{p}\right) = 1$, then $k(p) \mid (p-1)$.

(b) If $\left(\frac{\Delta}{p}\right) = -1$, then $k(p) \mid 2(p+1)\operatorname{ord}_p(c^2)$.

(c) If $p \mid \Delta$, then $k(p) = 2p \operatorname{ord}_p(\theta)$, where θ is the repeated root of $f(x)$.

(d) Let $m = \Pi p_i^{e_i}$ be the prime decomposition of m. Then $k(m) = \operatorname{lcm}(k(p_i^{e_i}))$.

We show in the next proposition how $k(u,v,m)$ is related with $k(m)$. Then we make the connection between $k(u,v,m), k(u,0,m)$ and $k(0,v,m)$.

Proposition 4.1. Let m be a given positive integer such that $\gcd(m,c) = 1$, and $a \not\equiv b \pmod m$.

1. If $m \mid a$, then we have $k(u,v,m) \mid mk(m)$.
2. If $\gcd(a,m) = 1$, then $k(u,v,m) \mid k(m)$.
3. If $\gcd(v,m) = 1$, then $k(0,v,m) = k(m)$.
4. $k(u,v,m) \mid \operatorname{lcm}(k(u,0,m), k(0,v,m))$.

Proof. Let $k(m)$ be the period of $(F_n \bmod m)$.

1. Suppose that $m \mid a$, then the first few terms of $(H_n)_n$ modulo m are given below.

n	0	1	2	3	4	5	6	7	8
H_n mod m	q	r	cq	$bcq + cr$	c^2q	$c^2(2bq + r)$	c^3q	$c^3(3bq + r)$	c^4q

TABLE 4.2: Some few terms of $(H_n \bmod m)_n$, with $m \mid a$.

From Table 1, it follows by induction on n that the terms of the sequence $(H_n)_{n\geq 0}$ have the following form

$$H_n = \begin{cases} c^{\frac{n}{2}}u, & \text{for } n \text{ even;} \\ \\ c^{\frac{n-1}{2}}(\frac{n-1}{2}bu+v), & \text{for } n \text{ odd.} \end{cases}$$

From Lemma 4.2(e), we have $k(m) = 2\operatorname{ord}_m(c)$. Then $H_{mk(m)} = c^{m\operatorname{ord}_m(c)}u$ and $H_{mk(m)+1} = c^{m\operatorname{ord}_m(c)}(m\operatorname{ord}_m(c)bu+v)$. Thus,

$$\begin{cases} H_{mk(m)} \equiv u \pmod{m}; \\ \\ H_{mk(m)+1} \equiv v \pmod{m}. \end{cases}$$

By (4.4), we obtain $k(u,v,m) \mid mk(m)$.

2. Assume that $a \not\equiv b \pmod{m}$. The period $k(m)$ is an even number, by part (e) of Lemma 4.2. Then using Lemma 4.1, one gets

$$H_{k(m)} = vF_{k(m)} + cuF_{k(m)-1},$$

and

$$H_{k(m)+1} = vF_{k(m)+1} + uc(b/a)F_{k(m)}.$$

Since $F_{k(m)} \equiv 0 \pmod{m}, F_{k(m)+1} \equiv 1 \pmod{m}$ and $F_{k(m)-1} \equiv F_{-1} \pmod{m}$, where $cF_{-1} = F_1 - bF_0 = 1$. Moreover, we have $\gcd(a,m) = 1$. Then

$$\begin{cases} H_{k(m)} \equiv u \pmod{m}; \\ \\ H_{k(m)+1} \equiv v \pmod{m}. \end{cases}$$

Therefore, by (4.4), $k(u,v,m) \mid k(m)$.

3. Assume $u = 0$, then Lemma 4.1 gives $H_n = rF_n$. Since $\gcd(v,m) = 1$, it follows that for any $i,j \in \mathbb{N}$, $F_i \equiv F_j \pmod{m}$ if and only if $vF_i \equiv vF_j \pmod{m}$.

