**ZONGULDAK BÜLENT ECEVİT UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

# CODING THEORY ON SPECIAL CASES OF THE GENERALIZED *m*-STEP FIBONACCI SEQUENCE

**DEPARTMENT OF MATHEMATICS**

**DOCTOR OF PHILOSOPHY THESIS**

**VEDAT İRGE**

**JANUARY 2024**

**ZONGULDAK BÜLENT ECEVİT UNIVERSITY**
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

# CODING THEORY ON SPECIAL CASES OF THE GENERALIZED *m*-STEP FIBONACCI SEQUENCE

**DEPARTMENT OF MATHEMATICS**

**DOCTOR OF PHILOSOPHY THESIS**

**Vedat İRGE**

**ADVISOR: Prof. Dr. Yüksel SOYKAN**

**ZONGULDAK**
**January 2024**

**APPROVAL OF THE THESIS:**

The thesis entitled "Coding Theory on Special Cases of The Generalized $m$-Step Fibonacci Sequence" and submitted by Vedat İRGE has been examined and accepted by the jury as a Doctor of Philosophy thesis in Department of Mathematics, Graduate School of Natural and Applied Sciences, Zonguldak Bülent Ecevit University. 23/01/2024

**Advisor:** Prof. Dr. Yüksel SOYKAN .....
Zonguldak Bülent Ecevit University, Faculty of Science, Department of Mathematics

**Member:** Assoc. Prof. Dr. Melih GÖCEN .....
Zonguldak Bülent Ecevit University, Faculty of Science, Department of Mathematics

**Member:** Assoc. Prof. Dr. Nazmiye GÖNÜL BİLGİN .....
Zonguldak Bülent Ecevit University, Faculty of Science, Department of Mathematics

**Member:** Assoc. Prof. Dr. Nejla ÖZMEN .....
Düzce University, Gölkaya Vocational School, Department of Computer Technologies

**Member:** Assist. Prof. Dr. Erkan TAŞDEMİR .....
Kırklareli University, Pınarhisar Vocational School, Department of Electronics and Automation

---

Approved by the Graduate School of Natural and Applied Sciences. …./…./2024

Prof. Dr. Fikret GÖLGELEYEN
Director

*"With this thesis it is declared that all the information in this thesis is obtained and presented according to academic rules and ethical principles. Also as required by academic rules and ethical principles all works that are not result of this study are cited properly."*

Vedat İRGE

## ABSTRACT

**Doctor of Philosophy Thesis**

**CODING THEORY ON SPECIAL CASES OF THE GENERALIZED *m*-STEP FIBONACCI SEQUENCE**

**Vedat İRGE**

**Zonguldak Bülent Ecevit University**
**Graduate School of Natural and Applied Sciences**
**Department of Mathematics**

**Thesis Advisor: Prof. Dr. Yüksel SOYKAN**
**January 2024, 197 pages**

In this thesis, we created new encoding and decoding algorithms for special cases of the generalized m-step Fibonacci sequence. We also presented applications for each algorithm and analyzed the security strength and complexity of the algorithms. This thesis consists of 16 chapters.

In the first chapter of the thesis, we presented some definitions and theorems of the basic mathematical tools we use in cryptography.

In chapter 2, we reminded generalized $m$-step Fibonacci numbers and some of their special cases.

In chapter 3, we presented a brief history of cryptology and some basic definitions and information about cryptology.

**ABSTRACT (continued)**

In chapter 4, we investigated some properties of Woodall number

In chapter 5, we created a new encoding and decoding algorithm using Fibonacci $Q$-matrix and $R$-matrix.

In chapter 6, we developed a new coding theory on Padovan matrices by examining the Padovan numbers.

In chapter 7, we established a new encryption and decryption algorithm using third order Jacobsthal matrices and the ElGamal technique.

In chapter 8, We obtained a public key cryptosystem using an n-variable linear Diophantine equations-based key exchange technique and Affine-Hill encryption with $\lambda$-step Pell numbers. We also performed a security strength and complexity analysis of the resulting system.

In chapter 9, we obtained a public-key cryptosystem using the ElGamal technique and Affine-Hill encryption with $\lambda$-step Jacobsthal numbers. We also performed a security strength and complexity analysis of the system.

In chapter 10, we created a new encryption and decryption algorithm using solutions of $n$-variable linear Diophantine equations and third order Pell matrices.

In chapter 11, we have introduced a new public key cryptosystem using $n$-variable linear Diophantine equations and key exchange based on the relationship between linear operators and $3-primes$ circulant matrices and Affine-Hill cryptography. We also performed a security strength and complexity analysis of the proposed system.

In chapter 12, first, we created a new key exchange algorithm using inner product and orthogonality, and then we developed a new encryption system using this key exchange algorithm, inner product, self-adjoint operators, and generalized $m$-step Fibonacci numbers. We examined the developed system in terms of security strength and complexity analysis.

**ABSTRACT (continued)**

In chapter 13, we developed a new cryptosystem using the public key technique obtained using inner product and orthogonality, inner product, self-adjoint operators, and generalized $m$-step Jacobsthal numbers. We examined the developed system in terms of security strength and complexity analysis.

In chapter 14, first, we found polynomials with rational coefficients that convert Woodall numbers to Woodall numbers. Next, we constructed a key exchange algorithm between first-order polynomials and linear Diophantine equations with $n$-variables that converts Woodall numbers to Woodall numbers. Finally, we created a new encoding and decoding algorithm using the key exchange algorithm, inner product, adjoint operators, Woodall matrices, and elliptic curves. We evaluated the algorithm in terms of security strength and complexity analysis.

In chapter 15, we introduced a new encryption and decryption algorithm using the eigenvalues and eigenvectors of the balancing matrices and, moreover, the Jordan canonical form. We performed a security analysis of the algorithm presented.

In chapter 16, we first created a symmetric encryption algorithm by making linear transformations from $R^2$ to $R^2$, Fibonacci numbers, and transitioning from the standard base of $R^2$ to a base we have determined. Later, we developed an asymmetric encryption algorithm by complicating this algorithm a little more and adding a key exchange algorithm. Complexity analysis of the developed algorithm was performed.

**Keywords:** Fibonacci number sequence, Algorithm, Coding, Decoding, Circulant matrix, Inner product, Linear operator, Elliptic curve, Eigenvalue, Eigenvector

**Science Code:** 403.03.01

# ÖZET

**Doktora Tezi**

**GENELLEŞTİRİLMİŞ $m$-BASAMAKLI FİBONACCİ DİZİSİNİN ÖZEL DURUMLARI ÜZERİNDE KODLAMA TEORİSİ**

**Vedat İRGE**

**Zonguldak Bülent Ecevit Üniversitesi**
**Fen Bilimleri Enstitüsü**
**Matematik Anabilim Dalı**

**Tez Danışmanı: Prof. Dr. Yüksel SOYKAN**
**Ocak 2024, 197 sayfa**

Bu tezde genelleştirilmiş $m$-basamaklı Fibonacci dizisinin özel durumları üzerinde yeni kodlama ve kod çözme algoritmaları oluşturulmuştur. Ayrıca her algoritma için uygulamalar sunulmuş ve algoritmaların güvenlik güçlülüğü ve komplekslik analizi yapılmıştır. Bu tez 16 bölümden oluşmaktadır.

Tezin ilk bölümünde kriptografi içinde kullandığımız temel matematiksel araçlara ait bazı tanım ve teoremler sunulmuştur.

İkinci bölümde, genelleştirilmiş $m$-basamak Fibonacci sayıları ve onların bazı özel durumları hatırlatılmıştır.

Üçüncü bölümde, kriptolojinin kısa tarihi ve kriptoloji hakkında bazı temel tanım ve bilgiler sunulmuştur.

## ÖZET (devam ediyor)

Dördüncü bölümde, Woodall sayılarının bazı özellikleri incelenmiştir.

Beşinci bölümde, Fibonacci $Q$-matris ve $R$-matris kullanılarak yeni bir kodlama ve kod çözme algoritması oluşturulmuştur.

Altıncı bölümde, Padovan sayıları incelenerek Padovan matrisleri üzerinde yeni bir kodlama teorisi geliştirilmiştir.

Yedinci bölümde, üçüncü dereceden Jacobsthal matrisleri ve ElGamal tekniği kullanılarak yeni bir şifreleme ve şifre çözme algoritması ortaya konulmuştur.

Sekizinci bölümde, $n$-değişkenli lineer Diophantine denklemleri tabanlı anahtar değişimi ve $\lambda$-basamak Pell sayıları ile Affine-Hill şifreleme kullanılarak bir açık anahtar kriptosistemi elde edilmiştir. Ayrıca elde edilen sistemin güvenlik güçlülüğü ve komplekslik analizi yapılmıştır.

Dokuzuncu bölümde, ElGamal tekniği ve $\lambda$-basamak Jacobsthal sayıları ile Affine-Hill şifreleme kullanılarak bir açık anahtar kriptosistemi elde edilmiştir. Ayrıca elde edilen sistemin güvenlik güçlülüğü ve komplekslik analizi yapılmıştır.

Onuncu bölümde, $n$-değişkenli lineer Diophantine denklemlerinin çözümleri ve üçüncü dereceden Pell matrisleri kullanılarak yeni bir şifreleme ve şifre çözme algoritması oluşturulmuştur.

Onbirinci bölümde, $n$-değişkenli lineer Diophantine denklemleri ve lineer operatörler arasındaki ilişkiye dayalı anahtar değişimi ve $3-primes$ circulant matrisleri ile Affine-Hill şifreleme kullanılarak yeni bir açık anahtar kriptosistemi ortaya konulmuştur. Ayrıca ortaya konulan sistemin güvenlik güçlülüğü ve komplekslik analizi yapılmıştır.

Onikinci bölümde, ilk olarak iç çarpım ve ortogonallik kullanılarak yeni bir anahtar değişim algoritması oluşturulmuş ve sonra bu anahtar değişim algoritması, iç çarpım, self adjoint

operatörler ve genelleştirilmiş $m$-basamaklı Fibonacci sayıları kullanılarak yeni bir kriptolama sistemi geliştirilmiştir. Geliştirilen sistem güvenlik güçlülüğü ve komplekslik analizi bakımından incelenmiştir.

Onüçüncü bölümde, iç çarpım ve ortogonallik kullanılarak oluşturulan açık anahtar tekniği, iç çarpım, self adjoint operatörler ve genelleştirilmiş $m$-basamaklı Jacobsthal sayıları kullanılarak yeni bir kriptosistem geliştirilmiştir. Geliştirilen sistemin güvenlik güçlülüğü ve komplekslik analizi bakımından incelemesi yapılmıştır.

Ondördüncü bölümde, ilk olarak Woodall sayılarını Woodall sayılarına dönüştüren rasyonel katsayılı polinomlar bulunmuştur. Sonra Woodall sayılarını Woodall sayılarına dönüştüren birinci dereceden polinomlar ve $n$-değişkenli lineer Diophantine denklemleri arasında bir anahtar değişim algoritması oluşturulmuştur. Son olarak anahtar değişim algoritması, iç çarpım, adjoint operatörler, Woodall matrisleri ve eliptik eğriler kullanılarak yeni bir kodlama ve kod çözme algoritması oluşturulmuştur. Oluşturulan algoritma güvenlik güçlülüğü ve komplekslik analizi bakımından değerlendirilmiştir.

Onbeşinci bölümde, balancing matrislerinin özdeğerleri ve özvektörleri, dahası Jordan kanonik formu kullanılarak yeni bir şifreleme ve şifre çözme algoritması ortaya konulmuştur. Ortaya konulan algoritmanın güvenlik analizi yapılmıştır.

Onaltıncı bölümde, ilk olarak $R^2$ den $R^2$ ye Fibonacci sayılarına lineer dönüşümler uygulayarak ve $R^2$ nin standart tabanından belirlediğimiz bir tabana geçiş yaparak simetrik bir şifreleme algoritması elde edilmiştir. Daha sonra bu algoritma biraz daha karmaşıklaştırılıp bir anahtar değişim algoritması eklenerek asimetrik bir şifreleme algoritması geliştirilmiştir. Geliştirilen algoritmanın komplekslik analizi yapılmıştır.

**Anahtar Kelimeler:** Fibonacci sayı dizisi, Algoritma, Kodlama, Kod çözme, Circulant matris, İç çarpım, Lineer operator, Eliptik eğri, Özdeğer, Özvektör

**Bilim Kodu:** 403.03.01

**ACKNOWLEDGEMENTS**

First of all, I would like to express my deepest gratitude to my esteemed advisor Prof. Yüksel SOYKAN for his guidance, support and dedication in the completion of this thesis. Without his wisdom, experience and encouragement, this achievement would not have been possible. He has not only developed me academically, but also played a critical role in my personal development. His patience, knowledge and suggestions have enhanced the quality of this work and broadened my perspective. His teachings will be a guiding light not only for this thesis but also for every stage of my life to come. Words are inadequate to express my gratitude to him. However, the value of his time and effort will be remembered for a lifetime. This process with his guidance and support was a great honor for me.

I would like to express my sincere thanks to Assoc. Prof. Melih GÖCEN for his support, guidance and care during the completion of this thesis. His helpfulness, knowledge and suggestions contributed significantly to the development of this study. I would also like to thank Assoc. Prof. Nejla ÖZMEN and Assist. Prof. Erkan TAŞDEMİR for their support.

I would like to express my endless gratitude to Prof. Yusuf KAYA, Head of the Department of Mathematics and the Department of Mathematics at Zonguldak Bülent Ecevit University for their support and interest throughout this thesis study.

I would like to express my deepest gratitude to my mother Satı Huri İRGE and my father Nihat İRGE who raised me. Their love and support have been the greatest source of strength for me in every aspect of my life. Their contribution to the completion of this study and the achievement of my dreams is immense.

I would like to express my endless gratitude to my wife, Burcu İLHAN İRGE, who supported me every step of the way during the completion of this thesis. Her patience, encouragement and sincere support were the key to completing this thesis and achieving my dreams. Despite every

difficulty and uncertainty, her presence has been a light for me. Her faith and support have always been my greatest source of strength. I cannot thank her enough for her sacrifices understanding and love during this process. Her love inspired me to complete this study. This thanks is not only for this thesis, but for every aspect of my life.

Finally, I would like to express my endless gratitude to my daughter Melis Beren İRGE, who has been a great source of motivation for the completion of my thesis. Her innocence and future helped me to do this study with a greater purpose.

## TABLE OF CONTENTS

**TABLE OF CONTENTS (Continued)**

**TABLE OF CONTENTS (Continued)**

**TABLE OF CONTENTS (Continued)**

**TABLE OF CONTENTS (Continued)**

**TABLE OF CONTENTS (Continued)**

## LIST OF TABLES

No Page

## LIST OF SYMBOLS AND ABBREVIATIONS

### SYMBOLS

$\phi$ : Euler $\phi$-function

$\Delta$ : The discriminant of elliptic curve

$E(K)$ : Elliptic curve $E$ over a field $K$

$SpA$ : The span of $A$

$L(V,W)$ : The set of all linear transformations $T:V \to W$

$\| \|$ : Norm

$B(X,Y)$ : The set of all continuous linear transformations $T:X \to Y$

$(.,.)$ : Inner product

$T^*$ : The adjoint of $T$

$F_n$ : Fibonacci number sequence

$L_n$ : Lucas number sequence

$J_n$ : Jacobsthal number sequence

$B_n$ : Balancing number sequence

$O$ : Big $O$

$R_n$ : Woodall number sequence

$C_n$ : Cullen number sequence

$GL_m(F_p)$ : General linear group, which consist of all invertible matrices of order $m \times m$ over $F_p$

# CHAPTER 1

# BASIC MATHEMATICAL TOOLS IN CRYPTOGRAPHY

Mathematical operations have an important place in modern crypto systems. The structure and analysis of these cryptosystems are made possible by mathematical tools. In this chapter, some basic definitions and theorems that will be used in the following chapters will be given. We will use [1-12] studies for this.

## 1.1 NUMBER THEORY

One of the most important used in cryptography is number theory. In this section, preliminary information about number theory and used in cryptography will be given.

### 1.1.1 Divisibility

**Definition 1.1** *[1] Let $a$ and $b$ be integers, with $b$ equal to non-zero. If there is an integer $c$ such that $a = bc$, we say that $b$ divides $a$ or that $a$ is divisible by $b$. To show that $b$ divides $a$, we write $b|a$. We write $b \nmid a$ if $b$ does not divide $a$.*

**Example 1.1** *We have $7|56$, since $56 = 7 \times 8$. On the other hand, $23 \nmid 862$, since $862 = 23 \times 37 + 11$, so $862$ is not an exact multiple of $23$.*

**Proposition 1.1** *[2] Assume that $a$, $b$, and $c$ are integers. If $a|b$ and $b|c$, then $a|c$.*

**Proposition 1.2** *[2] Let $a, b, c$ integers. If $a|b$ and $a|c$, then $a|(mb + nc)$ for all integers $m$ and $n$.*

### 1.1.2 Prime Numbers and Factorization

The prime numbers are possibly the most important object of study in number theory, and they will be crucial in cryptography as well. Let us review them.

**Definition 1.2** *[1] An integer $p \geq 2$ is said to be prime if its only positive factors are 1 and $p$ itself.*

**Remark 1.1** *We do not consider 1 as prime. Although some mathematicians have put 1 in the list of primes in the past, no one does so now. This is because mathematicians wish to claim that there is only one way to factor an integer into a product of primes. We would have an infinite number of methods to factor an integer into primes if 1 were a prime. For instance, if we were to factor 15, we would have $15 = 3 \times 5 = 3 \times 5 \times 1 = 3 \times 5 \times 1 \times 1$.*

**Lemma 1.3** *[2] Every integer greater than 1 is either prime or is divisible by a prime.*

**Theorem 1.4** *[2] There are infinitely many prime numbers.*

**Theorem 1.5** *[1] (Fundamental Theorem of Arithmetic) Every positive integer $n$ can be written as the product of prime numbers*

$n = p_1 \times p_2 \times \cdots \times p_r$.

*(The $p_i$ 's can repeat.) Furthermore, this product representation is unique up to changing the order of the factors.*

**Theorem 1.6** *[1] (Euclid's Lemma) An integer $p \geq 2$ is prime if and only if whenever $a$ and $b$ are integers such that $p$ divides $a \times b$, then $p$ divides at least one of $a$ and $b$.*

**Definition 1.3** *[1] An integer $n \geq 2$ which is not prime is said to be composite.*

**Proposition 1.7** *[2] If $n$ is composite, then $n$ has a prime factor $p \leq \sqrt{n}$.*

### 1.1.3 Division Algorithm and Greatest Common Divisor

**Theorem 1.8** *[3] For any integer $a$ and any integer $b \neq 0$, there exist unique integers $q$ and $r$ such that*

$a = bq + r,\ 0 \leq r < |b|\,,$

*where $a$ is called the dividend, $q$ the quotient, and $r$ the remainder. If $b \nmid a$, then $r$ satisfies the stronger inequalities $0 < r < |b|$.*

**Definition 1.4** *[1] A common divisor of two integers $a$ and $b$ is a positive integer $d$ that divides both of them. The greatest common divisor of $a$ and $b$ is, as its name suggests, the largest positive integer $d$ such that $d|a$ and $d|b$. The greatest common divisor of $a$ and $b$ is denoted $gcd(a, b)$. It can also be represented as the greatest common divisor $(a, b)$.*

**Remark 1.2** *[2] If $a$ and $b$ are both $0$, then $(a, b)$ is not defined. If $a \neq 0$, then $(a, 0) = |a|$.*

**Definition 1.5** *[2] Two integers $a$ and $b$ are said to be relatively prime if $(a, b) = 1$.*

**Proposition 1.9** *[2] If $a$ and $b$ are integers with $d = (a, b)$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

**Proposition 1.10** *Let $a$ and $b$ be two integers, at least one of which is non-zero. Then $(a, b) = (b, a)$.*

**Proposition 1.11** *[2] Let $a$ and $b$ be two integers, at least one of which is non-zero. If $m$ is a positive integer, then $(ma, mb) = m.(a, b)$.*

**Euclidean Algorithm:** [2] Let $a$ and $b$ be non-negative integers and assume that $b \neq 0$. By repeatedly applying the division algorithm,

$$\begin{aligned}
a &= bq_1 + r_1,\ 0 \leq r_1 < b \\
b &= r_1q_2 + r_2,\ 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3,\ 0 \leq r_3 < r_2 \\
&\vdots \\
r_{k-2} &= r_{k-1}q_k + r_k,\ 0 \leq r_k < r_{k-1} \\
r_{k-1} &= r_kq_{k+1} + 0r_{k+1}
\end{aligned}$$

is obtained. The last non-zero remainder, namely $r_k$, equals $(a, b)$.