   Thus,

$$F_i \equiv F_j \pmod{m} \Longleftrightarrow H_i \equiv H_j \pmod{m}.$$

   Therefore, we get $k(0,v,m) = k(m)$.

4. Let $\delta = \operatorname{lcm}(k(u,0,m), k(0,v,m))$. From Lemma 4.1, we have

$$H_{\delta+n} = vF_{\delta+n} + uc(b/a)^{\xi(\delta+n)}F_{\delta+n-1}.$$

Since $k(0,v,m) \mid \delta$ and $k(0,v,m) \mid \delta$, it follows that for all $n \geq 0$,

$$H_{\delta+n} \equiv vF_n + +uc(b/a)^{\xi(n)}F_{n-1} \pmod{m}.$$

Thus for all $n \geq 0$, we obtain

$$H_{\delta+n} \equiv H_n \bmod m.$$

We deduce that δ is a period of $(H_n \bmod m)_n$.

Therefore, we have $k(u,v,m) \mid \delta = \operatorname{lcm}(k(u,0,m), k(0,v,m))$.

□

4.3 Bi-periodic Horadam Sequence on Elliptic Curves

Let $E : y^2 = x^3 + \alpha x + \beta$ be a non-singular elliptic curve over the finite field $\mathbb{F}_p$, where p is an odd prime. Let

$$E(\mathbb{F}_p) = \{O\} \cup \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p | y^2 = x^3 + \alpha x + \beta\}.$$

Let a and b be positive integers. Given two points U and V on $E(\mathbb{F}_p)$. We define the bi-periodic Horadam sequence associated to the elliptic curve E, denoted by $(\mathbf{H}_n^{(U,V)})_{n\geq 0}$, as follows:

$$\mathbf{H}_n^{(U,V)} = \begin{cases} [a]\mathbf{H}_{n-1}^{(U,V)} + \mathbf{H}_{n-2}^{(U,V)}, & \text{for } n \text{ even;} \\ & \\ [b]\mathbf{H}_{n-1}^{(U,V)} + \mathbf{H}_{n-2}^{(U,V)}; & \text{for } n \text{ odd,} \end{cases} \quad \text{for } \; n \geq 2, \tag{4.5}$$

and initial conditions $\mathbf{H}_0^{(U,V)} = U, \mathbf{H}_1^{(U,V)} = V$.

We consider the non-singular elliptic curve $E : y^2 = x^3 + 7$ over the field $\mathbb{F}_5$. Then

$$E(\mathbb{F}_5) = \{O\} \cup \{(2,0), (3,3), (3,2), (4,1), (4,4)\}$$

Let $a = 1, b = 2$, and $V = (4,1) \in E(\mathbb{F}_5)$. We let $(\mathbf{H}_n^{(O,V)})_{n\geq 0}$ be the bi-periodic Horadam sequence associated to E.

We list down the first few terms of $\mathbf{H}_n^{(O,V)}$:

$$O,\ (4,1),\ (4,1),\ (2,0),\ (3,2),\ (4,4),\ (2,0),\ (4,4),\ (3,3),\ (2,0),\ (4,4),$$

$$(4,1),\ O,\ (4,1),\ (4,1),\ (2,0),\ (3,2),\ (4,4), \ldots$$

We can see that this sequence is periodic, since from $n = 12$ all terms repeat.

Now, we establish some basic properties of the sequence $(\mathbf{H}_n^{(U,V)})_{n\geq 0}$.

Proposition 4.2. Let U and V be two points on E. We have

(1) The sequence $(\mathbf{H}_n^{(U,V)})_n$ is given by

$$\mathbf{H}_n^{(U,V)} = [F_n]V + [(b/a)^{\xi(n)} F_{n-1}]U.$$

(2) If $U = O$, then $\mathbf{H}_n^{(U,V)} = [F_n]V$.

(3) The sequence $(\mathbf{H}_n^{(U,V)})_n$ is periodic.

Proof. (1) This is follows from a straightforward induction.