**Theorem 1.12** *[3] Let $a$ and $b$ be integers, at least one of which is non-zero. Then there exist integers $x$ and $y$ such that*

$d = (a, b) = ax + by.$

**Corollary 1.1** *[3] Let $a$ and $b$ be integers, at least one of which is non-zero. If $(a, b) = 1$, then there exist integers $x$ and $y$ such that*

$1 = ax + by.$

**Example 1.2** *Let's find* $(385, 66)$ *with the Euclidean algorithm.*

$$\begin{aligned} 385 &= 66.5 + 55 \\ 66 &= 55.1 + 11 \\ 55 &= 11.5 + 0. \end{aligned}$$

*We get* $(385, 66) = 11$. *Now let's write* $d = 11$ *as the linear sum of the numbers* 385 *and* 66.

$$\begin{aligned} 11 &= 66 - 55 \\ 11 &= 66 - (385 - 6.66) \\ 11 &= -1.385 + 6.66. \end{aligned}$$

*We have* $11 = -1.385 + 6.66$.

The following theorem is a consequence of the Euclidean algorithm.

**Theorem 1.13** *[2] Let* $a$ *and* $b$ *be two integers, at least one of which is non-zero. For any integers* $x$ *and* $y$, $(a, b) = (a, ax + by) = (b, ax + by)$.

**Theorem 1.14** *[2] Let* $n \geq 2$ *and* $a_1, a_2, \ldots, a_n$ *an be integers (at least one of them must be non-zero). Then there exist integers* $x_1, x_2, \ldots, x_n$ *such that*

$(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

**Corollary 1.2** *[2] If* $d$ *is the common divisor of* $a$ *and* $b$, *then* $d$ *divides* $(a, b)$.

**Lemma 1.15** *[2] If* $a, b, c$ *are integers such that* $(a, c) = (b, c) = 1$ *then* $(ab, c) = 1$.

**Lemma 1.16** *[2] Let* $a, b, c$ *be integers with* $a \neq 0$ *and* $(a, b) = 1$. *If* $a \backslash bc$ *then* $a \backslash c$.

**Lemma 1.17** *[2] Let* $a, b, c$ *be integers with* $a \neq 0$, $b \neq 0$ *and* $(a, b) = 1$. *If* $a \backslash c$ *and* $b \backslash c$ *then* $ab \backslash c$.

**Theorem 1.18** *[2] Assume that a,b and c are integers where at least one of* $a, b$ *is non-zero. Then the equation* $ax + by = c$ *has a solution if and only if* $(a, b) \backslash c$. *If it has one solution, then it has an infinite number. If* $(x_0, y_0)$ *is any particular solution, then all solutions are of the form*

$$x = x_0 + \frac{b.t}{(a, b)},\ y = y_0 - \frac{a.t}{(a, b)},$$

*where* $t$ *is an integer.*

### 1.1.4 Modular Arithmetic

The set of numbers we know, such as the set of integers, or the set of real numbers, is infinite. However, almost all cryptographic algorithms are based on arithmetic with a finite number of elements. The way to do this is with modular arithmetic, the basic definitions and theorems of which will be given below.

**Definition 1.6** *[4] Let $a$ and $b$ be integers and $m$ a positive integer.We say that "$a$ is congruent to $b$ modulo $m$", denoted by*

$a \equiv b (\mathrm{mod}\, m)$

*if $m$ is a divisor of $a - b$, or equivalently, if $m|(a - b)$. Similarly, we write*

$a \neq b (\mathrm{mod}\, m)$

*if $a$ is not congruent (or incongruent) to $b$ modulo $m$, or equivalently, if $m \nmid (a - b)$. Clearly, for $a \equiv b (\mathrm{mod}\, m)$ $(a \neq b (\mathrm{mod}\, m))$, we can write $a = km + b$ $(a \neq km + b)$ for some integer $k$. The integer $m$ is called the modulus.*

Clearly,

$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m|(a - b) \Leftrightarrow a = km + b,\ k \in \mathbb{Z}$

and

$a \neq b (\mathrm{mod}\, m) \Leftrightarrow m \nmid (a - b) \Leftrightarrow a \neq km + b,\ k \in \mathbb{Z}.$

**Proposition 1.19** *[2] If $a$ is an integer and $m$ is a positive integer, then there is a unique integer $r$ with $0 \leq r \leq m - 1$ so that $a \equiv r (\mathrm{mod}\, m)$. This integer $r$ is called the least non-negative residue of $a \mod m$.*

**Theorem 1.20** *[4] Let $a$, $b$, and $m$ are integers with $m > 0$. $a \equiv b (\mathrm{mod}\, m)$ if and only if the remainders obtained by dividing $a$ and $b$ by $m$ are equal.*

**Proposition 1.21** *[4] If $a$, $b$, $c$, $d$, $p$, $q$ and $m$ are integers with $m > 0$, then the following is true.*

**a)** $a \equiv a (\mathrm{mod}\, m)$.

**b)** $a \equiv b(\mathrm{mod}\, m) \Rightarrow b \equiv a(\mathrm{mod}\, m)$.

**c)** *If* $a \equiv b(\mathrm{mod}\, m)$ *and* $b \equiv c(\mathrm{mod}\, m)$, *then* $a \equiv c(\mathrm{mod}\, m)$.

**d)** $a \equiv b(\mathrm{mod}\, m) \Rightarrow a + p \equiv b + p(\mathrm{mod}\, m)$.

**e)** $a \equiv b(\mathrm{mod}\, m) \Rightarrow a.p \equiv b.p(\mathrm{mod}\, m)$.

**f)** *If* $a \equiv b(\mathrm{mod}\, m)$ *and* $c \equiv d(\mathrm{mod}\, m)$, *then* $a + c \equiv b + d(\mathrm{mod}\, m)$.

**g)** *If* $a \equiv b(\mathrm{mod}\, m)$ *and* $c \equiv d(\mathrm{mod}\, m)$, *then* $a - c \equiv b - d(\mathrm{mod}\, m)$.

**h)** *If* $a \equiv b(\mathrm{mod}\, m)$ *and* $c \equiv d(\mathrm{mod}\, m)$, *then* $a.c \equiv b.d(\mathrm{mod}\, m)$.

**ı)** *If* $a \equiv b(\mathrm{mod}\, m)$ *and* $c \equiv d(\mathrm{mod}\, m)$, *then* $p.a + q.c \equiv p.b + q.d(\mathrm{mod}\, m)$.

**Proposition 1.22** *[2] If* $a \equiv b(\mathrm{mod}\, m)$, *then* $a^n \equiv b^n(\mathrm{mod}\, m)$ *for any positive integer* $n$.

It's worth noting that Proposition 1.21 says nothing about division in congruences. That is, expression $a.p \equiv b.p(\mathrm{mod}\, m) \Rightarrow a \equiv b(\mathrm{mod}\, m)$ is not always true. For example, $6.7 \equiv 6.3(\mathrm{mod}\, 24)$. However $7 \neq 3(\mathrm{mod}\, 24)$.

**Proposition 1.23** *[2] If* $a.c \equiv b.c(\mathrm{mod}\, m)$ *and* $(c, m) = d$, *then*

$a \equiv b(\mathrm{mod}(m/d))$

*and*

$a \equiv b + (m/d).k(\mathrm{mod}\, m)$ *with* $0 \leq k \leq d - 1$.

**Corollary 1.3** *[2] If* $a.c \equiv b.c(\mathrm{mod}\, m)$ *and* $(c, m) = 1$, *then* $a \equiv b(\mathrm{mod}\, m)$.

**Proposition 1.24** *[2] Let* $a$, $b$, *and* $m$ *are integers with* $m > 0$. *If* $a \equiv b(\mathrm{mod}\, m)$, *then* $(a, n) = (b, n)$.

**Proposition 1.25** *[2] Let* $a$, $b$, *and* $m$ *are integers with* $m > 0$. *Then* $a.b \equiv 1(\mathrm{mod}\, m)$ *for some integer* $b$ *if and only if* $(a, m) = 1$.

If such an integer $b$ exists, then we say that $b$ is the (multiplicative) inverse of a modulo $m$.

**Proposition 1.26** *[2] If $p$ is a prime and $a.b \equiv 0(\mathrm{mod}\, p)$, then $a \equiv 0(\mathrm{mod}\, p)$ or $b \equiv 0(\mathrm{mod}\, p)$.*

Let us give below a consequence of proposition 1.26.

**Corollary 1.4** *[2] Let $p$ be prime. The congruence*

$x^2 \equiv 1(\mathrm{mod}\, p)$

*has only the solutions $x \equiv \pm 1(\mathrm{mod}\, p)$.*

### 1.1.5 Linear Modular Arithmetic

There is an important relationship between linear modular arithmetic and equations. In fact, the linear congruence $ax \equiv b(\mathrm{mod}\, m)$ is equivalent to the linear Diophantine equation $ax - my = b$. That is,

$ax \equiv b(\mathrm{mod}\, m) \Rightarrow ax - my = b.$

**Theorem 1.27** *[4] Let $(a, m) = d$. If $d \nmid b$, then the linear congruence*

$ax \equiv b(\mathrm{mod}\, n)$

*has no solution.*

**Theorem 1.28** *[2] Let $m$ be a positive integer and let $a \neq 0$. The congruence*

$ax \equiv b(\mathrm{mod}\, m)$

*has a solution if and only if $d = (m, a)$ is a divisor of $b$. If $d|b$, then there are exactly $d$ solutions that are distinct* $\mathrm{mod}\, m$*. In this case, if $x_0$ is a solution, the solutions* $\mathrm{mod}\, m$ *are*

$x = x_0 + (m/d).k$ *for* $0 \leq k \leq d$.

*The solution $x_0$ can be taken to be any integer satisfying*

$(a/d).x_0 \equiv (b/d)(\mathrm{mod}\, m/d).$

**Corollary 1.5** *[2] If $(a, m) = 1$, the congruence $ax \equiv b(\mathrm{mod}\, m)$ has exactly one solution* $\mathrm{mod}\, m$.

**Theorem 1.29** *[2] If $m$ and $n$ are relatively prime, then the system of congruences*

$x \equiv a(\mathrm{mod}\, m)$ *and* $x \equiv b(\mathrm{mod}\, n)$

*has a unique solution* $\mathrm{mod}\, mn$.

**Theorem 1.30** *[2] (Chinese Remainder Theorem) Assume that $m_1, m_2, \ldots, m_r$ are positive integers that are pairwise relatively prime (that is, $(m_i, m_j) = 1$ if $i \neq j$). Then the system of congruences*

$$\begin{aligned} x &\equiv a_1(\mathrm{mod}\, m_1) \\ x &\equiv a_2(\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv a_r(\mathrm{mod}\, m_r) \end{aligned}$$

*has a unique solution* $\mathrm{mod}\, m_1 m_2 \ldots m_r$.

**Example 1.3**

$$\begin{aligned} x &\equiv 1(\mathrm{mod}\, 2) \\ x &\equiv 2(\mathrm{mod}\, 3) \\ x &\equiv 1(\mathrm{mod}\, 7). \end{aligned}$$

$m_1 m_2 m_3 = 2.3.7 = 42$. *We get*
$r_1 = \frac{42}{2} = 21$, $r_1^{-1}.21 \equiv 1(\mathrm{mod}\, 2)$, $r_1^{-1} = 1$.
$r_2 = \frac{42}{3} = 14$, $r_2^{-1}.14 \equiv 1(\mathrm{mod}\, 3)$, $r_2^{-1} = 2$.
$r_3 = \frac{42}{7} = 6$, $r_3^{-1}.6 \equiv 1(\mathrm{mod}\, 7)$, $r_3^{-1} = 6$.
$x = a_1.r_1.r_1^{-1} + a_2.r_2.r_2^{-1} + a_3.r_3.r_3^{-1}$.
$x = 1.21.1 + 2.14.2 + 1.6.6 = 113 \equiv 29(\mathrm{mod}\, 42)$.

### 1.1.6 Fermat, Euler and Wilson

This subsection presents the Fermat, Euler, and Wilson theorems, which are based on modular arithmetic in number theory.

**Theorem 1.31** *[3] (Fermat's Little Theorem) Let $a$ be a positive integer and $(a, p) = 1$. If $p$ is prime, then*

$a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

**Corollary 1.6** *[2] Let $p$ be prime and let $b \neq 0 (\mathrm{mod}\, p)$. If $x \equiv y (\mathrm{mod}\, p-1)$, then*

$b^x \equiv b^y (\mathrm{mod}\, p)$.

**Definition 1.7** *[2] Let $n$ be integer with $n > 0$. Define the Euler $\phi$-function $\phi(n)$ to be the number of integers $j$ with $1 \leq j \leq n$ such that $(j, n) = 1$.*

**Proposition 1.32** *[2] Let $m, n$ be positive integers. If $(m, n) = 1$ then*

$\phi(mn) = \phi(m).\phi(n)$.

**Example 1.4** *Let's evaluate $\phi(35)$.*

$\phi(35) = \phi(5)\phi(7) = 4.6 = 24$.

**Proposition 1.33** *[2] If $p$ is a prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1}$.*

**Theorem 1.34** *[2] Let $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ with distinct primes $p_i$ and with exponents $a_i \geq 1$. Then*

$$\phi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{p|n} (1 - \frac{1}{p}),$$

*where the second product is over the primes dividing $n$.*

**Example 1.5** *Let's evaluate $\phi(35)$.*

$$\begin{aligned} \phi(35) &= 35.(1 - \frac{1}{5})(1 - \frac{1}{7}) \\ &= 35.\frac{4}{5}.\frac{6}{7} \\ &= 24. \end{aligned}$$

**Theorem 1.35** *[5] (Euler's Theorem) Let $n$ be a positive integer and let $b$ be an integer with $(b, n) = 1$. Then*

$b^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$.

**Theorem 1.36** *[2] (Wilson's Theorem) Let $p$ be prime. Then*

$(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

**Theorem 1.37** *[2] Let $n \geq 2$ be an integer. Then $n$ is prime if and only if* $(n-1)! \equiv -1 (\mathrm{mod}\, n)$.

The theorem above yields a primality test.

**Example 1.6** *Let $n = 4$. Then*

$(n-1)! = 3! = 6 \equiv 2 (\mathrm{mod}\, 4)$,

*which implies that 4 is not prime.*

### 1.1.7 Order and Primitive Roots

This subsection presents the fundamental definitions and theorems concerning order and primitive roots.

**Definition 1.8** *[2] Let $n > 0$ integer and let $(a, n) = 1$. The order of $a \bmod n$, denoted $ord_n(a)$, is the smallest positive integer $m$ such that*

$a^m \equiv 1 (\mathrm{mod}\, n)$.

**Example 1.7**

$$\begin{aligned} ord_{11}(1) &= 1, \\ ord_{11}(2) &= ord_{11}(6) = 10, \\ ord_{11}(4) &= ord_{11}(9) = 5, \\ ord_{11}(10) &= 2. \end{aligned}$$

There is always a prime of $m \geq 1$ such that $a^m \equiv 1 (\mathrm{mod}\, n)$. Because Euler's theorem tells us this. For this, the order exists and is less than or equal to $\phi(n)$.
In the following theorem, we present several important features of the order of an integer $a$ modulo $n$.

**Theorem 1.38** *[3] Let $n$ be a positive integer, $(a, n) = 1$, and $r = ord_n(a)$. Then*

**a)** $a^m \equiv 1 (\mathrm{mod}\, n) \Leftrightarrow r | m$, *where $m$ is a positive integer.*

**b)** $r | \phi(n)$.

**c)** *For nonnegative integers* $s$ *and* $t$, $a^s \equiv a^t (\mathrm{mod}\, n)$ *if and only if* $s \equiv t (\mathrm{mod}\, n)$.

**d)** *No two of the integers* $a, a^2, a^3, ..., a^r$ *are congruent modulo* $r$.

**e)** *If* $m$ *is a positive integer, then the order of* $a^m$ *modulo* $n$ *is* $\frac{r}{(r,m)}$.

**f)** *The order of* $a^m$ *modulo* $n$ *is* $r$ *if and only if* $(m, r) = 1$.

**Definition 1.9** *[3] Let* $n$ *be a positive integer and* $a$ *an integer such that* $(a, n) = 1$. *If the order of an integer* $a$ *modulo* $n$ *is* $\phi(n)$, *that is, order* $(a, n) = \phi(n)$, *then* $a$ *is called a primitive root of* $n$.

**Example 1.8** *Let's determine whether or not* 3 *is a primitive root of* 17. *Note that* $(3, 17) = 1$. *Now observe that* $3^{16} \equiv 1 (\mathrm{mod}\, 17)$. $ord_{17}(3) = 16$. *Because* 16 *is the smallest positive integer such that* $3^{16} \equiv 1 (\mathrm{mod}\, 17)$. *Note also that* $\phi(17) = 16$. *That is,* $ord_{17}(3) = \phi(17) = 16$. *Therefore* 3 *is a primitive root of* 17.

**Example 1.9** *Let's determine whether or not* 13 *is a primitive root of* 17. *Note that* $(3, 17) = 1$, $ord_{17}(13) = 4$ *and* $\phi(17) = 16$. *That is,* $ord_{17}(13) \neq \phi(17)$. *Therefore,* 13 *is not a primitive root of* 17.

**Example 1.10** 5 *is a primitive root of* 23, *because* $5^{\phi(23)} \equiv 5^{22} \equiv 1 (\mathrm{mod}\, 23)$. *Since the positive divisors of* 22 *are* 1,2,11,22, *it is sufficient to examine* $5^1, 5^2, 5^{11}$ *and* $5^{22}$. $5^1 \equiv 5 (\mathrm{mod}\, 23)$, $5^2 \equiv 2 (\mathrm{mod}\, 23)$, $5^{11} \equiv 22 (\mathrm{mod}\, 23)$. *Hence the rank of* 5 *according to (mod* 23*) is* 22.

**Example 1.11** 3 *is a primitive root of* 7, *because* $3^{\phi(7)} \equiv 3^6 \equiv 1 (\mathrm{mod}\, 7)$. *Since the positive divisors of* 6 *are* 1,2,3,6, *it is sufficient to examine* $3^1, 3^2, 3^3$ *and* $3^6$. *Note that* $3^1 \equiv 3 (\mathrm{mod}\, 7)$, $3^2 \equiv 2 (\mathrm{mod}\, 7)$, $3^3 \equiv 6 (\mathrm{mod}\, 7)$. *Hence the rank of* 3 *according to (mod* 7*) is* 6.

**Theorem 1.39** *[3] If* $n$ *has a primitive root, then there are* $\phi(\phi(n))$ *(incongruent) primitive roots modulo* $n$.

**Corollary 1.7** *[3] If* $p$ *is a prime number, then there exist* $\phi(p-1)$ *(incongruent) primitive roots modulo* $p$.

**Theorem 1.40** *[3] (Primitive Roots as Residue System) Suppose* $(a, n) = 1$. *If* $a$ *is a primitive root modulo* $n$, *then the set of integers* $\{a, a^2, a^3, ..., a^{\phi(n)}\}$ *is a reduced system of residues modulo* $n$.

**Example 1.12** *Let* $n = 14$. *Then there are* $\phi(\phi(14)) = 2$ *primitive roots of* 14, *namely,* $3, 5$. *Now let* $a = 3$ *such that* $(a, n) = (3, 14) = 1$. *Then*

$$\begin{aligned}\{a, a^2, a^3, ..., a^{\phi(n)}\} &= \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \bmod 14 \\ &= \{3, 9, 13, 11, 5, 1\} \\ &= \{1, 3, 5, 9, 11, 13\}\end{aligned}$$

*which forms a reduced system of residues modulo* 14.*We can of course choose* $a = 5$. $(5, 14) = 1$. *Then we have*

$$\begin{aligned}\{a, a^2, a^3, ..., a^{\phi(n)}\} &= \{5, 5^2, 5^3, 5^4, 5^5, 5^6\} \bmod 14 \\ &= \{5, 11, 13, 9, 3, 1\} \\ &= \{1, 3, 5, 9, 11, 13\}\end{aligned}$$

*which again forms a reduced system of residues modulo* 14.

**Theorem 1.41** *[3] An integer* $n > 1$ *has a primitive root modulo* $n$ *if and only if*

$n = 2, 4, p^\alpha$, *or* $2p^\alpha$,

*where* $p$ *is an odd prime and* $\alpha$ *is a positive integer.*

**Corollary 1.8** *[3] If* $n = 2^\alpha$ *with* $\alpha \geq 3$, *or* $n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *with* $\alpha \geq 2$ *or* $k \geq 2$, *then there are no primitive roots modulo* $n$.

**Theorem 1.42** *[3] If* $a$ *is a primitive root modulo* $n$, *then* $a^x \equiv a^y (mod n)$ *if and only if* $x \equiv y (\bmod \phi(n))$.

**Proposition 1.43** *[2] Let* $a$ *be a primitive root for the odd prime* $p$. *Then*

$a^{(p-1)/2} \equiv -1 (\bmod p)$.

**Proposition 1.44** *[2] Let* $p$ *be a prime and let* $h \neq 0 (mod p)$. *The following are equivalent:*

**a)** $a$ *is a primitive root for* $p$.

**b)** *For each prime* $l$ *dividing* $p - 1$,

$a^{(p-1)/l} \neq 1 (\bmod p)$.

### 1.1.8 Linear Diophantine Equations

An equation of the form

$$a_1x_1 + \cdots + a_nx_n = b, \tag{1.1}$$

where $a_1, a_2, ..., a_n, b$ are fixed integers and $x_1, x_2, \ldots, x_n$ are unknowns in integers, is called a linear Diophantine equation. We assume that $n \geq 2$ and that coefficients $a_1, a_2, ..., a_n$ are all different from zero.
Let us give the following theorem for $n = 2$.

**Theorem 1.45** *[6] Let $a, b, c$ be integers, $a$ and $b$ nonzero. Consider the linear Diophantine equation*

$$ax + by = c. \tag{1.2}$$

**a)** *The equation 1.2 is solvable in integers if and only if $(a, b)|c$.*

**b)** *If $(x, y) = (x_0, y_0)$ is a particular solution to 1.2, then every integer solution is of the form*

$$x = x_0 + \frac{b}{(a, b)}t,\ y = y_0 - \frac{a}{(a, b)}t, \tag{1.3}$$

*where $t$ is an integer.*

**c)** *If $c = (a, b)$ and $|a|$ or $|b|$ is different from 1, then a particular solution $(x, y) = (x_0, y_0)$ to 1.3 can be found such that $|x_0| < |b|$ and $|y_0| < |a|$.*

**Theorem 1.46** *[6] The equation 1.1 is solvable if and only if $(a_1, a_2, ..., a_n)|b$. In case of solvability, one can choose $n - 1$ solutions such that each solution is an integer linear combination of those $n - 1$ solutions.*

**Theorem 1.47** *[7] Given integers $a_1, a_2, ..., a_n$, $n > 2$ we have*

$$(a_1, a_2, ..., a_n) = (a_1, a_2, ..., a_{n-2}, (a_{n-1}, a_n)).$$

**Example 1.13** *Solve the equation*

$$2x + 3y + 5z = 6.$$

*Working modulo* 5 *we have* $2x + 3y \equiv 1 (\mathrm{mod}\, 5)$, *and hence*

$2x + 3y = 1 + 5m$, $m \in \mathbb{Z}$.

*A solution to this equation is* $x = -1 + 4m$, $y = 1 - m$. *Applying 1.3, we obtain* $x = -1 + 4m + 3t$, $y = 1 - m - 2t$, $t \in \mathbb{Z}$, *and substituting back into the original equation yields* $z = 1 - m$. *Hence all solutions are*

$(x, y, z) = (-1 + 4m + 3t, 1 - m - 2t, 1 - m)$, $m$,$t \in \mathbb{Z}$.

### 1.1.9 Elliptic Curves

This subsection presents basic information about elliptic curves. Elliptic curves have applications in various fields, including number theory, cryptography, and algebraic geometry.
One notable feature of elliptic curves is their group structure, which is utilized in elliptic curve cryptography (ECC). ECC has become a crucial component in modern cryptographic systems due to its efficiency and strong security properties.

**Definition 1.10** *[8] An elliptic curve* $E$ *over a field* $\mathbb{K}$ *is defined by an equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.4}$$

*where* $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ *and* $\Delta \neq 0$, *where* $\Delta$ *is the discriminant of* $E$ *and is defined as follows:*

$$\begin{aligned}
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

*If* $L$ *is any extension field of* $K$, *then the set of* $L$*-rational points on* $E$ *is*

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

*where* $\infty$ *is the point at infinity.*

We shall employ elliptic curves of the $y^2 = x^3 + ax + b$ form in this research, where $a, b \in \mathbb{K}$. The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$.

**Group law for** $E/\mathbb{K} : y^2 = x^3 + ax + b, char(\mathbb{K}) \neq 2, 3$

- Identity: $P + \infty = \infty + P = P$ for all $P \in E(\mathbb{K})$.

- Negatives: If $P = (x, y) \in E(\mathbb{K})$, then $(x, y) + (x, -y) = \infty$. The point $(x, -y)$ is denoted by $-P$ and is called the negative of $P$; note that $-P$ is indeed a point in $E(\mathbb{K})$. Also, $-\infty = \infty$.

- Point addition: Let $P = (x_1, y_1) \in E(K)$ and $Q = (x_2, y_2) \in E(\mathbb{K})$, where $P = \pm Q$. Then $P + Q = (x_3, y_3)$, where

  $x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$ and $y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1$.

- Point doubling: Let $P = (x_1, y_1) \in E(\mathbb{K})$, where $P = -P$. Then $2P = (x_3, y_3)$, where

  $x_3 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$ and $y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1$.

**Example 1.14** *[8] (Elliptic curve over the prime field $F_{29}$) Let $p = 29$, $a = 4$, and $b = 20$, and consider the elliptic curve*

$E : y^2 = x^3 + 4x + 20$

*defined over $F_{29}$. Note that $\Delta = -16(4a^3 + 27b^2) = -176896 \neq 0 (mod 29)$, so $E$ is indeed an elliptic curve. The points in $E(F_{29})$ are the following:*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\infty$ | $(2, 6)$ | $(4, 19)$ | $(8, 10)$ | $(13, 23)$ | $(16, 2)$ | $(19, 16)$ | $(27, 2)$ |
| $(0, 7)$ | $(2, 23)$ | $(5, 7)$ | $(8, 19)$ | $(14, 6)$ | $(16, 27)$ | $(20, 3)$ | $(27, 27)$ |
| $(0, 22)$ | $(3, 1)$ | $(5, 22)$ | $(10, 4)$ | $(14, 23)$ | $(17, 10)$ | $(20, 26)$ | |
| $(1, 5)$ | $(3, 28)$ | $(6, 12)$ | $(10, 25)$ | $(15, 2)$ | $(17, 19)$ | $(24, 7)$ | |
| $(1, 24)$ | $(4, 10)$ | $(6, 17)$ | $(13, 6)$ | $(15, 27)$ | $(19, 13)$ | $(24, 22)$ | |

*Examples of elliptic curve addition are $(5, 22) + (16, 27) = (13, 6)$, and $2(5, 22) = (14, 6)$.*

## 1.2 FUNCTIONAL ANALYSIS

In this section, we will give some essential concepts of linear algebra and functional analysis.

**Definition 1.11** *[9]Let $V$ be a non-empty set. If the*

$+ : (x, y) \to x + y$

*function defined from $V \times V$ to $V$ for all $x, y \in V$ and $\alpha \in \mathbb{F}$ and the*

$\cdot : (\alpha, x) \to \alpha.x$

*function defined from $\mathbb{F} \times V$ to $V$ satisfy the following axioms, the set $V$ is called a vector space over $\mathbb{F}$.*
*For any $\alpha, \beta \in \mathbb{F}$ and any $x, y, z \in V$,*

**a)** $x + y = y + x$, $x + (y + z) = (x + y) + z$;

**b)** *there exists a unique $0 \in V$ (independent of $x$) such that $x + 0 = x$;*

**c)** *there exists a unique $-x \in V$ such that $x + (-x) = 0$;*

**d)** $1x = x$, $\alpha(\beta x) = (\alpha\beta)x$;

**e)** $\alpha(x + y) = \alpha x + \alpha y$, $(\alpha + \beta)x = \alpha x + \beta x$.

If $\mathbb{F} = \mathbb{R}$ (respectively, $\mathbb{F} = \mathbb{C}$) then $V$ is a real (respectively, complex) vector space. Elements of $\mathbb{F}$ are called scalars, while elements of $V$ are called vectors. The operation $x + y$ is called vector addition, while the operation $\alpha x$ is called scalar multiplication.

**Definition 1.12** *[9] Let $V$ be a vector space, let $\mathbf{v} = \{v_1, ..., v_k\} \subset V$ , $k \geq 1$, be a finite set and $A \subset V$ be an arbitrary non-empty set.*

**a)** *A linear combination of the elements of $\mathbf{v}$ is any vector of the form*

$$x = \alpha_1 v_1 + \cdots + \alpha_k v_k = \sum_{i=1}^{k} \alpha_i v_i \in V,$$

*for any set of scalars $\alpha_1, \ldots, \alpha_k$.*

**b)** **v** *is linearly independent if the following implication holds:*

$$\alpha_1 v_1 + \cdots \alpha_k v_k = 0 \Rightarrow \alpha_1 = \ldots = \alpha_k = 0.$$

**c)** *A is linearly independent if every finite subset of A is linearly independent. If A is not linearly independent then it is linearly dependent.*

**d)** *The span of A (denoted SpA) is the set of all linear combinations of all finite subsets of A. This set is a linear subspace of V. Equivalently, SpA is the intersection of the set of all linear subspaces of V which contain A. Thus, SpA is the smallest linear subspace of V containing A.*

$$SpA = \{x = \sum_{i=1}^{k} \alpha_i v_i : k \in \mathbb{N},\ \alpha_1, \ldots, \alpha_k \in \mathbb{F},\ v_1, ..., v_k \in A\}.$$

**Definition 1.13** *[9] Let V, W be vector spaces over the same scalar field $\mathbb{F}$. A function $T : V \to W$ is called a linear transformation (or mapping) if, for all $\alpha,\ \beta \in \mathbb{F}$ and $x, y \in V$,*

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y).$$

*Equivalent to this, for all $\alpha,\ \beta \in \mathbb{F}$ and $x, y \in V$, if it satisfies the property*

$$T(x + y) = T(x) + T(y),\ T(\alpha x) = \alpha T(x),$$

*T is called a linear transformation.*

The set of all linear transformations $T : V \to W$ will be denoted by $L(V, W)$.

**Lemma 1.48** *[9] Let V, W, X be vector spaces and $T \in L(V, W)$, $S \in L(W, X)$. Then the composition $ST = ST \in L(V, X)$.*

**Definition 1.14** *[9] Let X and Y be normed linear spaces and $T : X \to Y$ be a linear transformation. T is said to be bounded if there exists a positive real number k such that*

$$\|T(x)\| \leq k \|x\|$$

*for all $x \in X$.*

Let $X$ and $Y$ be normed linear spaces. The set of all continuous linear transformations from $X$ to $Y$ is denoted by $B(X,Y)$. If $X$ and $Y$ are normed linear spaces then $B(X,Y) \subseteq L(X,Y)$.

**Theorem 1.49** *[9] Let $X$ be a finite-dimensional normed space, $Y$ be any normed linear space and $T : X \to Y$ be a linear transformation. Then $T$ is continuous.*

**Definition 1.15** *[9] Let $X$, $Y$ be normed linear spaces. An operator $T \in B(X,Y)$ is said to be invertible if there exists $S \in B(Y,X)$ such that $ST = I_X$, $TS = I_Y$, in which case $S$ is the inverse of $T$ and is denoted by $T^{-1}$.*

**Lemma 1.50** *[9] If $X$, $Y$, $Z$ are normed linear spaces and $T_1 \in B(X,Y)$, $T_2 \in B(Y,Z)$ are invertible, then:*

**a)** *$T^{-1}$ is linear, that is, the inverse of a linear operator is also linear.*

**b)** $(T^{-1})^{-1} = T$.

**c)** *$T_1T_2$ has an inverse and $(T_1T_2)^{-1} = T_2^{-1}T_1^{-1}$.*

**Definition 1.16** *[9] Let $X$ be a real vector space. An inner product on $X$ is a function $(.,.) : X \times X \to \mathbb{R}$ such that for all $x, y, z \in X$ and $\alpha, \beta \in \mathbb{R}$,*

**a)** $(x,x) \geq 0$;

**b)** $(x,x) = 0$ *if and only if* $x = 0$;

**c)** $(\alpha x + \beta y, z) = \alpha(x,z) + \beta(y,z)$;

**d)** $(x,y) = (y,x)$.

**Definition 1.17** *[9] Let $X$ be a complex vector space. An inner product on $X$ is a function $(.,.) : X \times X \to \mathbb{C}$ such that for all $x, y, z \in X$, $\alpha$, $\beta \in \mathbb{C}$,*

**a)** $(x,x) \in \mathbb{R}$ *and* $(x,x) \geq 0$;

**b)** $(x,x) = 0$ *if and only if* $x = 0$;

**c)** $(\alpha x + \beta y, z) = \alpha(x, z) + \beta(y, z)$;

**d)** $(x, y) = \overline{(y, x)}$.

**Definition 1.18** *[9] A real or complex vector space $X$ with an inner product $(.,.)$ is called an inner product space.*

**Definition 1.19** *[9] Let $X$ be an inner product space. The vectors $x, y \in X$ are said to be orthogonal if $(x, y) = 0$.*

**Definition 1.20** *[9] An inner product space which is complete with respect to the metric associated with the norm induced by the inner product is called a Hilbert space.*

**Theorem 1.51** *[9] Every finite-dimensional inner product space is a Hilbert space.*

**Theorem 1.52** *[9] Let $\mathcal{H}$ and $\mathcal{K}$ be complex Hilbert spaces and $T \in B(\mathcal{H}, \mathcal{K})$. There exists a unique operator $T^* \in B(\mathcal{K}, \mathcal{H})$ such that*

$(Tx, y) = (x, T^*y)$

*for all $x \in \mathcal{H}$ and all $y \in \mathcal{K}$.*

**Definition 1.21** *[9] If $\mathcal{H}$ and $\mathcal{K}$ are complex Hilbert spaces and $T \in B(\mathcal{H}, \mathcal{K})$ the operator $T^*$ constructed in Theorem 1.52 is called the adjoint of $T$.*

**Definition 1.22** *[9] If $A = [a_{i,j}] \in M_{mn}(\mathbb{F})$ then the matrix $[\overline{a_{j,i}}]$ is called the adjoint of $A$ and is denoted by $A^*$.*

**Definition 1.23** *[9]*

**a)** *If $\mathcal{H}$ is a complex Hilbert space and $T \in B(\mathcal{H})$ then $T$ is normal if*

$$TT^* = T^*T.$$

**b)** *If $A$ is a square matrix then $A$ is normal if*

$$AA^* = A^*A.$$

**Definition 1.24** *[9]*

**a)** *If $\mathcal{H}$ is a complex Hilbert space and $T \in B(\mathcal{H})$ then $T$ is self-adjoint if $T = T^*$.*

**b)** *If $A$ is a square matrix then $A$ is self-adjoint if $A = A^*$.*

**Example 1.15** *The matrix* $A = \begin{pmatrix} 3 & -i \\ i & 5 \end{pmatrix}$ *is self-adjoint.*

$A^* = \begin{pmatrix} 3 & -i \\ i & 5 \end{pmatrix} = A.$

**Lemma 1.53** *[9] Let $\mathcal{H}$ be a complex Hilbert space and $T \in B(\mathcal{H})$. Then $TT^*$ and $T^*T$ are self-adjoint.*

**Definition 1.25** *[10] Let $A$ be any square matrix. A scalar $\lambda$ is called an eigenvalue of $A$ if there exists a nonzero (column) vector $v$ such that $Av = \lambda v$. Any vector satisfying this relation is called an eigenvector of $A$ belonging to the eigenvalue $\lambda$.*

We note that each scalar multiple $kv$ of an eigenvector $v$ belonging to $\lambda$ is also such an eigenvector, because

$A(kv) = k(Av) = k(\lambda v) = \lambda(kv).$

**Theorem 1.54** *[10] An $n$-square matrix $A$ is similar to a diagonal matrix $D$ if and only if $A$ has $n$ linearly independent eigenvectors. In this case, the diagonal elements of $D$ are the corresponding eigenvalues and $D = P^{-1}AP$, where $P$ is the matrix whose columns are the eigenvectors.*

Suppose a matrix $A$ can be diagonalized as above, say $D = P^{-1}AP$, where $D$ is diagonal. Then $A$ has the extremely useful diagonal factorization:

$PDP^{-1} = A.$

**Theorem 1.55** *[10] Suppose $v_1, v_2, ..., v_n$ are nonzero eigenvectors of a matrix $A$ belonging to distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. Then $v_1, v_2, ..., v_n$ are linearly independent.*

For an $n \times n$-type matrix $A$ to be diagonalizable, a sufficient condition is that it has $n$ different eigenvalues. It may be the case that $A$ is not diagonalizable. Such a situation arises when $A$ has repeated eigenvalues, and therefore there are no $n$ linearly independent eigenvectors. In such cases, we will use the Jordan Canonical Form.

**Definition 1.26** *[11] ($\lambda$-Jordan block) For $\lambda \in \mathbb{C}$, $m \in \mathbb{N}$, define*

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} \in \mathbb{C}_{n\times n}.$$

*This is a $\lambda$-Jordan block of order $n$.*

**Example 1.16** $J_1(\lambda) = (\lambda)$, $J_2(7) = \begin{pmatrix} 7 & 1 \\ 0 & 7 \end{pmatrix}$, $J_3(5) = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 5 \end{pmatrix}$.

Let's start with some fundamental Jordan block information. First, we will present some significant results.

Notice that $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda \\ 0 \\ 0 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, that is, $\lambda$ is an eigenvalue of $J_3(\lambda)$ with eigenvector the standard basis vector $e_1$.

**Theorem 1.56** *[11] Consider a general Jordan block $J_n(\lambda)$;*

**a)** *$J_n(\lambda)$ is an upper triangular matrix.*

**b)** $\det(J_n(\lambda)) = \lambda^n$.

**c)** *$J_n(\lambda)$ is invertible* $\Leftrightarrow \lambda \neq 0$.

**d)** *$\lambda$ is the only eigenvalue of $J_n(\lambda)$ and the standard basis vector $e_1$ spans the eigenspace $E_\lambda(J_n(\lambda))$..*

**e)** $\dim(E_\lambda(J_n(\lambda))) = 1$.

**f)** *The characteristic polynomial of $J_n(\lambda)$ is $\mathcal{X}_{J_n(\lambda)}(x) = (x-\lambda)^n$.*

**g)** $J_n(\lambda)^k = \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \cdots \\ 0 & \lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \cdots \\ 0 & 0 & \lambda^k & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^k \end{pmatrix}$ *for* $k \in \mathbb{N}$.

**Theorem 1.57** *[12] (Jordan canonical form theorem) Every $n \times n$-type matrix $A$ is similar to a Jordan form given by the formula*

$$J=diag(J_1, J_2, \ldots, J_r) = \begin{pmatrix} J_1 & 0 & \cdots & 0 & 0 \\ 0 & J_2 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots \\ \vdots & \vdots & \cdots & J_{r-1} & 0 \\ 0 & 0 & \cdots & 0 & J_r \end{pmatrix}_{n\times n}, \ 1 \leq r \leq n,$$

*that is, $P^{-1}AP = J$, where $P$ is the transition matrix,*

$$J_{s_i}(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{pmatrix}, \ i = 1, 2, \ldots, r,$$

*each $J_{s_i}$ is a $s_i \times s_i$ type matrix, $\sum_{i=1}^{r} s_i = n$ and also $\sum \dim(E_{\lambda_i}(J_{s_i}(\lambda_i))) = r$ .*

The number of Jordan blocks corresponding to one eigenvalue $\lambda$ is called the geometric multiplicity of $\lambda$, and this number, in turn, equals the number of linearly independent eigenvectors corresponding to $\lambda$. The algebraic multiplicity of an eigenvalue $\lambda$ is the number of times it is repeated. If the algebraic multiplicity of $\lambda$ is 1 (i.e., $\lambda$ is not repeated), then we refer to $\lambda$ as simple. If the geometric multiplicity of $\lambda$ is equal to its algebraic multiplicity (i.e., only $1 \times 1$ Jordan blocks correspond to $\lambda$), then it is called semisimple.