(2) This is a special case of part (1) with $U = O$.

(3) The proof follows from an argument similar to the proof of Theorem 2.1 using the fact that an elliptic curve over a finite field has only finitely many points with coordinates in that finite field.

□

In the sequel, we will need the following lemmas.

Lemma 4.3. If $n \mid m$, then $k(n) \mid k(m)$.

Proof. Since $F_{k(m)+n} \equiv F_n \pmod{m}$, for $n \geq 0$ and $n \mid m$, then we have $F_{k(m)+n} \equiv F_n \pmod{n}$. Thus, $k(n) \mid k(m)$. □

Let $h = \#E(\mathbb{F}_p)$ denotes the order of the group $E(\mathbb{F}_p)$. If $[k]P = O$ for some minimal k, then k is the order of P in $E(\mathbb{F}_p)$. Let $h_P = \operatorname{ord}(P)$ denotes the order of any point $P \in E(\mathbb{F}_p)$.

Lemma 4.4. Let P be a point in $E(\mathbb{F}_p)$. Let l and n be positive integers. We have,

$$[l]P = [n]P \quad \textit{if and only if} \quad l \equiv n \pmod{h_P}.$$

Proof. Since h_P is the order of P in the finite group $E(\mathbb{F}_p)$, then we have

$$[l]P = [n]P \quad \textit{if and only if} \quad [l-n]P = [0]P = O \quad \textit{if and only if} \quad l - n = kh_P, \quad k \in \mathbb{Z}.$$

□

Let $r = K(U, V, E)$ denotes the period of the sequence $(\mathbf{H}_n^{(U,V)})_n$. That is, the least positive integer satisfying $\mathbf{H}_{n+r}^{(U,V)} = \mathbf{H}_n^{(U,V)}$, for all $n \geq 0$. Every such r is a multiple of $K(U, V, E)$. Lemma 4.4 permit us to make the connection between periods of the sequence $(\mathbf{H}_n^{(U,V)})_n$ and periods of $(F_n \bmod m)_n$. We will see that the period of the sequence $(\mathbf{H}_n^{(O,V)})_n$ depends only on the order of the point V, such that all points of $E(\mathbb{F}_p)$ with the same order will generate sequence $(\mathbf{H}_n^{(O,V)})_n$ with exactly the same length.

Theorem 4.2. Let $a \not\equiv 0 \pmod{h_U}$. We have

1. $K(O, V, E) = k(h_V)$.

2. $K(U, O, E) \mid k(h_U)$.

3. $K(U, V, E) \mid \operatorname{lcm}[K(U, O, E), K(O, V, E)]$.

4. $K(U, V, E) \mid k(h)$.

Proof. 1. Assume that $U = O$. Then Proposition 4.2(2) gives $\mathbf{H}_n^{(O,V)} = [F_n]V$.

Now, using Lemma 4.4 we get

$$F_i \equiv F_j \pmod{h_V} \iff [F_i]V = [F_j]V,$$

for any $i, j \in \mathbb{N}$. Then,

$$F_i \equiv F_j \pmod{h_V} \iff \mathbf{H}_i^{(O,V)} = \mathbf{H}_j^{(O,V)}.$$

Therefore, $K(O, V, E) = k(h_V)$.

2. Let $l = k(h_U)$. We have $F_{n+l} \equiv F_n \pmod{h_U}$, for all $n \geq 0$.

Assume $a \not\equiv b \pmod{h_U}$, it follows from Theorem 2.2 that l is an even number. Then Property (1.10) gives

$$\xi(n + l) = \xi(n) + \xi(l) - 2\xi(n)\xi(l).$$

So, we get $\xi(n + l) = \xi(n)$. Thus,

$$F_{n+l} \equiv F_n \pmod{h_U} \implies (b/a)^{\xi(n+l)}F_{n+l} \equiv (b/a)^{\xi(n)}F_n \pmod{h_U}.$$

By Lemma 4.4, we get

$$(b/a)^{\xi(n+l)}F_{n+l} \equiv (b/a)^{\xi(n)}F_n \pmod{h_U} \iff [(b/a)^{\xi(n+l)}F_{n+l}]U = [(b/a)^{\xi(n)}F_n]U.$$

Therefore, for all $n \geq 0$ we have

$$F_{n+l} \equiv F_n \pmod{h_U} \implies [(b/a)^{\xi(n+l)}F_{n+l}]U = [(b/a)^{\xi(n)}F_n]U.$$

We conclude that $K(U, O, E) \mid k(h_U)$.