**Remark 1.3** *[12] Since $P^{-1}AP = J$, then*

$$AP = PJ. \tag{1.5}$$

*Let $P = (\xi_1, \xi_2, \ldots, \xi_n)$. Equating the first $s_1$ columns of both sides in formula (1.5), we obtain*

$$A\xi_1 = \lambda_1\xi_1, \ldots; A\xi_i = \lambda_1\xi_i + \xi_{i-1},\ i = 2, 3, \ldots, s_1. \tag{1.6}$$

*Clearly, $\xi_1$ is the only eigenvector of $A$ in the Jordan chain $\xi_1, \xi_2, \ldots, \xi_{s_1}$ . The other vectors $\xi_2, \xi_3, \ldots, \xi_{s_1}$ are called generalized eigenvectors of $A$, and they may be obtained by using the difference equation*

$(A - \lambda_1 I)\xi_i = \xi_{i-1},\ i = 2, 3, ..., s_1.$

*Repeating this process for the remainder of the Jordan blocks, one may find the generalized eigenvectors corresponding to the $m-th$ Jordan block using the difference equation*

$(A - \lambda_m I)\xi_{m_i} = \xi_{m_i-1},\ i = 2, 3, ..., s_m.$

*Thus, the $P$ matrix is obtained.*

**Remark 1.4** *We can find $J$ without finding $P$. The eigenvalues of $A$ are the diagonal elements of $J$, and how much* 1 *will be written in the upper triangle is found by subtracting the number of linearly independent eigenvectors from the size of the matrix.*

We will now present the matrices of linear transformations and the change of basis.
Let $T$ be a linear operator (transformation) from a vector space $V$ into itself, and suppose $S = \{u_1, u_2, \ldots, u_n\}$ is a basis of $V$. Now $T(u_1), T(u_2), \ldots, T(u_n)$ are vectors in $V$, and so each is a linear combination of the vectors in the basis $S$; say,

$$\begin{aligned} T(u_1) &= a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n \\ T(u_2) &= a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n \\ &\cdots \\ T(u_n) &= a_{n1}u_1 + a_{n2}u_2 + \cdots + a_{nn}u_n. \end{aligned}$$

**Definition 1.27** *[10] The transpose of the above matrix of coefficients, denoted by $[T]_S$, is called the matrix representation of $T$ relative to the basis $S$, or simply the matrix of $T$ in the basis $S$. (The subscript $S$ may be omitted if the basis $S$ is understood.)*

$$[T]_S = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}.$$

**Definition 1.28** *[10] Let $S = \{u_1, u_2, \ldots, u_n\}$ be a basis of a vector space $V$, and let $S' = \{v_1, v_2, \ldots, v_n\}$ be another basis. (For reference, we will call $S$ the "old" basis and $S'$ the "new" basis.) Because $S$ is a basis, each vector in the "new" basis $S'$ can be written uniquely as a linear combination of the vectors in $S$; say,*

$$\begin{aligned} v_1 &= a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n \\ v_2 &= a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n \\ &\cdots \\ v_n &= a_{n1}u_1 + a_{n2}u_2 + \cdots + a_{nn}u_n. \end{aligned}$$

*Let $P$ be the transpose of the above matrix of coefficients; that is, let $P = [p_{ij}]$, where $p_{ij} = a_{ji}$. Then $P$ is called the change-of-basis matrix (or transition matrix) from the "old" basis $S$ to the "new" basis $S'$.*

**Theorem 1.58** *[10] Let $P$ be the change-of-basis matrix from a basis $S$ to a basis $S'$ in a vector space $V$. Then, for any linear operator $T$ on $V$,*

$$[T]_{S'} = P^{-1}[T]_S P.$$

# CHAPTER 2

# SOME FUNDAMENTAL DEFINITIONS AND RESULTS

Let us introduce some basic definitions and some theorems that we need throughout the thesis. We will use the information in [13] in the following section.

## 2.1 GENERALIZED $m$-STEP FIBONACCI NUMBERS

Several generalizations of Fibonacci numbers and identities have been studied by mathematicians over the years. For $m \geq 2$, the generalized $m$-step Fibonacci numbers (or the generalized $m$-step Fibonacci sequence), $\{V_n(V_0, V_1, V_2, ..., V_{m-1}; r_1, r_2, , ..., r_m)\}_{n \geq m}$ (or shortly $\{V_n\}_{n \geq m}$), $(n \geq m)$, is defined by the $m$-order linear recurrence relation

$$V_n = \sum_{i=1}^{m} r_i V_{n-i} = r_1 V_{n-1} + r_2 V_{n-2} + r_3 V_{n-3} + ... + r_{m-1} V_{n-(m-1)} + r_m V_{n-m} \tag{2.1}$$

with $m$ initial terms

$$V_0 = c_0,\ V_1 = c_1,\ V_2 = c_2, ..., V_{m-1} = c_{m-1},$$

where $r_i$, $1 \leq i \leq m$, are all real numbers and $c_i$, $0 \leq i \leq m-1$, are all real or complex numbers. Such a sequence is also called the generalized Fibonacci $m$-sequence, or generalized $m$-nacci sequence, or the $m$-generalized Fibonacci sequence.
The sequences $\{V_n\}_{n \geq m}$ can be extended to negative subscripts by defining

$$V_{-n} = -\frac{r_{m-1}}{r_m} V_{-(n-1)} - \frac{r_{m-2}}{r_m} V_{-(n-2)} - \frac{r_{m-3}}{r_m} V_{-(n-3)} - ... - \frac{r_1}{r_m} V_{-(n-(m-1))} + \frac{1}{r_m} V_{-(n-m)}$$

for $n = m-2, m-1, m, m+1....$ Therefore, recurrence (2.1) holds for all integer $n$.
For $m \geq 2$, the $m$-step Fibonacci numbers, $U_n$ $(n \geq m)$, is defined by the $m$-order linear recurrence relation

$$U_n = \sum_{i=1}^{m} U_{n-i} = U_{m-1} + U_{m-2} + U_{m-3} + ... + U_{n-m} \tag{2.2}$$

with $m$ initial terms

$$\begin{cases} U_k = 0 & , \quad -m+2 \leq k \leq 0 \\ U_{-k+1} = 1 & , \quad k = m \end{cases} . \tag{2.3}$$

Some of the well known members of this $m$-step Fibonacci numbers include Fibonacci numbers $F_n$ ($m = 2$, $U = F$), Tribonacci numbers $T_n$ ($m = 3$, $U = T$), Tetranacci numbers $M_n$ ($m = 4$, $U = M$) and Pentanacci numbers $P_n$ ($m = 5$, $U = P$). Here $r_i = 1$ for all $1 \leq i \leq m$. See Table 2.1 for some values of these numbers.

Table 2.1 The first few sequences of $m$-step Fibonacci numbers.

| $m$ | Name | $n$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | Fibonacci | $F_n$ | $-8$ | 5 | $-3$ | 2 | $-1$ | 1 | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 |
| 3 | Tribonacci | $T_n$ | $-3$ | 2 | 0 | $-1$ | 1 | 0 | 0 | 1 | 1 | 2 | 4 | 7 | 13 | 24 | 44 | 81 |
| 4 | Tetranacci | $M_n$ | 0 | 0 | $-1$ | 1 | 0 | 0 | 0 | 1 | 1 | 2 | 4 | 8 | 15 | 29 | 56 | 108 |
| 5 | Pentanacci | $P_n$ | 0 | $-1$ | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 4 | 8 | 16 | 31 | 61 | 120 |

Like the $m$-step Fibonacci numbers, $m$-step Lucas numbers are defined by the same the $m$-order recurrence relations (2.2) but with different initial terms, namely the $m$-step Lucas numbers, $W_n$ , is defined by the $m$-order linear recurrence relation

$$W_n = \sum_{i=1}^{m} W_{n-i} = W_{m-1} + W_{m-2} + W_{m-3} + ... + W_{n-m} \tag{2.4}$$

with the $m$ initial terms

$$\begin{cases} W_k = -1 & , \quad -m+1 \leq k \leq -1 \\ W_k = m & , \quad k = 0 \end{cases} . \tag{2.5}$$

Some of the well known members of this $m$-step Fibonacci numbers include Lucas numbers $L_n$ ($m = 2$, $W = L$), Tribonacci-Lucas numbers $K_n$ ($m = 3$, $W = K$), Tetranacci-Lucas numbers $R_n$ ($m = 4$, $V = n$) and Pentanacci-Lucas numbers $Q_n$ ($m = 5$, $W = Q$). Here $r_i = 1$ for all $1 \leq i \leq m$. See Table 2.2 for some values of these numbers.

Table 2.2 The first few sequences of $m$-step Lucas numbers.

| $m$ | Name | $n$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | Lucas | $L_n$ | 7 | $-4$ | 3 | $-1$ | 2 | 1 | 3 | 4 | 7 | 11 | 18 | 29 | 47 | 76 |
| 3 | Tribonacci-Lucas | $K_n$ | $-5$ | 5 | $-1$ | $-1$ | 3 | 1 | 3 | 7 | 11 | 21 | 39 | 71 | 131 | 241 |
| 4 | Tetranacci-Lucas | $R_n$ | 7 | $-1$ | $-1$ | $-1$ | 4 | 1 | 3 | 7 | 15 | 26 | 51 | 99 | 191 | 367 |
| 5 | Pentanacci-Lucas | $Q_n$ | $-1$ | $-1$ | $-1$ | $-1$ | 5 | 1 | 3 | 7 | 15 | 31 | 57 | 113 | 223 | 439 |

Next we consider the case $r_i = 1$ for all $1 \leq i \leq m-1$ and $r_m = 2$. For $m \geq 2$, $m$-step (order) Jacobsthal numbers, $\{J_n^{(m)}(J_0^{(m)}, J_1^{(m)}, J_2^{(m)}, ..., J_{m-1}^{(m)}; 1, 1, , ..., 1, 2)\}_{n \geq m}$ (or shortly $\{J_n^{(m)}\}_{n \geq m}$), $(n \geq m)$, is defined by the $m$-order linear recurrence relation

$$J_n^{(m)} = \sum_{i=1}^{m-1} r_i J_{n-i}^{(m)} + 2J_{n-m}^{(m)} \tag{2.6}$$

with $m$ initial terms

$J_0^{(m)} = 0$ and $J_i^{(m)} = 1$ for $i = 1, 2, ..., m-1$.

For the $m$th order Jacobsthal-Lucas numbers $j_n^{(m)}$ we use the same recursion (2.6) with initial conditions $j_i^{(m)} = j_i^{(m-1)}$ for $i = 0, 1, 2, ..., m-1$ and $j_0^{(2)} = 2$, $j_1^{(2)} = 1$. See Table 2.3 and Table 2.4 for $m$th order Jacobsthal numbers and $m$th order Jacobsthal-Lucas numbers, respectively.

Table 2.3 The first few sequences of $m$th order Jacobsthal numbers.

| $m$ | Name | $n$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | second order Jacobsthal | $J_n^{(2)}$ | $\frac{3}{8}$ | $-\frac{1}{4}$ | $\frac{1}{2}$ | 0 | 1 | 1 | 3 | 5 | 11 | 21 | 43 | 85 | 171 |
| 3 | third order Jacobsthal | $J_n^{(3)}$ | $-\frac{1}{4}$ | $\frac{1}{2}$ | 0 | 0 | 1 | 1 | 2 | 5 | 9 | 18 | 37 | 73 | 146 |
| 4 | fourth order Jacobsthal | $J_n^{(4)}$ | $\frac{5}{8}$ | $\frac{1}{4}$ | $-\frac{1}{2}$ | 0 | 1 | 1 | 1 | 3 | 7 | 13 | 25 | 51 | 103 |
| 5 | fifth order Jacobsthal | $J_n^{(5)}$ | $\frac{1}{2}$ | 0 | $-1$ | 0 | 1 | 1 | 1 | 1 | 4 | 9 | 17 | 33 | 65 |

Table 2.4 The first few sequences of $m$th order Jacobsthal-Lucas numbers.

| $m$ | Name | $n$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | second order Jacobsthal-Lucas | $j_n^{(2)}$ | $-\frac{7}{8}$ | $\frac{5}{4}$ | $-\frac{1}{2}$ | 2 | 1 | 5 | 7 | 17 | 31 | 65 | 127 |
| 3 | third order Jacobsthal-Lucas | $j_n^{(3)}$ | 1 | $-1$ | 1 | 2 | 1 | 5 | 10 | 17 | 37 | 74 | 145 |
| 4 | fourth order Jacobsthal-Lucas | $j_n^{(4)}$ | $-\frac{5}{4}$ | $\frac{1}{2}$ | 1 | 2 | 1 | 5 | 10 | 20 | 37 | 77 | 154 |
| 5 | fifth order Jacobsthal-Lucas | $j_n^{(5)}$ | $\frac{1}{4}$ | $\frac{1}{2}$ | 1 | 2 | 1 | 5 | 10 | 20 | 40 | 77 | 157 |

For more details about generalized $m$-step Fibonacci numbers we refer to, for example, the works in [14-16], among others. Now, we consider the cases $m = 2, 3, 4, 5$ of the generalized $m$-step Fibonacci numbers separately.

Horadam sequence (generalized Fibonacci sequence) $\{V_n(V_0, V_1; r, s)\}_{n \geq 0}$ (or shortly $\{V_n\}_{n \geq 0}$) is defined as follows:

$$V_n = rV_{n-1} + sV_{n-2}, \qquad V_0 = c_0, V_1 = c_1, \quad n \geq 2 \tag{2.7}$$

where $V_0, V_1$ are arbitrary reel or complex numbers and $r, s$ are real numbers. The sequence $\{V_n\}_{n \geq 0}$ can be extended to negative subscripts by defining

$$V_{-n} = -\frac{r}{s} V_{-(n-1)} + \frac{1}{s} V_{-(n-2)}$$

for $n = 1, 2, 3, ...$ when $s \neq 0$. Therefore, recurrence (2.7) holds for all integer $n$. See Table 2.5 for a few members of Horadam sequences.

Table 2.5 A few members of Horadam sequences.

| Sequences (Numbers) | Notation |
|---|---|
| Fibonacci | $\{F_n\} = \{V_n(0, 1; 1, 1)\}$ |
| Lucas | $\{L_n\} = \{V_n(2, 1; 1, 1)\}$ |
| Pell | $\{P_n\} = \{V_n(0, 1; 2, 1)\}$ |
| Pell-Lucas | $\{Q_n\} = \{V_n(2, 2; 2, 1)\}$ |
| second order Jacobsthal | $\{J_n\} = \{V_n(0, 1; 1, 2)\}$ |
| second order Jacobsthal-Lucas | $\{j_n\} = \{V_n(2, 1; 1, 2)\}$ |

The first few values of the sequences with non-negative indices are shown below (see Table 2.6).

Table 2.6 A few values of Horadam sequences with non-negative and negative indices

| $n$ | $-7$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_n$ | 13 | $-8$ | 5 | $-3$ | 2 | $-1$ | 1 | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 |
| $L_n$ | $-29$ | 18 | $-11$ | 7 | $-4$ | 3 | $-1$ | 2 | 1 | 3 | 4 | 7 | 11 | 18 | 29 |
| $P_n$ | 169 | $-70$ | 29 | $-12$ | 5 | $-2$ | 1 | 0 | 1 | 2 | 5 | 12 | 29 | 70 | 169 |
| $Q_n$ | $-478$ | 198 | $-82$ | 34 | $-14$ | 6 | $-2$ | 2 | 2 | 6 | 14 | 34 | 82 | 198 | 478 |
| $J_n$ | $\frac{43}{128}$ | $-\frac{21}{64}$ | $\frac{11}{32}$ | $-\frac{5}{16}$ | $\frac{3}{8}$ | $-\frac{1}{4}$ | $\frac{1}{2}$ | 0 | 1 | 1 | 3 | 5 | 11 | 21 | 43 |
| $j_n$ | $-\frac{127}{128}$ | $\frac{65}{64}$ | $-\frac{31}{32}$ | $\frac{17}{16}$ | $-\frac{7}{8}$ | $\frac{5}{4}$ | $-\frac{1}{2}$ | 2 | 1 | 5 | 7 | 17 | 31 | 65 | 127 |

The generalized Tribonacci sequence $\{V_n(V_0, V_1, V_2; r, s, t)\}_{n\geq 0}$ (or shortly $\{V_n\}_{n\geq 0}$) is defined as follows:

$$V_n = rV_{n-1} + sV_{n-2} + tV_{n-3}, \qquad V_0 = c_0, V_1 = c_1, V_2 = c_2, \quad n \geq 3 \tag{2.8}$$

where $V_0, V_1, V_2$ are arbitrary reel or complexs numbers and $r, s, t$ are real numbers. The sequence $\{V_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$V_{-n} = -\frac{s}{t}V_{-(n-1)} - \frac{r}{t}V_{-(n-2)} + \frac{1}{t}V_{-(n-3)}$$

for $n = 1, 2, 3, ...$ when $t \neq 0$. Therefore, recurrence (2.8) holds for all integer $n$.

In literature, for example, the following names and notations (see Table 2.7) are used for the special case of $r, s, t$ and initial values.

Table 2.7 A few members of generalized Tribonacci sequences.

| Sequences (Numbers) | Notation |
|---|---|
| Tribonacci | $\{T_n\} = \{V_n(0,1,1;1,1,1)\}$ |
| Tribonacci-Lucas | $\{K_n\} = \{V_n(3,1,3;1,1,1)\}$ |
| Padovan (Cordonnier) | $\{P_n\} = \{V_n(1,1,1;0,1,1)\}$ |
| Pell-Padovan | $\{R_n\} = \{V_n(1,1,1;0,2,1)\}$ |
| Jacobsthal-Padovan | $\{JP_n\} = \{V_n(1,1,1;0,1,2)\}$ |
| Perrin | $\{Q_n\} = \{V_n(3,0,2;0,1,1)\}$ |
| Pell-Perrin | $\{pQ_n\} = \{V_n(3,0,2;0,2,1)\}$ |
| Jacobsthal-Perrin | $\{JQ_n\} = \{V_n(3,0,2;0,1,2)\}$ |
| Padovan-Perrin | $\{S_n\} = \{V_n(0,0,1;0,1,1)\}$ |
| Narayana | $\{N_n\} = \{V_n(0,1,1;1,0,1)\}$ |
| third order Jacobsthal | $\{J_n\} = \{V_n(0,1,1;1,1,2)\}$ |
| third order Jacobsthal-Lucas | $\{j_n\} = \{V_n(2,1,5;1,1,2)\}$ |

The first few values of the sequences with non-negative and negative indices are shown below (see Table 2.8).

Table 2.8 A few values of generalized Tribonacci sequences.

| $n$ | $-7$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_n$ | $1$ | $-3$ | $2$ | $0$ | $-1$ | $1$ | $0$ | $0$ | $1$ | $1$ | $2$ | $4$ | $7$ | $13$ | $24$ |
| $K_n$ | $-15$ | $11$ | $-1$ | $-5$ | $5$ | $-1$ | $-1$ | $3$ | $1$ | $3$ | $7$ | $11$ | $21$ | $39$ | $71$ |
| $P_n$ | $1$ | $-1$ | $1$ | $0$ | $0$ | $1$ | $0$ | $1$ | $1$ | $1$ | $2$ | $2$ | $3$ | $4$ | $5$ |
| $R_n$ | $-41$ | $25$ | $-15$ | $9$ | $-5$ | $3$ | $-1$ | $1$ | $1$ | $1$ | $3$ | $3$ | $7$ | $9$ | $17$ |
| $JP_n$ | $-\frac{3}{64}$ | $-\frac{1}{32}$ | $\frac{5}{16}$ | $-\frac{1}{8}$ | $\frac{1}{4}$ | $\frac{1}{2}$ | $0$ | $1$ | $1$ | $1$ | $3$ | $3$ | $5$ | $9$ | $11$ |
| $Q_n$ | $-1$ | $-2$ | $4$ | $-3$ | $2$ | $1$ | $-1$ | $3$ | $0$ | $2$ | $3$ | $2$ | $5$ | $5$ | $7$ |
| $pQ_n$ | $-96$ | $59$ | $-36$ | $22$ | $-13$ | $8$ | $-4$ | $3$ | $0$ | $2$ | $3$ | $4$ | $8$ | $11$ | $20$ |
| $JQ_n$ | $-\frac{85}{128}$ | $\frac{25}{64}$ | $\frac{19}{32}$ | $-\frac{15}{16}$ | $\frac{11}{8}$ | $\frac{1}{4}$ | $-\frac{1}{2}$ | $3$ | $0$ | $2$ | $6$ | $2$ | $10$ | $14$ | $14$ |
| $S_n$ | $-2$ | $2$ | $-1$ | $0$ | $1$ | $-1$ | $1$ | $0$ | $0$ | $1$ | $0$ | $1$ | $1$ | $1$ | $2$ |
| $N_n$ | $-2$ | $1$ | $1$ | $-1$ | $0$ | $1$ | $0$ | $0$ | $1$ | $1$ | $1$ | $2$ | $3$ | $4$ | $6$ |
| $J_n$ | $-\frac{9}{64}$ | $-\frac{9}{32}$ | $\frac{7}{16}$ | $-\frac{1}{8}$ | $-\frac{1}{4}$ | $\frac{1}{2}$ | $0$ | $0$ | $1$ | $1$ | $2$ | $5$ | $9$ | $18$ | $37$ |
| $j_n$ | $\frac{7}{16}$ | $\frac{7}{8}$ | $-\frac{5}{4}$ | $\frac{1}{2}$ | $1$ | $-1$ | $1$ | $2$ | $1$ | $5$ | $10$ | $17$ | $37$ | $74$ | $145$ |

The generalized Tetranacci sequence $\{V_n(V_0, V_1, V_2, V_3; r, s, t, u)\}_{n\geq 0}$ (or shortly $\{V_n\}_{n\geq 0}$)

is defined as follows:

$$V_n = rV_{n-1} + sV_{n-2} + tV_{n-3} + uV_{n-4}, \qquad V_0 = c_0, V_1 = c_1, V_2 = c_2, \ , V_3 = c_3, \ n \geq 4 \quad (2.9)$$

where $V_0, V_1, V_2, V_3$ are arbitrary reel or complex numbers and $r, s, t, u$ are real numbers. The sequence $\{V_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$V_{-n} = -\frac{t}{u}V_{-(n-1)} - \frac{s}{u}V_{-(n-2)} - \frac{r}{u}V_{-(n-3)} + \frac{1}{u}V_{-(n-4)}$$

for $n = 1, 2, 3, ...$ when $u \neq 0$. Therefore, recurrence (2.9) holds for all integer $n$.
In literature, for example, the following names and notations (see Table 2.9) are used for the special case of $r, s, t, u$ and initial values.

Table 2.9 A few members of generalized Tetranacci sequences.

| Sequences (Numbers) | Notation |
|---|---|
| Tetranacci | $\{M_n\} = \{V_n(0, 1, 1, 2; 1, 1, 1, 1)\}$ |
| Tetranacci-Lucas | $\{R_n\} = \{V_n(4, 1, 3, 7; 1, 1, 1, 1)\}$ |
| fourth order Jacobsthal | $\{J_n\} = \{V_n(0, 1, 1, 1; 1, 1, 1, 2)\}$ |
| fourth order Jacobsthal-Lucas | $\{j_n\} = \{V_n(2, 1, 5, 10; 1, 1, 1, 2)\}$ |

The first few values of the sequences with non-negative and negative indices are shown below (see Table 2.10).

Table 2.10 A few values of generalized Tetranacci sequences.

| $n$ | $-7$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $M_n$ | 2 | 0 | 0 | $-1$ | 1 | 0 | 0 | 0 | 1 | 1 | 2 | 4 | 8 | 15 | 29 | 56 |
| $R_n$ | $-1$ | $-1$ | $-6$ | 7 | $-1$ | $-1$ | $-1$ | 4 | 1 | 3 | 7 | 15 | 26 | 51 | 99 | 191 |
| $J_n$ | $\frac{77}{128}$ | $\frac{13}{64}$ | $-\frac{19}{32}$ | $-\frac{3}{16}$ | $\frac{5}{8}$ | $\frac{1}{4}$ | $-\frac{1}{2}$ | 0 | 1 | 1 | 1 | 3 | 7 | 13 | 25 | 51 |
| $j_n$ | $-\frac{89}{64}$ | $\frac{7}{32}$ | $\frac{7}{16}$ | $\frac{7}{8}$ | $-\frac{5}{4}$ | $\frac{1}{2}$ | 1 | 2 | 1 | 5 | 10 | 20 | 37 | 77 | 154 | 308 |

The generalized Pentanacci sequence $\{V_n(V_0, V_1, V_2, V_3, V_4; r, s, t, u, v)\}_{n\geq 0}$ (or shortly $\{V_n\}_{n\geq 0}$) is defined as follows:

$$V_n = rV_{n-1} + sV_{n-2} + tV_{n-3} + uV_{n-4} + vV_{n-5}, \quad (2.10)$$

$$V_0 = c_0, V_1 = c_1, V_2 = c_2, \ V_3 = c_3, V_4 = c_4, \ n \geq 5$$

where $V_0, V_1, V_2, V_3, V_4$ are arbitrary reel or complex numbers and $r, s, t, u$ are real numbers. The sequence $\{V_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$V_{-n} = -\frac{u}{v}V_{-n+1} - \frac{t}{v}V_{-n+2} - \frac{s}{v}V_{-n+3} - \frac{r}{v}V_{-n+4} + \frac{1}{v}V_{-n+5}$$

for $n = 1, 2, 3, ...$ when $u \neq 0$. Therefore, recurrence (2.10) holds for all integer $n$.

In literature, for example, the following names and notations (see Table 2.11) are used for the special case of $r, s, t, u, v$ and initial values.

Table 2.11 A few members of generalized Pentanacci sequences.

| Sequences (Numbers) | Notation |
|---|---|
| Pentanacci | $\{P_n\} = \{V_n(0, 1, 1, 2, 4; 1, 1, 1, 1, 1)\}$ |
| Pentanacci-Lucas | $\{Q_n\} = \{V_n(5, 1, 3, 7, 15; 1, 1, 1, 1, 1)\}$ |
| fifth order Jacobsthal | $\{J_n\} = \{V_n(0, 1, 1, 1, 1; 1, 1, 1, 1, 2)\}$ |
| fifth order Jacobsthal-Lucas | $\{j_n\} = \{V_n(2, 1, 5, 10, 20; 1, 1, 1, 1, 2)\}$ |

The first few values of the sequences with non-negative and negative indices are shown below (see Table 2.12).

Table 2.12 A few values of generalized Pentanacci sequences.

| $n$ | $-8$ | $-7$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $P_n$ | 0 | 0 | 0 | $-1$ | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 4 | 8 | 16 | 31 | 61 |
| $Q_n$ | $-1$ | $-1$ | $-7$ | 9 | $-1$ | $-1$ | $-1$ | $-1$ | 5 | 1 | 3 | 7 | 15 | 31 | 57 | 113 | 223 |
| $J_n$ | $\frac{31}{64}$ | $-\frac{1}{32}$ | $-\frac{17}{16}$ | $-\frac{1}{8}$ | $\frac{3}{4}$ | $\frac{1}{2}$ | 0 | $-1$ | 0 | 1 | 1 | 1 | 1 | 4 | 9 | 17 | 33 |
| $j_n$ | $\frac{13}{128}$ | $\frac{13}{64}$ | $\frac{13}{32}$ | $\frac{13}{16}$ | $-\frac{11}{8}$ | $\frac{1}{4}$ | $\frac{1}{2}$ | 1 | 2 | 1 | 5 | 10 | 20 | 40 | 77 | 157 | 314 |

## 2.2 SPECIAL CASES OF THE GENERALIZED $m$-STEP FIBONACCI SEQUENCE

In this section, we will give some basic information about special cases of the generalized $m$-step Fibonacci sequence.

### 2.2.1 Fibonacci and Lucas Numbers

We will use the information in [17] in the subsection.

Fibonacci and Lucas numbers are defined by

$$F_{n+1} = F_n + F_{n-1},\ n \geq 1,\ F_0 = 0,\ F_1 = 1$$

$$L_{n+1} = L_n + L_{n-1},\ n \geq 1,\ L_0 = 2,\ L_1 = 1$$

respectively. Also, The Fibonacci $Q$-matrix and the $R$-matrix are defined as follws:

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } R = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}.$$

$n$.th power of the Fibonacci $Q$-matrix has the following form:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Using the Fibonacci $Q$-matrix and the $R$-matrix, it was obtained the matrix $R_n$ of the following form:

$$R_n = RQ^n = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix}.$$

### 2.2.2 $m$-Step Fibonacci Numbers

In this section, we will give information from [18].

The $m$-step Fibonacci sequence is given by the $m^{th}$ order recurrence relation:

$$F_{n+m} = F_{n+m-1} + F_{n+m-2} + \ldots + F_{n+1} + F_n,\ n \geq 0,\ m \in \mathbb{Z}^+ \tag{2.11}$$

with initial values $F_i = 0$, $F_{m-1} = 1$ for $i = 0, 1, 2, \ldots, m-2$.

The corresponding multinacci $\boldsymbol{F}_m$ matrix of order $m$, given by

$$\begin{aligned} \boldsymbol{F}_m &= \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}_{m\times m} \\ &= \begin{pmatrix} F_m & F_{m-1} + \ldots + F_1 & F_{m-1} + \ldots + F_2 & \ldots & F_{m-1} \\ F_{m-1} & F_{m-2} + \ldots + F_0 & F_{m-2} + \ldots + F_1 & \ldots & F_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_2 & F_1 + \ldots + F_{1-(m-2)} & F_1 + \ldots + F_{1-(m-3)} & \ldots & F_1 \\ F_1 & F_0 + \ldots + F_{0-(m-2)} & F_0 + \ldots + F_{0-(m-3)} & \ldots & F_0 \end{pmatrix}_{m\times m}. \end{aligned}$$

It can be easily seen that

$$\boldsymbol{F}_m^n = \begin{pmatrix} F_{n+m-1} & F_{n+m-2}+\ldots+F_n & F_{n+m-2}+\ldots+F_{n+1} & \ldots & F_{n+m-2} \\ F_{n+m-2} & F_{n+m-3}+\ldots+F_{n-1} & F_{n+m-3}+\ldots+F_n & \ldots & F_{n+m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{n+1} & F_n+\ldots+F_{n-(m-2)} & F_n+\ldots+F_{n-(m-3)} & \ldots & F_n \\ F_n & F_{n-1}+\ldots+F_{(n-1)-(m-2)} & F_{n-1}+\ldots+F_{(n-1)-(m-3)} & \ldots & F_{n-1} \end{pmatrix}_{m\times m} \tag{2.12}$$

is by the mathematical induction method.

Also note that

$$\boldsymbol{F}_{m}^{-n}=\begin{pmatrix} F_{-n+m-1} & F_{-n+m-2}+\ldots+F_{-n} & F_{-n+m-2}+\ldots+F_{-n+1} & \ldots & F_{-n+m-2} \\ F_{-n+m-2} & F_{-n+m-3}+\ldots+F_{n-1} & F_{-n+m-3}+\ldots+F_{n} & \ldots & F_{-n+m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{-n+1} & F_{-n}+\ldots+F_{-n-(m-2)} & F_{-n}+\ldots+F_{-n-(m-3)} & \ldots & F_{-n} \\ F_{-n} & F_{-n-1}+\ldots+F_{(-n-1)-(m-2)} & F_{-n-1}+\ldots+F_{(-n-1)-(m-3)} & \ldots & F_{-n-1} \end{pmatrix}_{m\times m}.$$

### 2.2.3 Padovan Numbers

We will use the information in [19] in the subsection.

The Padovan numbers $P_n$ are defined by the recurrence relation

$$P_{n+3}=P_{n+1}+P_n, \quad P_0=1, P_1=1, P_2=1.$$

The sequences $\{P_n\}_{n\geq 0}$, can be extended to negative subscripts by defining

$$P_{-n}=-P_{-(n-1)}+P_{-(n-3)}.$$

The characteristic equation associated with Padovan sequences is $x^3-x-1=0$ with roots $\alpha$, $\beta$ and $\gamma$ in which

$$\alpha=(\frac{1}{2}+\sqrt{\frac{23}{108}})^{1/3}+(\frac{1}{2}-\sqrt{\frac{23}{108}})^{1/3}\simeq 1.32471795724$$

is called plastic number (or plastic ratio or plastic constant or silver number) and

$$\lim_{n\longrightarrow\infty}\frac{P_{n+1}}{P_n}=\alpha.$$

The plastic number is used in art and architecture. Moreover Padovan numbers $P_n$ and plastic number $\alpha$ play a very important role in the construction of Padovan coding theory.

### 2.2.4 Third Order Jacobsthal Numbers

The third order Jacobsthal sequence [16] is the sequence of integers $J_n$ defined by the initial $J_0=0$, $J_1=1$, $J_2=1$ and the recurrence relation

$$J_n=J_{n-1}+J_{n-2}+2J_{n-3},\ n\geq 3.$$

The third order Jacobsthal numbers have the $\mathbf{J}$ matrix, where

$$\boldsymbol{J}=\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \det(\mathbf{J})=2.$$

Note that

$$\boldsymbol{J}^n = \begin{pmatrix} J_{n+1} & J_n + 2J_{n-1} & 2J_n \\ J_n & J_{n-1} + 2J_{n-2} & 2J_{n-1} \\ J_{n-1} & J_{n-2} + 2J_{n-3} & 2J_{n-2} \end{pmatrix}.$$

### 2.2.5 Jacobsthal Numbers and $\lambda$-Step Jacobsthal Numbers

The Jacobsthal sequence [16] is the sequence of the integers $J_n$ defined by the initial $J_0 = 0$, $J_1 = 1$ and the recurrence relation

$J_n = J_{n-1} + 2J_{n-2}$, for $n \geq 2$.

The Jacobsthal numbers have the

$$\begin{aligned} \boldsymbol{J}_2 &= \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}, \boldsymbol{J}_2^n = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} J_{n+1} & 2J_n \\ J_n & 2J_{n-1} \end{pmatrix}, \\ \det(\boldsymbol{J}_2^n) &= (-2)^n = (-1)^n 2^n. \end{aligned}$$

Also, we have

$$\begin{aligned} (\boldsymbol{J}_2^n)^{-1} &= (\boldsymbol{J}_2)^{-n} = \begin{pmatrix} -\frac{J_{n-1}}{J_n^2 - J_{n-1}J_{n+1}} & \frac{J_n}{J_n^2 - J_{n-1}J_{n+1}} \\ \frac{J_n}{2J_n^2 - 2J_{n-1}J_{n+1}} & -\frac{1}{2J_n^2 - 2J_{n-1}J_{n+1}} J_{n+1} \end{pmatrix} = \begin{pmatrix} J_{-n+1} & 2J_{-n} \\ J_{-n} & 2J_{-n-1} \end{pmatrix}, \\ J_{-n} &= \frac{(-1)^{n+1} J_n}{2^n}, (n = 0, 1, 2, \ldots). \end{aligned}$$

The $\lambda$-step Jacobsthal sequence [16] is given by the $\lambda^{th}$ order recurrence relation:

$$J_{n+\lambda} = J_{n+\lambda-1} + J_{n+\lambda-2} + \ldots + J_{n+1} + 2J_n,\ n \geq 0,\ \lambda \in \mathbb{Z}^+ \tag{2.13}$$

with initial values $J_0 = 0$, $J_i = 1$ for $i = 1, 2, \ldots, \lambda - 1$.

The corresponding $\boldsymbol{J}_\lambda$ matrix of order $\lambda$, given by

$$\begin{aligned} \boldsymbol{J}_\lambda &= \begin{pmatrix} 1 & 1 & \ldots & 1 & 2 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}_{\lambda \times \lambda} \\ &= \begin{pmatrix} J_\lambda & J_{\lambda-1} + \ldots + 2J_1 & J_{\lambda-1} + \ldots + 2J_2 & \ldots & 2J_{\lambda-1} \\ J_{\lambda-1} & J_{\lambda-2} + \ldots + 2J_0 & J_{\lambda-2} + \ldots + 2J_1 & \ldots & 2J_{\lambda-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ J_2 & J_1 + \ldots + 2J_{1-(\lambda-2)} & J_1 + \ldots + 2J_{1-(\lambda-3)} & \ldots & 2J_1 \\ J_1 & J_0 + \ldots + 2J_{0-(\lambda-2)} & J_0 + \ldots + 2J_{0-(\lambda-3)} & \ldots & 2J_0 \end{pmatrix}. \end{aligned}$$

Also, we obtain

$$(\boldsymbol{J}_\lambda)^n = \begin{pmatrix} J_{n+\lambda-2} & J_{n+\lambda-3}+\ldots+2J_{n-1} & J_{n+\lambda-3}+\ldots+2J_n & \ldots & 2J_{n+\lambda-3} \\ J_{n+\lambda-3} & J_{n+\lambda-4}+\ldots+2J_{n-2} & J_{n+\lambda-4}+\ldots+2J_{n-1} & \ldots & 2J_{n+\lambda-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ J_n & J_{n-1}+\ldots+2J_{(n-1)-(\lambda-2)} & J_{n-1}+\ldots+2J_{(n-1)-(\lambda-3)} & \ldots & 2J_{n-1} \\ J_{n-1} & J_{n-2}+\ldots+2J_{(n-2)-(\lambda-2)} & J_{n-2}+\ldots+2J_{(n-2)-(\lambda-3)} & \ldots & 2J_{n-2} \end{pmatrix}, \tag{2.14}$$

$\det(\boldsymbol{J}_\lambda) = 2.(-1)^{\lambda-1} \Longrightarrow \det(\boldsymbol{J}_\lambda^n) = 2^n(-1)^{(\lambda-1).n}$

and

$$(\boldsymbol{J}_\lambda)^{-n} = \begin{pmatrix} J_{-n+\lambda-2} & J_{-n+\lambda-3}+\ldots+2J_{-n-1} & J_{-n+\lambda-3}+\ldots+2J_{-n} & \ldots & 2J_{-n+\lambda-3} \\ J_{-n+\lambda-3} & J_{-n+\lambda-4}+\ldots+2J_{-n-2} & J_{-n+\lambda-4}+\ldots+2J_{-n-1} & \ldots & 2J_{-n+\lambda-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ J_{-n} & J_{-n-1}+\ldots+2J_{(-n-1)-(\lambda-2)} & J_{-n-1}+\ldots+2J_{(-n-1)-(\lambda-3)} & \ldots & 2J_{-n-1} \\ J_{-n-1} & J_{-n-2}+\ldots+2J_{(-n-2)-(\lambda-2)} & J_{-n-2}+\ldots+2J_{(-n-2)-(\lambda-3)} & \ldots & 2J_{-n-2} \end{pmatrix}. \tag{2.15}$$

**Lemma 2.1** *Let $p$ is prime and $\boldsymbol{J}$ is generalized Jacobsthal matrix, then*

$$\det(\boldsymbol{J})(\mathrm{mod}\, p) = \det(\boldsymbol{J}(\mathrm{mod}\, p)). \tag{2.16}$$

Proof. It can be easily seen using the matrix, determinant, and modular arithmetic properties. □

### 2.2.6 Third Order Pell Numbers

The third order Pell sequence [20] is the sequence of integers $P_n$ defined by the initial $P_0 = 0$, $P_1 = 1$, $P_2 = 2$ and the recurrence relation

$P_n = 2P_{n-1} + P_{n-2} + P_{n-3}$, $n \geq 3$.

The third order Pell numbers have the $\mathbf{P}$ matrix, where

$$\mathbf{P} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \det(\mathbf{P}) = 1.$$

It can be easily seen that is by mathematical induction.

$$\mathbf{P}^n = \begin{pmatrix} P_{n+1} & P_n + P_{n-1} & P_n \\ P_n & P_{n-1} + P_{n-2} & P_{n-1} \\ P_{n-1} & P_{n-2} + P_{n-3} & P_{n-2} \end{pmatrix}$$

is by mathematical induction.

### 2.2.7 Pell Numbers and $\lambda$-Step Pell Numbers

The Pell sequence [21] is the sequence of the integers $P_n$ defined by the initial $P_0 = 0$, $P_1 = 1$ and the recurrence relation

$P_n = 2P_{n-1} + P_{n-2}, P_0 = 0, P_1 = 1$ for $n \geq 2$.