3. Let $\theta = \operatorname{lcm}(K(U, O, E), K(O, V, E))$. From the definition of $K(U, V, E)$ and Proposition 4.2(1), we have for any $n \in \mathbb{N}$,

$$\begin{cases} \mathbf{H}_{K(U,O,E)+n}^{(U,O)} = [(b/a)^{\xi(n)}F_{n-1}]U, \\ \\ \mathbf{H}_{K(O,V,E)+n}^{(O,V)} = [F_n]V. \end{cases}$$

Now, since $K(U,O,E) \mid \theta$ and $K(O,V,E) \mid \theta$, then for any $n \in \mathbb{N}$ we have $\mathbf{H}_{\theta+n}^{(U,O)} = [(b/a)^{\xi(n)}F_{n-1}]U$ and $\mathbf{H}_{\theta+n}^{(O,V)} = [F_n]V$. These facts and part (1) of Proposition 4.2 give

$$\mathbf{H}_{\theta+n}^{(U,V)} = \mathbf{H}_{n}^{(U,V)}.$$

Hence, $K(U,V,E) \mid \theta = \operatorname{lcm}(K(U,O,E), K(O,V,E))$.

4. Let $h_U = \operatorname{ord}(U)$, $h_V = \operatorname{ord}(V)$. We have $h_V \mid h$ and $h_U \mid h$. Then by Lemma 4.3, we get $k(h_V) \mid k(h)$ and $k(h_U) \mid k(h)$. The fact that $K(O,V,E) = k(h_V)$ and $K(U,O,E) \mid k(h_U)$ gives $K(O,V,E) \mid k(h)$ and $K(U,O,E) \mid k(h)$. Thus, the result follows from part (3).

□

Corollary 4.1. Let U and V be points on $E(\mathbb{F}_p)$. Suppose that $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, with integers $n_1, n_2 > 1$ such that $n_1 \mid n_2$. Then we have $K(U,V,E) \mid k(n_2)$.

Proof. Let U and $V \in E(\mathbb{F}_p)$. Using Theorem 1.18 and the fact that the order of any point in $E(\mathbb{F}_p)$ divides n_2, we have $h_V \mid n_2$ and $h_U \mid n_2$. Then from Lemma 4.3 it follows that $k(h_V) \mid k(n_2)$ and $k(h_U) \mid k(n_2)$.

Now, using the fact that $K(O,V,E) = k(h_V)$ and $K(U,O,E) \mid k(h_U)$ gives $K(O,V,E) \mid k(n_2)$ and $K(U,O,E) \mid k(n_2)$. Thus, the result follows from part 3 of Theorem 4.2. □

Since $k(ord(V))$ is equal to $K(O,V,E)$ and $k(ord(A))$ is a multiple of $K(O,V,E)$ when $a \not\equiv b \pmod{h_U}$. Then we can generalized some properties of the periods of the sequence $(F_n)_{n\geq 0}$ modulo a positive integer to the case of the sequence $(\mathbf{H}_n^{(O,V)})_{n\geq 0}$ and $(\mathbf{H}_n^{(U,O)})_{n\geq 0}$ on elliptic curves.

Theorem 4.3. Let U and V be points on $E(\mathbb{F}_p)$, and let $a \not\equiv b \pmod{h_U}$.