The Pell numbers have the

$$\begin{aligned} \boldsymbol{P}_2 &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \boldsymbol{P}_2^n = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{pmatrix}, \\ \det(\boldsymbol{P}_2^n) &= (-1)^n = (-1)^n. \end{aligned}$$

Also, we have

$$\begin{aligned} (\boldsymbol{P}_2^n)^{-1} &= (\boldsymbol{P}_2)^{-n} = \begin{pmatrix} -\frac{P_{n-1}}{P_n^2 - P_{n-1}P_{n+1}} & \frac{P_n}{P_n^2 - P_{n-1}P_{n+1}} \\ \frac{P_n}{P_n^2 - P_{n-1}P_{n+1}} & -\frac{P_{n+1}}{P_n^2 - P_{n-1}P_{n+1}} \end{pmatrix} = \begin{pmatrix} P_{-n+1} & -P_{-n} \\ -P_{-n} & P_{-n-1} \end{pmatrix}, \\ P_{-n} &= (-1)^{n+1} P_n, \ (n = 0, 1, 2, \ldots). \end{aligned}$$

The $\lambda$-step Pell sequence [21] is given by the $\lambda^{th}$ order recurrence relation:

$$P_{n+\lambda} = 2P_{n+\lambda-1} + P_{n+\lambda-2} + \ldots + P_{n+1} + P_n, \ n \geq 0, \ \lambda \in \mathbb{Z}^+ \tag{2.17}$$

with initial values , for $1 - \lambda \leq n \leq 0$

$$P_n^i = \begin{cases} 1 & , \quad \text{if } i = 1 - n \\ 0 & , \quad \text{otherwise} \end{cases}$$

, where $P_n^i$ is the $n$th term of the $i$th generalized order-$\lambda$ Pell sequence.

The corresponding multinacci $\boldsymbol{P}_\lambda$ matrix of order $\lambda$, given by

$$\begin{aligned} \boldsymbol{P}_\lambda &= \begin{pmatrix} 2 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}_{\lambda \times \lambda} \\ &= \begin{pmatrix} P_\lambda & P_{\lambda-1} + \ldots + P_1 & P_{\lambda-1} + \ldots + P_2 & \ldots & P_{\lambda-1} \\ P_{\lambda-1} & P_{\lambda-2} + \ldots + P_0 & P_{\lambda-2} + \ldots + P_1 & \ldots & P_{\lambda-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_2 & P_1 + \ldots + P_{1-(\lambda-2)} & P_1 + \ldots + P_{1-(\lambda-3)} & \ldots & P_1 \\ P_1 & P_0 + \ldots + P_{0-(\lambda-2)} & P_0 + \ldots + P_{0-(\lambda-3)} & \ldots & P_0 \end{pmatrix}_{\lambda \times \lambda}. \end{aligned}$$

$$(\boldsymbol{P}_\lambda)^n=\begin{pmatrix} P_{n+\lambda-1} & P_{n+\lambda-2}+\ldots+P_n & P_{n+\lambda-2}+\ldots+P_{n+1} & \ldots & P_{n+\lambda-2} \\ P_{n+\lambda-2} & P_{n+\lambda-3}+\ldots+P_{n-1} & P_{n+\lambda-3}+\ldots+P_n & \ldots & P_{n+\lambda-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{n+1} & P_n+\ldots+P_{n-(\lambda-2)} & P_n+\ldots+P_{n-(\lambda-3)} & \ldots & P_n \\ P_n & P_{n-1}+\ldots+P_{(n-1)-(\lambda-2)} & P_{n-1}+\ldots+P_{(n-1)-(\lambda-3)} & \ldots & P_{n-1} \end{pmatrix}_{\lambda\times\lambda}, \tag{2.18}$$

$$\det(\boldsymbol{P}_\lambda)=(-1)^{\lambda-1} \Longrightarrow \det(\boldsymbol{J}_\lambda^n)=(-1)^{(\lambda-1).n}$$

and

$$(\boldsymbol{P}_\lambda)^{-n}=\begin{pmatrix} P_{-n+\lambda-1} & P_{-n+\lambda-2}+\ldots+P_{-n} & P_{-n+\lambda-2}+\ldots+P_{-n+1} & \ldots & P_{-n+\lambda-2} \\ P_{-n+\lambda-2} & P_{-n+\lambda-3}+\ldots+P_{-n-1} & P_{-n+\lambda-3}+\ldots+P_{-n} & \ldots & P_{-n+\lambda-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{-n+1} & P_{-n}+\ldots+P_{-n-(\lambda-2)} & P_{-n}+\ldots+P_{-n-(\lambda-3)} & \ldots & P_{-n} \\ P_{-n} & P_{-n-1}+\ldots+P_{(-n-1)-(\lambda-2)} & P_{-n-1}+\ldots+P_{(-n-1)-(\lambda-3)} & \ldots & P_{-n-1} \end{pmatrix}_{\lambda\times\lambda}. \tag{2.19}$$

**Lemma 2.2** *Let $p$ is prime and $\boldsymbol{P}$ is generalized Pell matrix, then*

$$\det(\boldsymbol{P})(\mathrm{mod}\, p)=\det(\boldsymbol{P}(\mathrm{mod}\, p)). \tag{2.20}$$

Proof. It can be easily seen using the matrix, determinant, and modular arithmetic properties. □

### 2.2.8 3-Primes Numbers and Circulant Matrices

In this section we will give information from [20, 22-23].

The generalized $(r,s,t)$ sequence (or generalized Tribonacci sequence orgeneralized 3-step Fibonacci sequence)

$$\{W_n(W_0,W_1,W_2;r,s,t)\}_{n\geq 0}$$

(or shortly $\{W_n\}_{n\geq 0}$) is defined as follows:

$$W_n=rW_{n-1}+sW_{n-2}+tW_{n-3},\ W_0=a,W_1=b,W_2=c,\ n\geq 3 \tag{2.21}$$

where $W_0,W_1,W_2$ are arbitrary complex (or real) numbers and $r,s,t$ are real numbers. In this paper we consider the case $r=2,s=3,t=5$ and in this case we write $V_n=W_n$. A $3-primes$ sequence $\{G_n\}_{n\geq 0}=\{G_n(G_0,G_1,G_2)\}_{n\geq 0}$ is defined by the third-order recurrence relations

$$G_n=2G_{n-1}+3G_{n-2}+5G_{n-3} \tag{2.22}$$

with the initial values $G_0 = 0, G_1 = 1, G_2 = 2$.

Let $n \geq 2$ be an integer. An $n \times n$ matrix $C = (c_{ij}) \in M_{n\times n}(\mathbb{C})$ is called a circulant matrix if it is of the form

$$\boldsymbol{C} = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-3} & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_{n-1} & c_0 \end{pmatrix}_{n\times n}$$

i.e.

$$c_{ij} = \begin{cases} c_{j-i} & , \quad j \geq i \\ c_{n+j-i} & , \quad j < i \end{cases}$$

and the circulant matrix $\boldsymbol{C}$ is denoted by $\boldsymbol{C} = \mathrm{Circ}(c_0, c_1, ..., c_{n-1})$. Circulant matrix was first proposed by Davis in [24].

**Definition 2.1** *A, $n\times n$ circulant matrix with generalized $(r, s, t)$ (generalized Tribonacci) numbers entries is defined by*

$$\begin{aligned} \boldsymbol{C}_n(W) &= \begin{pmatrix} W_0 & W_1 & W_2 & \cdots & W_{n-2} & W_{n-1} \\ W_{n-1} & W_0 & W_1 & \cdots & W_{n-3} & W_{n-2} \\ W_{n-2} & W_{n-1} & W_0 & \cdots & W_{n-4} & W_{n-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ W_1 & W_2 & W_3 & \cdots & W_{n-1} & W_0 \end{pmatrix}_{n\times n} \\ &= \mathrm{Cir}c(W_0, W_1, \ldots, W_{n-1}). \end{aligned}$$

### 2.2.9 Balancing Numbers

Behera and Panda [25] defined balancing numbers $n$ as solutions of the diophantine equation

$$1 + 2 + \cdots + (n-1) = (n+1) + (n+2) + \cdots + (n+r),$$

for some natural number $r$, called the balancer corresponding to $n$. The $n$th balancing number is denoted by $B_n$. In fact, $B_n$ satisfy the second order linear recurrence relation

$$B_n = 6B_{n-1} - B_{n-2}, \quad B_0 = 0,\ B_1 = 1.$$

The $Q$-matrix was first studied by Charles H. King [26] in 1960. The $Q$-matrix is given as

$$Q_B = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2.23}$$

**Theorem 2.3** *[27] Let $Q_B$ be the balancing $Q$-matrix given in (2.23). Then for every positive integer $n$*

$$Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix},$$

*where $B_n$ is the $n$th balancing number.*

The importance of number sequences in cryptography is increasing day by day. Many authors have studied on the use of number sequences in cryptology in recent years, see for example, [17, 28-41].

# CHAPTER 3

# INTRODUCTION TO CRYPTOGRAPHY

Coding and secret encryption have been used by governments, armies, and private individuals since ancient times. Until recently, it was used in limited fields such as military, espionage, business, and commerce. Afterwards, the development of the banking sector, credit card information, contracts, and sending important information in medicine and different fields over open communication channels forced cryptography to develop and caused this discipline to develop new techniques. Some of these developments are: The increased capacity of computers and computing has allowed for more complex cryptosystems that cannot be done manually and can be done on the computer. As cryptoanalysis was developed by computers, more complex systems were produced. With the discovery of the public key technique, the security of public communication channels has been increased. Recent developments in the field of cryptology have made it an important discipline in both mathematics and computer science and engineering. In mathematics, cryptology is applied in different sub-fields such as algebra, number theory, graph theory, algebraic geometry, probability, and statistics. Analysis of cryptographic security has led to the use of theoretical computer science and complexity theory in particular. Because an important aspect of encryption protocols is their security. That is the ability to withstand attacks. Since modern cryptography is done on a computer, cryptographic security uses on computer science and complexity theory.
In this chapter, we will present a brief history of cryptography and some basic information about cryptography in [1, 42- 48].

## 3.1 A BRIEF HISTORY OF CRYPTOGRAPHY

Cryptography and encryption have a long history. Until recently, cryptography was mainly concerned with message privacy. It was primarily used in military and espionage situations. Later, this field expanded to different cryptographic techniques such as digital

signatures and message authentication.

The Bible also uses what is called the Atabash code in the book of Jeremiah. Kabbalists and Kabbalah believe that each letter of the Bible also represents a number and is a code from heaven. They have developed different ways to decipher it.

Julius Caesar used to send encrypted messages in military situations. This method he developed was called the Caesar code. This is a swipe password. That is, each letter is shifted to the right by a certain amount. The Caesar code resurfaced and was used during the years of the American Civil War.

Encoded messages produced by most historical methods reveal statistical data about plain text. This data often helps crack the codes. In the ninth century, the Arab mathematician Al-Kindi developed frequency analysis and made basic classical ciphers almost easily crackable.

During the Middle Ages, political intrigues led to the development of ciphers, and the employment of codes and codebooks became common in diplomacy. In the 1470s, Leon Alberti devised a strategy to avoid statistical analysis. This is a multi-alphabet cipher, which encrypts different parts of the message using different alphabets. This is an illustration of a polyalphabetic coding. A century later, this strategy was mistakenly referred to Vigenere. J. Trithemius and G. B. Belasso worked extensively on polyalphabetic codes in the 16th century.

Another way to prevent statistical attacks is to use spaces or nonsense letters in the message. Mary, Queen of Scots, used a random cipher containing meaningless symbols. But unfortunately, their messages were decrypted, and the outcome was not good for the queen.

Before computers, various physical devices began to be used for cryptography. The most famous of these was the Enigma device, developed by the German army during the Second World War. It was a machine built on a polyalphabetic system. It was cracked by Polish cryptographers. For this reason, a more difficult system was established, but later British cryptographers led by Alan Turing broke it as well.

With the development of computers, more complex encryption systems have been developed. In addition, cryptanalysis, that is, the ability to break cryptosystems, has developed thanks to computers. In 1976, Diffie and Hellman developed the first key exchange protocol. This allowed the transmission of confidential data over open air routes.

Later, Rivest, Adelman, and Shamir developed the RSA key exchange algorithm. Both Diffie-Hellman and RSA require very large key spaces. It is suggested to apply Diffie-Hellman to other commutative groups in order to reduce the key space size. For this reason, algebraic geometry is included in cryptography. In 1985, Neil Koblitz and Victor Miller independently used elliptic curves on finite fields and their corresponding groups in cryptography. This method provided faster encryption and created smaller key gaps.
As cryptography applications became widespread and evolved, it was felt that there should be an encryption standard. In 1976, the Data Encryption Standard (DES) was adopted as the symmetric key encryption standard. DES is what is called a block cipher. DES is now insecure for many applications. There were successful attacks in 1999. Thereupon, a competition was held for a secure system, and the system developed by Rijmen and Daemen won the competition. This method is called the Rijndael cipher. In 2001, the United States National Institute of Standards and Technology adopted a standardization of the Rijndael cipher, called the Advanced Encryption Standard (AES), for symmetric key encryption.
In recent years, the ideas of quantum algorithms have prompted researchers to work on public key methods using non-commutative groups. With the development of quantum computers, quantum cryptography will develop further.
I will introduce basic information and citations relating to cryptography.

## 3.2 BASIC TERMINOLOGY

- An *algorithm* is a finite sequence of well-defined, computer-implementable instructions in mathematics and computer science.

- In cryptography, the original unencrypted text is called *plain text*.

- The algorithm used to convert plain text to ciphertext is called *cipher*.

- Encoded or encrypted text is called *cipher text*.

- The art of encrypting a message with the appropriate algorithm and key is called *cryptography*.

- The study of the principles and methods of deciphering the ciphertext without knowing the key or the algorithm is called *cryptanalysis*.

- Although cryptology is used synonymously with cryptography in some books, cryptology is more comprehensive. That is, *cryptology* includes cryptography and cryptanalysis.

- *Encryption* is an operation that transforms a generic message, $M$, into a cryptogram, $C$, applying a function, $f$:

  $M \longrightarrow f(M) \longrightarrow C.$

- *Decryption* is an operation that returns the message in cleartext, $M$, from the cryptogram, $C$, applying a function, $g$:

  $C \longrightarrow g(C) \longrightarrow M.$

  The $f$ and $g$ functions are inverses of each other. That is, the function $f$ is injective.

- The information, usually some type of number, used with the algorithm to encrypt or decrypt the message is called a *key*.

- The total number of possible keys that can be used is called the *keyspace*.

- *Symmetric encryption* uses only one shared key to both encrypt and decrypt the message.

- *Asymmetric encryption* implements more parameters to generate a public key (to encrypt the message) and just one private key to decrypt the message.

Now that we understand the main concepts of cryptography, we can explain the difference between private and public keys.

## 3.3 PRIVATE AND PUBLIC KEYS

### 3.3.1 Private Key

For thousands of years, cryptography has been used to provide confidential communication between trusted parties. Usually, two people, X and Y, agree on a particular secret key. Then X can send a secret message to Y (or if Y sends a message to X). Keys are used to convert the original message (often called plain text) into an encrypted form that is incomprehensible to those who do not have the key. This is known as encryption, and encrypted messages are known as ciphertext. Once Y has the ciphertext, it can use the key to convert the ciphertext back to plain text. This is the decryption method. An encryption system generates a comprehensive key specification and describes how it is used to encrypt and decrypt data. Throughout history, several cryptographic systems of increasing complexity have been utilized for a variety of purposes. Covert communication between political leaders, military activities, and other applications are notable. However, as applications such as the internet and e-commerce have evolved, numerous new and diverse applications have emerged. Encryption of passwords, credit card numbers, email, papers, files, and digital media are examples of such instances.

Also, keep in mind that, in addition to data transferred from one party to another, encryption techniques are also commonly used to protect stored data. For example, users can use laptops, external hard drives, clouds, databases, and more. You may want to encrypt your stored data.

Security concerns must be addressed in the design and implementation of cryptographic systems. Traditionally, threat encryption entails listening in on enemy threats that capture the ciphertext and attempt to decipher it. Nothing can be done if the other person holds the key. So the most essential security issue is an adversary that lacks the key and attempts to crack the ciphertext. The method used by a competitor to "crack" a cryptosystem is known as cryptanalysis. Attempting to guess the key is the most obvious sort of cryptanalysis. An exhaustive key lookup attack occurs when an attacker attempts to decode the ciphertext using all available keys in sequence. If an adversary uses the proper key, the plaintext will be found; but, if a different key is used, the "decrypted" ciphertext may be nonsensical. As a result, identifying a large number of viable keys is the first stage in building a safe cryptographic system. Inadequate keys make it impossi-

ble to test against an adversary in a fair length of time. The encryption model described above is referred to as secret key encryption. This shows that X and Y are both aware of the secret key. As a result, the key is a "secret" known to both parties. This key is used to encrypt plain text as well as decrypt ciphertext. As a result, the encryption and decryption functions are inverses of one another.

### 3.3.2 Public Key

Diffie and Hellman introduced the idea of public key encryption in the 1970s. They reasoned that it would be feasible to create an encryption system with two distinct keys. The public key is used to encrypt the plaintext, while the private key is used to decode the ciphertext. The public key is known to "everyone," while the private key is only known to one person (i.e., the recipient of the encrypted message). As a result, with public-key cryptosystems, anybody can encrypt a message, for example, send it to Bob and only Y can decrypt it. The first and most famous example of a public-key encryption system is the RSA encryption system, invented by Rivest, Shamir, and Adleman.

Public key encryption eliminates the need for two parties to agree on a pre-shared secret key. However, a method must be developed for the secure distribution of public keys. However, this is not necessarily a trivial goal. The main issue is the accuracy or authenticity of the so-called public keys.

## 3.4 CLASSICAL CRYPTOGRAPHY

### 3.4.1 Some Cryptosystems

The primary goal of cryptography is to allow two persons, commonly referred to as Alice and Bob, to communicate via an insecure channel in such a way that others cannot understand what they are saying. A telephone line or a computer network can serve as this channel. Alice uses a predefined key to encrypt the plaintext and sends the resultant ciphertext across the channel. Bob can decipher the ciphertext and recreate the plaintext by knowing the encryption key.

Now, based on these ideas, let's give the definition of a cryptosystem using mathematical notation.

**Definition 3.1** *A cryptosystem is called a five-tuple* $(M, C, K, E, D)$ *that satisfies the following conditions.*

**a)** $M$ *is a finite set of possible plaintexts.*

**b)** $C$ *is a finite set of possible ciphertexts.*

**c)** $K$*, the keyspace, is a finite set of possible keys.*

**d)** *For each* $k \in K$*, there is an encryption rule* $e_k \in E$ *and a corresponding decryption rule* $d_k \in D$*. Each* $e_k : M \to C$ *and* $d_k : C \to M$ *are functions*

*such that* $d_k(e_k(x)) = x$ *for every plaintext element* $x \in M$*.*

It is obvious that each encryption function $e_k$ must be an injective function (i.e., one-to-one), as decryption would not be possible otherwise.

**Shift Cipher**

Let $M = C = K = \mathbb{Z}_{26}$. For $0 \leq k \leq 25$, define

$e_k(x) = (x + k) \bmod 26$

and

$d_k(y) = (y - k) \bmod 26$, $x, y \in \mathbb{Z}_{26}$.

It is defined over $\mathbb{Z}_{26}$ since there are 26 letters in the English alphabet, though it could be defined over $\mathbb{Z}_m$ for any modulus $m$. It is easy to see that the Shift Cipher forms a cryptosystem as defined above.

**Substitution Cipher**

Let $M = C = \mathbb{Z}_{26}$. $K$ consists of all possible permutations of the 26 symbols $0, 1, 2, \ldots, 25$. For each permutation $\pi \in K$, define

$e_\pi(x) = \pi(x)$,

and define

$d_\pi(y) = \pi^{-1}(y)$,

where $\pi^{-1}$ is the inverse permutation to $\pi$.

### The Hill Cipher

The encryption system devised by Hill replaces $n$ consecutive plaintext letters with $n$ ciphertext letters. We utilize the matrix representations $M$ for plaintext, $K$ for key matrix and $C$ for ciphertext (encrypted matrix), where $M$, $K$, and $C$ are given as:

$$M = (M_1, \ldots, M_m)\,,\; K = \begin{pmatrix} K_{11} & K_{12} & \cdots & K_{1n} \\ K_{21} & K_{22} & \cdots & K_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ K_{n1} & K_{n2} & \cdots & K_{nn} \end{pmatrix} \text{ and } C = (C_1, \ldots, C_m) \tag{3.1}$$

where $M_i'$s and $C_i'$s are block matrix of size $1 \times n$. The Hill cipher encryption-decryption technique is defined as follows:

$$e(M) : C_i \equiv M_i K (\mathrm{mod}\, p) \tag{3.2}$$

$$d(C) : M_i \equiv C_i K^{-1} (\mathrm{mod}\, p) \tag{3.3}$$

, where $p$ is prime and $\gcd(\det(K), p) = 1$.

### The Affine Cipher

The Affine Cipher is a type of substitution cipher that is described as

$$e_k(x) : y \equiv (ax + b) (\mathrm{mod}\, 26) \tag{3.4}$$

$$d_k(y) : x \equiv a^{-1}(y - b) (\mathrm{mod}\, 26) \tag{3.5}$$

, where $a, b, x, y \in \mathbb{Z}_{26}$ and $\gcd(a, 26) = 1$, which confirms the existence of $a^{-1}$.

### The Affine-Hill Cipher

The Affine-Hill Cipher is a polygraphic block cipher that builds on the Hill Cipher concept outlined before. Its encryption-decryption method is as follows:

$$e(M) : C_i \equiv (M_i K + B) (\mathrm{mod}\, p) \tag{3.6}$$

$$d(C) : M_i \equiv (C_i - B) K^{-1} (\mathrm{mod}\, p) \tag{3.7}$$

, where $M_i, C_i$ and $B$ are $1 \times n$ matrices, $K$ is $n \times n$ key matrix, $p$ is prime greater than the number of different characters used in plaintext.

**Stream Ciphers**

So far, in the cryptosystems we've looked at, successive plaintext items are encrypted with the same key, $K$. To put it another way, the ciphertext string $y$ is obtained as follows:

$$y = y_1 y_2 \cdots = e_K(x_1)e_K(x_2)\cdots.$$

This type of cryptosystem is frequently referred to as a *block cipher*.
A different method is to employ what are known as *stream ciphers*. The main concept is to create a keystream $z = z_1 z_2 \cdots$, and use it to encrypt a plaintext string $x = x_1 x_2 \cdots$ according to the rule

$$y = y_1 y_2 \cdots = e_{z_1}(x_1)e_{z_2}(x_2)\cdots.$$

### 3.4.2 Public Key Cryptography and Discrete Logarithms

The topic of this subsection is public-key cryptosystems based on the Discrete Logarithm issue. The Discrete Logarithm issue lies at the heart of several encryption systems. The first and most well-known of them is the ElGamal Cryptosystem.
The ElGamal cryptosystem is based on the discrete logarithm problem. In order to explain this problem, we first consider the case of a finite multiplicative group $(G, .)$. For an element $\alpha \in G$ having order $n$, define

$$\langle\alpha\rangle = \{\alpha^i : 0 \leq i \leq n-1\}.$$

It is obvious that $\langle\alpha\rangle$ is a subgroup of G and that $\langle\alpha\rangle$ is cyclic of order $n$. The subgroup $\langle\alpha\rangle$ is called the subgroup generated by $\alpha$. We define a general version of the Discrete Logarithm problem in a subgroup $\langle\alpha\rangle$ of a group $(G, .)$.

**Problem 3.1** *(Discrete Logarithm) A multiplicative group $(G, .)$, an element $\alpha \in G$ having order $n$, and an element $\beta \in \langle\alpha\rangle$. Find the unique integer $a$, $0 \leq a \leq n-1$, such that*

$$\alpha^a = \beta.$$

*We will denote this integer $a$ by $\log_\alpha \beta$; it is called the discrete logarithm of $\beta$.*

**The ElGamal Cryptosystem**

1. $p$ is prime.

2. $D$ is a private key, where $1 < D < \phi(p)$.

3. Select a primitive root of $p$, say $\alpha$.

4. Assign $E_1 = \alpha$ and $E_2 \equiv E_1^D (\mathrm{mod}\, p)$.

5. Make $(p, E_1, E_2)$ as public key and keep $D$ as secret key.

Suppose entity Vedat and Mehmet want to exchange keys. Vedat produces signature $k$ using the public key $(p, E_1, E_2)$ mentioned above by computing $k = E_1^e (\mathrm{mod}\, p)$, where $e$ is a random integer with $1 < e < \phi(p)$, and secret key $\lambda = E_2^e (\mathrm{mod}\, p)$. Mehmet's public key makes it possible for Vedat to encrypt messages using their secret key and send them $(k, C)$.
Mehmet recovers secret key by utilizing their secret key $D$ as follows after getting $(k, C)$ from Vedat:

$\lambda = k^D = (E_1^e)^D = (E_1^D)^e \equiv (E_2)^e (\mathrm{mod}\, p)$.

As a result, Mehmet successfully locates the secret key and uses it to decrypt the ciphertext $C$ and obtain the original plaintext $P$.

**Big $O$ Notation**

When we do a computation, we want it to be as quick as feasible, or at least as fast as possible. To discuss (roughly) what it implies, we'll need to use big $O$ notation.

**Definition 3.2** *Let $f(x)$ and $g(x)$ be two functions, we say that $f(x) = O(g(x))$ if there is some constant $C > 0$, which does not depend on $x$, so that $|f(x)| \leq C\,|g(x)|$ for all $x$.*

**Remark 3.1** *There is a slight subtlety here: what does for all $x$ mean? It could mean for all $x \in \mathbb{R}$, but we will use it slightly more weakly to mean for all sufficiently large $x$, i.e., there is some $A$ so that $|f(x)| \leq C\,|g(x)|$ for all $x \geq A$.*

**Example 3.1** *If* $f(x) = x^4 + 7x^3 - 5x^2 + 3x + 12$*, then* $f(x) = O(x^4)$*. More generally, if* $f(x)$ *is a polynomial of the form* $ax^n +$ *lower order terms, then* $f(x) = O(x^n)$*. We also have that* $f(x) = O(x^{n+1})$ *or* $O(x^{n+2})$*, Typically, we'll be looking for a big* $O$ *that's near to the best we can do.*

**Example 3.2** *For* $x \to 0$*,* $\sin 2x = O(x)$*. Because for* $\forall x \in \mathbb{R}$*,* $|\sin 2x| \leq 2\,|x|$*.*

When using big $O$ notation for $g(x)$, there are a number of functions that we like to employ. $O(x^2)$, $O(x^3)$, $O(log(x))$, $O(2^x)$ are commonly used. Another notation we will use is $O(x^{2+\varepsilon})$. $\varepsilon$ is typically used in mathematics to denote a very small positive number. So $f(x) = O(x^{2+\varepsilon})$ means that for any $r > 2$, $f(x) = O(x^r)$, but it might not be the case that $f(x) = O(x^2)$. This often indicates that $f(x)$ is about $x^2$ times a function that contains logarithms.

**Example 3.3** *For any* $b, c > 1$*,* $\log_b x = O(\log_c x)$*, and vice versa. To see this, note that* $\log_b x = \frac{\log_c x}{\log_c b}$*, so* $\log_b x$ *and* $\log_c x$ *differ only by a multiplicative constant, which is exactly the sort of thing that big* $O$ *notation measures.*

**Example 3.4** *For any* $\varepsilon > 0$*,* $\log x = O(x^\varepsilon)$*. Thus, while* $\log x$ *as* $x \to \infty$*, it gets there very slowly.*

### Running Times of Algorithms

When discussing the running time of algorithms, we will usually utilize big $O$ notation: how long does it take to run a program to do something?

Suppose that instead of having a program that takes in a number and outputs another number, we have a program that takes in some string of characters and outputs another string of characters. How do we measure the size of the input now? The natural answer is that we measure the length of the input string.

So, if we measure the running time of an algorithm involving an input string in terms of the length of the string, perhaps we should do that for an algorithm involving an input number: we measure it in terms of the number of digits in the number.

In this thesis, we will give the time complexity for matrices without going into too much detail.

Computers are required to do many Matrix Multiplications at a time, and hence it is desirable to find algorithms to reduce the number of steps required to multiply two matrices together. Until 1968, we had only the Trivial Algorithm to multiply matrices together. This is as follows:

**Algorithm 3.1** *If we have two $n \times n$ matrices, $n \in \mathbb{N}$, $A$ and $B$, with entries in a field $\mathbb{K}$, such that*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \text{ and } B = \begin{pmatrix} b_{11} & b_{12} & \cdots \\ b_{21} & b_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

*then*

$$[AB]_{pq} = \sum_{i=1}^{n} a_{pi} b_{iq}$$

*where multiplication is defined as in the field $\mathbb{K}$.*

We see that this algorithm requires $2n^3 - n^2$ operations in $\mathbb{K}$ to multiply two $n \times n$ matrices, of which $n^3$ are multiplications and $n^3 - n^2$ are additions.

**Definition 3.3** *The exponent of matrix multiplication over a field $\mathbb{K}$ is defined as*

$$\omega(\mathbb{K}) = \inf\{\varepsilon \in \mathbb{R} : M_{\mathbb{K}}(n) = O(n^{\varepsilon})\}.$$

We see from the trivial algorithm that $\omega(\mathbb{K})$ has an upper limit of 3. Since the output must include $n^2$ entries, the total number of matrix multiplication operations must be less than this, so hence $\omega(\mathbb{K}) \in [2, 3]$. In 1968, Strassen demonstrated via a recursive method that $\omega(\mathbb{K}) \leq \log_2 7$, see [49].

## CHAPTER 4

# GENERALIZED WOODALL NUMBERS: AN INVESTIGATION OF PROPERTIES OF WOODALL AND CULLEN NUMBERS VIA THEIR THIRD ORDER LINEAR RECURRENCE RELATIONS

In this chapter, we will give definitions, theorems and properties related to Woodall numbers. Our work which is given in this chapter is original. This chapter was published as the journal, see [50].

The Woodall numbers $\{R_n\}$, sometimes called Riesel numbers, and also called Cullen numbers of the second kind, are numbers of the form

$R_n = n \times 2^n - 1.$

The first few Woodall numbers are:

$1, 7, 23, 63, 159, 383, 895, 2047, 4607, 10239, 22527, 49151, 106495, 229375, 491519, 1048575, \ldots$

(sequence A003261 in the OEIS [51]). Woodall numbers were first studied by Allan J. C. Cunningham and H. J. Woodall in [52] in 1917, inspired by James Cullen's earlier study of the similarly-defined Cullen numbers.

The Cullen numbers $\{C_n\}$ are numbers of the form

$C_n = n \times 2^n + 1.$

The first few Cullen numbers are:

$1, 3, 9, 25, 65, 161, 385, 897, 2049, 4609, 10241, 22529, 49153, 106497, 229377, 491521, ...$

(sequence A002064 in the OEIS).

Woodall and Cullen sequences have been studied by many authors and more detail can be found in the extensive literature dedicated to these sequences, see for example, [52-62] and references therein.

Note that $\{R_n\}$ and $\{C_n\}$ hold the following relations:

$$\begin{aligned} R_n &= 4R_{n-1} - 4R_{n-2} - 1, \\ C_n &= 4C_{n-1} - 4C_{n-2} + 1. \end{aligned}$$

Note also that the sequences $\{R_n\}$ and $\{C_n\}$ satisfy the following third order linear recurrences:

$$R_n = 5R_{n-1} - 8R_{n-2} + 4R_{n-3}, \qquad R_0 = -1, R_1 = 1, R_2 = 7, \tag{4.1}$$

$$C_n = 5C_{n-1} - 8C_{n-2} + 4C_{n-3}, \qquad C_0 = 1, C_1 = 3, C_2 = 9. \tag{4.2}$$

The purpose of this study is to generalize and investigate these interesting sequence of numbers (i.e., Woodall, Cullen numbers) via their third order linear recurrence relations (4.1) and (4.2). First, we recall some properties of generalized Tribonacci numbers.
The generalized $(r, s, t)$ sequence (or generalized Tribonacci sequence or generalized 3-step Fibonacci sequence)

$$\{W_n(W_0, W_1, W_2; r, s, t)\}_{n\geq 0}$$

(or shortly $\{W_n\}_{n\geq 0}$) is defined as follows:

$$W_n = rW_{n-1} + sW_{n-2} + tW_{n-3}, \qquad W_0 = a, W_1 = b, W_2 = c, \quad n \geq 3 \tag{4.3}$$

where $W_0, W_1, W_2$ are arbitrary complex (or real) numbers and $r, s, t$ are real numbers. This sequence has been studied by many authors, see for example [22,63-75].
The sequence $\{W_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$W_{-n} = -\frac{s}{t}W_{-(n-1)} - \frac{r}{t}W_{-(n-2)} + \frac{1}{t}W_{-(n-3)}$$

for $n = 1, 2, 3, ...$ when $t \neq 0$. Therefore, recurrence (4.3) holds for all integer $n$.
As $\{W_n\}$ is a third-order recurrence sequence (difference equation), it's characteristic equation is

$$x^3 - rx^2 - sx - t = 0 \tag{4.4}$$

whose roots are

$$\begin{aligned} \alpha &= \alpha(r, s, t) = \frac{r}{3} + A + B, \\ \beta &= \beta(r, s, t) = \frac{r}{3} + \omega A + \omega^2 B, \\ \gamma &= \gamma(r, s, t) = \frac{r}{3} + \omega^2 A + \omega B, \end{aligned}$$

where

$$A = \left(\frac{r^3}{27}+\frac{rs}{6}+\frac{t}{2}+\sqrt{\Delta}\right)^{1/3},\ B=\left(\frac{r^3}{27}+\frac{rs}{6}+\frac{t}{2}-\sqrt{\Delta}\right)^{1/3},$$

$$\Delta = \Delta(r,s,t)=\frac{r^3t}{27}-\frac{r^2s^2}{108}+\frac{rst}{6}-\frac{s^3}{27}+\frac{t^2}{4},\ \ \omega=\frac{-1+i\sqrt{3}}{2}=\exp(2\pi i/3).$$

Note that we have the following identities

$$\begin{aligned}\alpha+\beta+\gamma &= r,\\ \alpha\beta+\alpha\gamma+\beta\gamma &= -s,\\ \alpha\beta\gamma &= t.\end{aligned}$$

In the case of two distinct roots, i.e., $\alpha=\beta\neq\gamma$, Binet's formula can be given as follows:

**Theorem 4.1** *(Two Distinct Roots Case: $\alpha=\beta\neq\gamma$) Binet's formula of generalized Fibonacci numbers is*

$$W_n=(A_1+A_2n)\times\alpha^n+A_3\gamma^n$$

where

$$\begin{aligned}A_1 &= \frac{-W_2+2\alpha W_1-\gamma(2\alpha-\gamma)W_0}{(\alpha-\gamma)^2},\\ A_2 &= \frac{W_2-(\alpha+\gamma)W_1+\alpha\gamma W_0}{\alpha(\alpha-\gamma)},\\ A_3 &= \frac{W_2-2\alpha W_1+\alpha^2W_0}{(\alpha-\gamma)^2}.\end{aligned}$$

Next, we give the ordinary generating function $\sum_{n=0}^{\infty}W_nx^n$ of the sequence $W_n$.

**Lemma 4.2** *Suppose that $f_{W_n}(x)=\sum_{n=0}^{\infty}W_nx^n$ is the ordinary generating function of the generalized $(r,s,t)$ sequence (the generalized Tribonacci sequence) $\{W_n\}_{n\geq0}$. Then, $\sum_{n=0}^{\infty}W_nx^n$ is given by*

$$\sum_{n=0}^{\infty}W_nx^n=\frac{W_0+(W_1-rW_0)x+(W_2-rW_1-sW_0)x^2}{1-rx-sx^2-tx^3}. \tag{4.5}$$

Matrix formulation of $W_n$ can be given as

$$\begin{pmatrix}W_{n+2}\\W_{n+1}\\W_n\end{pmatrix}=\begin{pmatrix}r&s&t\\1&0&0\\0&1&0\end{pmatrix}^n\begin{pmatrix}W_2\\W_1\\W_0\end{pmatrix}. \tag{4.6}$$

For matrix formulation (4.6), see [76]. In fact, Kalman gave the formula in the following form

$$\begin{pmatrix} W_n \\ W_{n+1} \\ W_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ r & s & t \end{pmatrix}^n \begin{pmatrix} W_0 \\ W_1 \\ W_2 \end{pmatrix}.$$

Now, we present Simson's formula of generalized Tribonacci numbers.

**Theorem 4.3 (Simson's Formula of Generalized Tribonacci Numbers)** *For all integers $n$, we have*

$$\begin{vmatrix} W_{n+2} & W_{n+1} & W_n \\ W_{n+1} & W_n & W_{n-1} \\ W_n & W_{n-1} & W_{n-2} \end{vmatrix} = t^n \begin{vmatrix} W_2 & W_1 & W_0 \\ W_1 & W_0 & W_{-1} \\ W_0 & W_{-1} & W_{-2} \end{vmatrix}. \tag{4.7}$$

Proof. For a proof, see Soykan [13]. □

Next, we consider two special cases of the generalized $(r, s, t)$ sequence $\{W_n\}$ which we call them $(r, s, t)$ and Lucas $(r, s, t)$ sequences. $(r, s, t)$ sequence $\{G_n\}_{n\geq 0}$ and Lucas $(r, s, t)$ sequence $\{H_n\}_{n\geq 0}$ are defined, respectively, by the third-order recurrence relations

$$G_{n+3} = rG_{n+2} + sG_{n+1} + tG_n, \qquad G_0 = 0, G_1 = 1, G_2 = r, \tag{4.8}$$

$$H_{n+3} = rH_{n+2} + sH_{n+1} + tH_n, \qquad H_0 = 3, H_1 = r, H_2 = 2s + r^2. \tag{4.9}$$

The sequences $\{G_n\}_{n\geq 0}$ and $\{H_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$G_{-n} = -\frac{s}{t}G_{-(n-1)} - \frac{r}{t}G_{-(n-2)} + \frac{1}{t}G_{-(n-3)},$$

$$H_{-n} = -\frac{s}{t}H_{-(n-1)} - \frac{r}{t}H_{-(n-2)} + \frac{1}{t}H_{-(n-3)}$$

for $n = 1, 2, 3, ...$ respectively. Therefore, recurrences (4.8)-(4.9) hold for all integers $n$.

In the case of two distinct roots, i.e., $\alpha = \beta \neq \gamma$, for all integers $n$, Binet's formula of $(r, s, t)$ and Lucas $(r, s, t)$ numbers (using initial conditions in (4.8)-(4.9)) can be expressed as follows:

**Theorem 4.4** *(Two Distinct Roots Case: $\alpha = \beta \neq \gamma$) For all integers $n$, Binet's formula of $(r, s, t)$ and Lucas $(r, s, t)$ numbers are*

$$G_n = \left(\frac{-\gamma}{(\alpha-\gamma)^2} + \frac{1}{(\alpha-\gamma)}n\right) \times \alpha^n + \frac{\gamma}{(\alpha-\gamma)^2}\gamma^n,$$

$$H_n = 2\alpha^n + \gamma^n,$$

*respectively.*

Lemma 4.2 gives the following results as particular examples (generating functions of $(r,s,t)$ and Lucas $(r,s,t)$ numbers).

**Corollary 4.1** *Generating functions of* $(r,s,t)$ *and Lucas* $(r,s,t)$ *numbers are*

$$\sum_{n=0}^{\infty} G_n x^n = \frac{x}{1-rx-sx^2-tx^3},$$
$$\sum_{n=0}^{\infty} H_n x^n = \frac{3-2rx-sx^2}{1-rx-sx^2-tx^3},$$

*respectively.*

The following theorem shows that the generalized Tribonacci sequence $W_n$ at negative indices can be expressed by the sequence itself at positive indices.

**Theorem 4.5** *For* $n \in \mathbb{Z}$, *we have*

$$W_{-n} = t^{-n}(W_{2n} - H_n W_n + \frac{1}{2}(H_n^2 - H_{2n})W_0).$$

Proof. For the proof, see Soykan [77, Theorem 2.]. □

Now, we present a basic relation between $\{H_n\}$ and $\{W_n\}$ which can be used to write $H_n$ in terms of $W_n$.