(a) If h_V is an odd prime and $\left(\frac{\Delta}{h_V}\right) = 1$, then $K(O,V,E) \mid 2(h_V - 1)$. If h_U is an odd primes and $\left(\frac{\Delta}{h_U}\right) = 1$, then $K(U,O,E) \mid 2(h_U - 1)$.

(b) If h_V is an odd prime and $\left(\frac{\Delta}{h_V}\right) = -1$, then $K(O,V,E) \mid 2(h_V + 1)$. If h_U is an odd prime and $\left(\frac{\Delta}{h_U}\right) = -1$, then $K(U,O,E) \mid 2(h_U + 1)$.

(c) If h_V is an odd prime and $h_V \mid \Delta$, then $K(O,V,E) = 2h_V \operatorname{ord}_{h_V}(\theta)$. If h_U is an odd prime and $h_U \mid \Delta$, then $K(U,O,E) \mid 2h_U \operatorname{ord}_{h_U}(\theta)$, where θ is the repeated root of the polynomial $x^2 - (ab+2)x + 1$.

(d) If h_U has prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$, then $K(O,V,E) = \operatorname{lcm}(k(p_i^{e_i}))$ and $K(U,O,E) \mid \operatorname{lcm}(k(p_i^{e_i}))$.

(e) If $h_U \mid h_V$, then $K(U,O,E) \mid K(O,V,E)$.

Proof. For (e) suppose that $h_U \mid h_V$. Lemma 4.3 gives $k(h_U) \mid k(h_V)$. From Theorem 4.2, we have $K(U,O,E) \mid k(h_U)$ and $k(h_V) = K(O,V,E)$. Thus, $K(U,O,E) \mid K(O,V,E)$.

For the others use the results of Theorem 4.2 in Lemma 4.2.

□

Conclusion and Perspectives

Along this thesis, we have given some necessary definitions and mathematical preliminaries. Then, we have investigated the periodicity of the generalized bi-periodic Fibonacci sequence when reduced modulo $m \geq 2$. We have extended some well-known results on the period and the rank of the classical Fibonacci sequence to the bi-periodic case. Afterwards, we have introduced the matrix method in the study of the periodicity of this sequence. We have shown that the study of the period of this sequence whose elements are in $\mathbb{Z}_m$ is equivalent to the study of the period of the sequence $(C^n)_{n\geq 0}$ over the group of invertible matrices with entries in $\mathbb{Z}_m$, where C is a matrix representation of the sequence. We have seen that this method permit to express the period modulo a power of prime $m = p^e$ in terms of the period modulo p, which allows to give bounds for the period for each positive integer m. Furthermore, we have first investigated the period of the bi-periodic Horadam sequence modulo a positive integer m. Next, we have defined the bi-periodic Horadam sequence associated to an elliptic curve E defined over the finite field $\mathbb{F}_p$, for p an odd prime, and we investigate its periodicity on E. Finally, we have shown that the study of periods of the bi-periodic Horadam sequence on an elliptic curve is closely related to the study of periods of the generalized bi-periodic Fibonacci sequence.

Some challenging questions are part of interest. As a first perspective, we are interested in the application of the results obtained in this work in cryptography.

Our second perspective is to explore the case of the k-periodic Fibonacci sequence [12], defined by a non-linear recurrence relation that depends on k real parameter:

$$u_n = \begin{cases} a_1 u_{n-1} + u_{n-2}, & \text{for } n \equiv 2 \pmod{k}; \\ a_2 u_{n-1} + u_{n-2}, & \text{for } n \equiv 3 \pmod{k}; \\ \vdots & \\ a_{k-1} u_{n-1} + u_{n-2}, & \text{for } n \equiv 0 \pmod{k}; \\ a_k u_{n-1} + u_{n-2}, & \text{for } n \equiv 1 \pmod{k}, \end{cases}$$

and initial conditions $u_0 = 0$ and $u_1 = 1$. As a first step, we would like to investigate the case of tri-periodic Fibonacci sequence obtain by setting $k = 3$.

BIBLIOGRAPHY

[1] N. R. Ait-amrane and H. Belbachir, Bi-periodic r-Fibonacci sequence and bi-periodic r-Lucas sequence of type s, *Hacettepe Journal of Mathematics and Statistics* **51** (2022), 680–699.

[2] L. Ait-Amrane, H. Belbachir, and K. Betina, Periods of Morgan-Voyce sequences and elliptic curves *Math. Slovaca* **6** (2016), 1267–1284.

[3] L. Ait-Amrane and H. Belbachir, Periods of Tribonacci sequences and elliptic curves, *Algebra Discrete Math.* **25** (2018), 17.

[4] J. Ascano, and E. Gueco, the bi-periodic Fibonacci-Horadam matrix, *Integers* **21** (2021), 21.

[5] H. Belbachir, and F. Bencherif, Linear recurrent sequences and powers of a square matrix, *Integers* **6** (2006), 17.

[6] H. Belbachir and C. Salhi, Generalized Bi-Periodic Fibonacci Sequence Modulo m, *Journal of Integer Sequences* **24** (2021), 13.

[7] H. Belbachir and C. Salhi, Periodicity of the generalized bi-periodic Fibonacci sequence using matrix method, submitted (2022).

[8] G. Bilgici, Two generalizations of Lucas sequence, *Applied Mathematics and Computation* **245** (2014), 526–538.

[9] Y. Bilu, C. A. Gómez, J. C. Gómez, and F. Luca, Elliptic curves over finite fields with Fibonacci numbers of points, *New York Journal of Mathematics* **26** (2020), 711–734.

[10] D. Coleman, A. Deidra, et al. Periods of (q, r)-Fibonacci sequences and elliptic curves, *Fibonacci Quarterly* **44** (2006), 59–70.

[11] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, Recurrence Sequences, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003, ISBN: 0-8218-3387-1.

[12] M. Edson, S. Lewis, and O. Yayenie, the k-periodic Fibonacci sequence and an extended Binet's formula, *Integers* **11** (2011), 739–751.

[13] M. Edson and O. Yayenie, A new generalization of Fibonacci sequences and extended Binet's formula, *Integers* **9** (2009), 639–654.

[14] S. Falcon and Á. Plaza, k-Fibonacci sequences modulo m, *Chaos, Solitons and Fractals* **41** (2009), 497–504.

[15] S. Falcón and Á. Plaza, On the Fibonacci k-numbers, *Chaos, Solitons and Fractals* **32** (2007), 1615–1624.

[16] S. Falcón and Á. Plaza, On the k-Lucas numbers, *International Journal of Contemporary Mathematical Sciences* **21** (2011), 1039–1050.

[17] J. B. Fraleigh, A First Course in Abstract Algebra, 7th ed., Addison Wesley, Boston, 2003.

[18] S. Gupta, P. Rockstroh, and F. E. Su, Splitting fields and periods of Fibonacci sequences modulo primes, *Math. Mag.* **85** (2012), 130–135.

[19] A.F. Horadam, Basic properties of a certain generalized sequence of numbers, *Fibonacci Quarterly* **3** (1965), 161–176.

[20] A.F. Horadam, Jacobsthal representation numbers, *significance* **2** (1996), 2–8.

[21] K. Ireland et M. Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics, Springer-Verlag, New York, 1990, ISBN0-387-97329-X.

[22] D. Kalman, Generalized Fibonacci numbers by matrix methods, *Fibonacci Quarterly* **20** (1982), 73–76.

[23] H. Leung and E. Tan, Some higher-order identities for generalized bi-periodic Horadam sequences, *The Korean Journal of Mathematics* **24** (2016), 681–691.

[24] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[25] H. C. Li, On second-order linear recurrence sequences, *Fibonacci Quarterly* **37** (1999), 342–349.

[26] E. Lucas, Théorie des fonctions numériques simplement périodiques, *American Journal of Mathematics* (1878), 289–321.

[27] G.L. Mullen, D. Panario, Handbook of Finite Fields, Taylor and Francis, Boca Raton, 2013.

[28] D. Panario, M. Sahin and Q. Wang, A family of Fibonacci-like conditional sequences, *Integers* **13** (2013), 1042–1055.

[29] D. W. Robinson, The Fibonacci matrix modulo m, *Fibonacci Quarterly* **1** (1963), 29–36.

[30] P. Ribenboim, An algorithm to determine the points with integral coordinates in certain elliptic curves, *J. Number Theory* **74** (1999), 19–38.

[31] M. Renault, The period, rank and order of the (a,b)-Fibonacci sequence mod m, *Math. Mag.* **86** (2013), 372–380.

[32] D. W. Robinson, The rank and period of a linear recurrent sequence over a ring, *Fibonacci Quarterly* **14** (1976), 210–214.

[33] J. Reynolds, Perfect powers in elliptic divisibility sequences, *J. Number Theory* **132** (2012), 998–1015.

[34] M. Sahin, The Gelin-Cesàro identity in some conditional sequences, *Hacet. J. Math. Stat.* **40** (2011), 855–861.

[35] C. Salhi and H. Belbachir, Periods of the bi-periodic Horadam sequence and elliptic curves, submitted (2022).

[36] J. Sang Pyo and K. Ho Choi, Some properties of the generalized Fibonacci sequence q_n by matrix methods, *The Korean Journal of Mathematics* **24** (2016), 681–691.

[37] J. H. Silverman, The arithmetic of elliptic curves, Springer, Dordrecht, second édition, 2009, ISBN 978-0-387-09493-9.

[38] J. R. Silvester, Fibonacci properties by matrix methods, *The Mathematical Gazette* **425** (1979), 188–191.

[39] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org, 2021.

[40] L. Somer, The divisibility properties of primary Lucas recurrences with respect to primes, *Fibonacci Quarterly* **4** (1980), 316–334.

[41] D. Tascı and G. Ozkan Kızılırmak, On the periods of biperiodic Fibonacci and biperiodic Lucas numbers, *Discrete Dyn. Nat. Soc.* (2016), 1–5.

[42] E. Tan and A. Ekin, Some identities on conditional sequences by using matrix method, *Miskolc Mathematical Notes* **18** (2017), 469–477.

[43] E. Tan, Some properties of the bi-periodic Horadam sequences, *Notes on Number Theory and Discrete Mathematics* **23** (2017), 56–65.

[44] E. Tan and H. Leung, Some basic properties of the generalized bi-periodic Fibonacci and Lucas sequences, *Adv. Difference Equ.* **26** (2020), 1–11.

[45] E. Tan and H. Leung, A note on congruence properties of the generalized bi-periodic Horadam sequence, *Hacettepe Journal of Mathematics and Statistics* (2020), 1–10.

[46] Ş. Uygun and H. Eldogan, Properties of k-Jacobsthal and k-Jacobsthal Lucas sequences, *General Mathematics Notes* **36** (2016), 34–47.

[47] Ş. Uygun and E. Owusu, A New Generalization of Jacobsthal Lucas Numbers (Bi-Periodic Jacobsthal Lucas Sequence), *Journal of Advances in Mathematics and Computer Science* **34** (2019), 1–13.

[48] J. Vinson, The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence, *Fibonacci Quarterly* **1** (1963), 37–45.

[49] D. Vella and A. Vella, Cycles in the Generalized Fibonacci Sequence Modulo a Prime, *Math. Mag.* **75** (2002), 294–299.

[50] D. Vella and A. Vella, Calculating exact cycle lengths in the generalized Fibonacci sequence modulo p, *The Mathematical Gazette* **90** (2006), 70–77.

[51] A. Vince, Period of a linear recurrence, *Acta Arith.* **4** (1981), 303–311.

[52] D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.

[53] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman and Hall/CRC, 2008, ISBN 978-1-4200-7146-7.

[54] O. Yayenie, A note on generalized Fibonacci sequences, *Appl. Math. Comput.* **217** (2011), 5603–5611.