**Lemma 4.6** *The following equality is true:*

$(W_2^3 + (t+rs)W_1^3 + t^2W_0^3 + (r^2-s)W_1^2W_2 - 2rW_1W_2^2 - sW_0W_2^2 + rtW_0^2W_2 + (s^2+rt)W_0W_1^2 + 2stW_0^2W_1 + (rs-3t)W_0W_1W_2)H_n = (3W_2^2 + (r^2-s)W_1^2 + rtW_0^2 - 4rW_1W_2 - 2sW_0W_2 + (rs-3t)W_0W_1)W_{n+2} + (-2rW_2^2 + 3tW_1^2 - 2sW_1W_2 - 3tW_0W_2 + 3rsW_1^2 + 2stW_0^2 + 2r^2W_1W_2 + 2s^2W_0W_1 + rsW_0W_2 + 2rtW_0W_1)W_{n+1} + (-sW_2^2 + (s^2+rt)W_1^2 + 3t^2W_0^2 + (rs-3t)W_1W_2 + 2rtW_0W_2 + 4stW_0W_1)W_n$.

Proof. It is given in Soykan [22]. □

Using Theorem 4.5, we have the following corollary, see Soykan [77, Corollary 6].

**Corollary 4.2** *For* $n \in \mathbb{Z}$, *we have*

**(a)** $G_{-n} = \frac{1}{t^{n+1}}((2rt-s^2)G_n^2 + tG_{2n} + sG_{n+2}G_n - (3t+rs)G_{n+1}G_n)$.

**(b)** $H_{-n} = \frac{1}{2t^n}(H_n^2 - H_{2n})$.

Note that $G_{-n}$ and $H_{-n}$ can be given as follows by using $G_0 = 0$ and $H_0 = 3$ in Theorem 4.5,

$$\begin{aligned} G_{-n} &= t^{-n}(G_{2n} - H_n G_n + \frac{1}{2}(H_n^2 - H_{2n})G_0) = t^{-n}(G_{2n} - H_n G_n), \\ H_{-n} &= t^{-n}(H_{2n} - H_n H_n + \frac{1}{2}(H_n^2 - H_{2n})H_0) = \frac{1}{2t^n}(H_n^2 - H_{2n}), \end{aligned}$$

respectively.

## 4.1 GENERALIZED WOODALL SEQUENCE

In this section, we consider the case $r = 5, s = -8, t = 4$. A generalized Woodall sequence $\{W_n\}_{n\geq 0} = \{W_n(W_0, W_1, W_2)\}_{n\geq 0}$ is defined by the third-order recurrence relations

$$W_n = 5W_{n-1} - 8W_{n-2} + 4W_{n-3} \tag{4.10}$$

with the initial values $W_0 = c_0, W_1 = c_1, W_2 = c_2$ not all being zero.
The sequence $\{W_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$W_{-n} = 2W_{-(n-1)} - \frac{5}{4}W_{-(n-2)} + \frac{1}{4}W_{-(n-3)}$$

for $n = 1, 2, 3, ....$ Therefore, recurrence (4.10) holds for all integer $n$.
Theorem 4.1 can be used to obtain Binet formula of generalized Woodall numbers. Binet formula of generalized Woodall numbers can be given as
(two distinct roots case: $\alpha = \beta \neq \gamma$)

$$W_n = (A_1 + A_2 n) \times \alpha^n + A_3 \gamma^n$$

where

$$\begin{aligned} A_1 &= \frac{-W_2 + 2\alpha W_1 - \gamma(2\alpha - \gamma)W_0}{(\alpha - \gamma)^2}, \\ A_2 &= \frac{W_2 - (\alpha + \gamma)W_1 + \alpha\gamma W_0}{\alpha(\alpha - \gamma)}, \\ A_3 &= \frac{W_2 - 2\alpha W_1 + \alpha^2 W_0}{(\alpha - \gamma)^2}. \end{aligned}$$

Here, $\alpha, \beta$ and $\gamma$ are the roots of the cubic equation

$$x^3 - 5x^2 + 8x - 4 = (x - 2)^2(x - 1) = 0.$$

Moreover

$$\begin{aligned}\alpha &= \beta = 2,\\ \gamma &= 1.\end{aligned}$$

So,

$$W_n = (A_1 + A_2 n) \times 2^n + A_3$$

where

$$\begin{aligned}A_1 &= -W_2 + 4W_1 - 3W_0,\\ A_2 &= \frac{W_2 - 3W_1 + 2W_0}{2},\\ A_3 &= W_2 - 4W_1 + 4W_0,\end{aligned}$$

i.e.,

$$W_n = ((-W_2 + 4W_1 - 3W_0) + \frac{W_2 - 3W_1 + 2W_0}{2} n) \times 2^n + (W_2 - 4W_1 + 4W_0). \qquad (4.11)$$

The first few generalized Woodall numbers with positive subscript and negative subscript are given in the following Table 4.1.

Table 4.1 A few generalized Woodall numbers

| $n$ | $W_n$ | $W_{-n}$ |
|---|---|---|
| 0 | $W_0$ | $W_0$ |
| 1 | $W_1$ | $\frac{1}{4}(8W_0 - 5W_1 + W_2)$ |
| 2 | $W_2$ | $(11W_0 - 9W_1 + 2W_2)$ |
| 3 | $4W_0 - 8W_1 + 5W_2$ | $\frac{1}{16}(52W_0 - 47W_1 + 11W_2)$ |
| 4 | $20W_0 - 36W_1 + 17W_2$ | $(57W_0 - 54W_1 + 13W_2)$ |
| 5 | $68W_0 - 116W_1 + 49W_2$ | $\frac{1}{64}(240W_0 - 233W_1 + 57W_2)$ |
| 6 | $196W_0 - 324W_1 + 129W_2$ | $(247W_0 - 243W_1 + 60W_2)$ |
| 7 | $516W_0 - 836W_1 + 321W_2$ | $\frac{1}{256}(1004W_0 - 995W_1 + 247W_2)$ |
| 8 | $1284W_0 - 2052W_1 + 769W_2$ | $\frac{1}{256}(1013W_0 - 1008W_1 + 251W_2)$ |
| 9 | $3076W_0 - 4868W_1 + 1793W_2$ | $\frac{1}{1024}(4072W_0 - 4061W_1 + 1013W_2)$ |
| 10 | $7172W_0 - 11268W_1 + 4097W_2$ | $\frac{1}{1024}(4083W_0 - 4077W_1 + 1018W_2)$ |
| 11 | $16388W_0 - 25604W_1 + 9217W_2$ | $\frac{1}{4096}(16356W_0 - 16343W_1 + 4083W_2)$ |
| 12 | $36868W_0 - 57348W_1 + 20481W_2$ | $\frac{1}{4096}(16369W_0 - 16362W_1 + 4089W_2)$ |
| 13 | $81924W_0 - 126980W_1 + 45057W_2$ | $\frac{1}{16\,384}(65504W_0 - 65489W_1 + 16369W_2)$ |

Now, we define four special cases of the sequence $\{W_n\}$. Modified Woodall sequence $\{G_n\}_{n\geq 0}$ , modified Cullen sequence $\{H_n\}_{n\geq 0}$, Woodall sequence $\{R_n\}$ and Cullen sequence $\{C_n\}$ are defined, respectively, by the third-order recurrence relations

$$G_n = 5G_{n-1} - 8G_{n-2} + 4G_{n-3}, \quad G_0 = 0, G_1 = 1, G_2 = 5, \tag{4.12}$$

$$H_n = 5H_{n-1} - 8H_{n-2} + 4H_{n-3}, \quad H_0 = 3, H_1 = 5, H_2 = 9, \tag{4.13}$$

$$R_n = 5R_{n-1} - 8R_{n-2} + 4R_{n-3}, \quad R_0 = -1, R_1 = 1, R_2 = 7, \tag{4.14}$$

$$C_n = 5C_{n-1} - 8C_{n-2} + 4C_{n-3}, \quad C_0 = 1, C_1 = 3, C_2 = 9. \tag{4.15}$$

The sequences $\{G_n\}_{n\geq 0}$, $\{H_n\}_{n\geq 0}$, $\{R_n\}_{n\geq 0}$ and $\{C_n\}_{n\geq 0}$ can be extended to negative subscripts by defining

$$\begin{aligned}
G_{-n} &= 2G_{-(n-1)} - \frac{5}{4}G_{-(n-2)} + \frac{1}{4}G_{-(n-3)}, \\
H_{-n} &= 2H_{-(n-1)} - \frac{5}{4}H_{-(n-2)} + \frac{1}{4}H_{-(n-3)}, \\
R_{-n} &= 2R_{-(n-1)} - \frac{5}{4}R_{-(n-2)} + \frac{1}{4}R_{-(n-3)}, \\
C_{-n} &= 2C_{-(n-1)} - \frac{5}{4}C_{-(n-2)} + \frac{1}{4}C_{-(n-3)},
\end{aligned}$$

for $n = 1, 2, 3, ...$ respectively. Therefore, recurrences (4.12)-(4.15) hold for all integer $n$. Next, we present the first few values of the modified Woodall, modified Cullen, Woodall and Cullen numbers with positive and negative subscripts:

Table 4.2 The first few values of the special third-order numbers with positive and negative subscripts.

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $G_n$ | 0 | 1 | 5 | 17 | 49 | 129 | 321 | 769 | 1793 | 4097 | 9217 | 20481 | 45057 |
| $G_{-n}$ | | 0 | $\frac{1}{4}$ | $\frac{1}{2}$ | $\frac{11}{16}$ | $\frac{13}{16}$ | $\frac{57}{64}$ | $\frac{15}{16}$ | $\frac{247}{256}$ | $\frac{251}{256}$ | $\frac{1013}{1024}$ | $\frac{509}{512}$ | $\frac{4083}{4096}$ |
| $H_n$ | 3 | 5 | 9 | 17 | 33 | 65 | 129 | 257 | 513 | 1025 | 2049 | 4097 | 8193 |
| $H_{-n}$ | | 2 | $\frac{3}{2}$ | $\frac{5}{4}$ | $\frac{9}{8}$ | $\frac{17}{16}$ | $\frac{33}{32}$ | $\frac{65}{64}$ | $\frac{129}{128}$ | $\frac{257}{256}$ | $\frac{513}{512}$ | $\frac{1025}{1024}$ | $\frac{2049}{2048}$ |
| $R_n$ | $-1$ | 1 | 7 | 23 | 63 | 159 | 383 | 895 | 2047 | 4607 | 10239 | 22527 | 49151 |
| $R_{-n}$ | | $-\frac{3}{2}$ | $-\frac{3}{2}$ | $-\frac{11}{8}$ | $-\frac{5}{4}$ | $-\frac{37}{32}$ | $-\frac{35}{32}$ | $-\frac{135}{128}$ | $-\frac{33}{32}$ | $-\frac{521}{512}$ | $-\frac{517}{512}$ | $-\frac{2059}{2048}$ | $-\frac{1027}{1024}$ |
| $C_n$ | 1 | 3 | 9 | 25 | 65 | 161 | 385 | 897 | 2049 | 4609 | 10241 | 22529 | 49153 |
| $C_{-n}$ | | $\frac{1}{2}$ | $\frac{1}{2}$ | $\frac{5}{8}$ | $\frac{3}{4}$ | $\frac{27}{32}$ | $\frac{29}{32}$ | $\frac{121}{128}$ | $\frac{31}{32}$ | $\frac{503}{512}$ | $\frac{507}{512}$ | $\frac{2037}{2048}$ | $\frac{1021}{1024}$ |

$G_n, H_n$, $R_n$ and $C_n$ are the sequences A000337, A000051 (and A048578), A003261 and A002064 in [51], respectively. Note that $\{H_n\}$ satisfies the following second order linear

recurrence:

$H_n = 3H_{n-1} - 2H_{n-2}, \quad H_0 = 3, H_1 = 5$

and satisfies the following first order non-linear recurrence:

$H_n = 2H_{n-1} - 1, \quad H_0 = 3.$

For all integers $n$, modified Woodall, modified Cullen, Woodall and Cullen numbers (using initial conditions in (4.11)) can be expressed using Binet's formulas as

$$\begin{aligned} G_n &= (n-1)\,2^n + 1 \\ H_n &= 2^{n+1} + 1 \\ R_n &= n \times 2^n - 1 \\ C_n &= n \times 2^n + 1 \end{aligned}$$

respectively.

Next, we give the ordinary generating function $\sum_{n=0}^{\infty} W_n x^n$ of the sequence $W_n$.

**Lemma 4.7** *Suppose that $f_{W_n}(x) = \sum_{n=0}^{\infty} W_n x^n$ is the ordinary generating function of the generalized Woodall sequence $\{W_n\}_{n\geq 0}$. Then, $\sum_{n=0}^{\infty} W_n x^n$ is given by*

$$\sum_{n=0}^{\infty} W_n x^n = \frac{W_0 + (W_1 - 5W_0)x + (W_2 - 5W_1 + 8W_0)x^2}{1 - 5x + 8x^2 - 4x^3}.$$

Proof. Take $r = 5, s = -8, t = 4$ in Lemma 4.2. □

The previous lemma gives the following results as particular examples.

**Corollary 4.3** *Generated functions of modified Woodall, modified Cullen, Woodall and Cullen numbers are*

$$\begin{aligned} \sum_{n=0}^{\infty} G_n x^n &= \frac{x}{1 - 5x + 8x^2 - 4x^3}, \\ \sum_{n=0}^{\infty} H_n x^n &= \frac{3 - 10x + 8x^2}{1 - 5x + 8x^2 - 4x^3}, \\ \sum_{n=0}^{\infty} R_n x^n &= \frac{-1 + 6x - 6x^2}{1 - 5x + 8x^2 - 4x^3}, \\ \sum_{n=0}^{\infty} C_n x^n &= \frac{1 - 2x + 2x^2}{1 - 5x + 8x^2 - 4x^3}, \end{aligned}$$

*respectively.*

## 4.2 SIMSON FORMULAS

There is a well-known Simson Identity (formula) for Fibonacci sequence $\{F_n\}$, namely,

$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$

which was derived first by R. Simson in 1753 and it is now called as Cassini Identity (formula) as well. This can be written in the form

$$\begin{vmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{vmatrix} = (-1)^n.$$

The following theorem gives generalization of this result to the generalized Woodall sequence $\{W_n\}_{n\geq 0}$.

**Theorem 4.8 (Simson Formula of Generalized Woodall Numbers)** *For all integers $n$, we have*

$$\begin{vmatrix} W_{n+2} & W_{n+1} & W_n \\ W_{n+1} & W_n & W_{n-1} \\ W_n & W_{n-1} & W_{n-2} \end{vmatrix} = -2^{2n-4}(W_2 - 4W_1 + 4W_0)(W_2 - 3W_1 + 2W_0)^2.$$

Proof. Take $r = 5, s = -8, t = 4$ in Theorem 4.3. □

The previous theorem gives the following results as particular examples.

**Corollary 4.4** *For all integers $n$, Simson formula of modified Woodall, modified Cullen, Woodall and Cullen numbers are given as*

$$\begin{vmatrix} G_{n+2} & G_{n+1} & G_n \\ G_{n+1} & G_n & G_{n-1} \\ G_n & G_{n-1} & G_{n-2} \end{vmatrix} = -2^{2n-2},$$

$$\begin{vmatrix} H_{n+2} & H_{n+1} & H_n \\ H_{n+1} & H_n & H_{n-1} \\ H_n & H_{n-1} & H_{n-2} \end{vmatrix} = 0,$$

$$\begin{vmatrix} R_{n+2} & R_{n+1} & R_n \\ R_{n+1} & R_n & R_{n-1} \\ R_n & R_{n-1} & R_{n-2} \end{vmatrix} = 2^{2n-2},$$

$$\begin{vmatrix} C_{n+2} & C_{n+1} & C_n \\ C_{n+1} & C_n & C_{n-1} \\ C_n & C_{n-1} & C_{n-2} \end{vmatrix} = -2^{2n-2},$$

*respectively.*

## 4.3 SOME IDENTITIES

In this section, we obtain some identities of generalized Woodall, modified Woodall, modified Cullen, Woodall and Cullen numbers. First, we can give a few basic relations between $\{W_n\}$ and $\{G_n\}$.

**Lemma 4.9** *The following equalities are true:*

**(a)** $16W_n = (52W_0 - 47W_1 + 11W_2)G_{n+4} + (199W_1 - 216W_0 - 47W_2)G_{n+3} + 4(57W_0 - 54W_1 + 13W_2)G_{n+2}$.

**(b)** $4W_n = (11W_0 - 9W_1 + 2W_2)G_{n+3} + (40W_1 - 47W_0 - 9W_2)G_{n+2} + (52W_0 - 47W_1 + 11W_2)G_{n+1}$.

**(c)** $4W_n = (8W_0 - 5W_1 + W_2)G_{n+2} + (25W_1 - 36W_0 - 5W_2)G_{n+1} + 4(11W_0 - 9W_1 + 2W_2)G_n$.

**(d)** $W_n = W_0G_{n+1} + (-5W_0 + W_1)G_n + (8W_0 - 5W_1 + W_2)G_{n-1}$.

**(e)** $W_n = W_1G_n + (-5W_1 + W_2)G_{n-1} + 4W_0G_{n-2}$.

**(f)** $4(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2G_n = (8W_1^2 - 5W_1W_2 - 4W_0W_1 + W_2^2)W_{n+4} + (-36W_1^2 - 5W_2^2 + 20W_0W_1 - 4W_0W_2 + 25W_1W_2)W_{n+3} + 4(4W_0^2 + 16W_1^2 + 2W_2^2 - 16W_0W_1 + 5W_0W_2 - 11W_1W_2)W_{n+2}$.

**(g)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2G_n = (W_1^2 - W_0W_2)W_{n+3} + (4W_0^2 - 8W_0W_1 + 5W_0W_2 - W_1W_2)W_{n+2} + (8W_1^2 + W_2^2 - 4W_0W_1 - 5W_1W_2)W_{n+1}$.

**(h)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2G_n = (4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{n+2} + (W_2^2 - 4W_0W_1 + 8W_0W_2 - 5W_1W_2)W_{n+1} + 4(W_1^2 - W_0W_2)W_n$.

**(i)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2G_n = (20W_0^2 + 25W_1^2 + W_2^2 - 44W_0W_1 + 8W_0W_2 - 10W_1W_2)W_{n+1} + 4(-8W_0^2 + 16W_0W_1 - W_2W_0 - 9W_1^2 + 2W_2W_1)W_n + 4(4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{n-1}$.

**(j)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 G_n = (68W_0^2 + 89W_1^2 + 5W_2^2 - 156W_0W_1 + 36W_0W_2 - 42W_1W_2)W_n + 4(-36W_0^2 + 80W_0W_1 - 16W_0W_2 - 45W_1^2 + 19W_1W_2 - 2W_2^2)W_{n-1} + 4(20W_0^2 + 25W_1^2 + W_2^2 - 44W_0W_1 + 8W_0W_2 - 10W_1W_2)W_{n-2}$.

Proof. Note that all the identities hold for all integers $n$. We prove (a). To show (a), writing

$$W_n = a \times G_{n+4} + b \times G_{n+3} + c \times G_{n+2}$$

and solving the system of equations

$$\begin{aligned} W_0 &= a \times G_4 + b \times G_3 + c \times G_2 \\ W_1 &= a \times G_5 + b \times G_4 + c \times G_3 \\ W_2 &= a \times G_6 + b \times G_5 + c \times G_4 \end{aligned}$$

we find that $a = \frac{1}{16}(52W_0 - 47W_1 + 11W_2), b = -\frac{1}{16}(216W_0 - 199W_1 + 47W_2), c = \frac{1}{4}(57W_0 - 54W_1 + 13W_2)$. The other equalities can be proved similarly. □

Note that all the identities in the above Lemma can be proved by induction as well.

Next, we present a few basic relations between $\{W_n\}$ and $\{H_n\}$.

**Lemma 4.10** *The following equalities are true:*

**(a)** $2\,(2W_0 - 3W_1 + W_2)\,(4W_0 - 4W_1 + W_2)\,H_n = (8W_0 - 10W_1 + 3W_2)W_{n+4} + (36W_1 - 28W_0 - 11W_2)W_{n+3} + 2(12W_0 - 16W_1 + 5W_2)W_{n+2}$.

**(b)** $(2W_0 - 3W_1 + W_2)(4W_0 - 4W_1 + W_2)H_n = (6W_0 - 7W_1 + 2W_2)W_{n+3} + (24W_1 - 20W_0 - 7W_2)W_{n+2} + 2(8W_0 - 10W_1 + 3W_2)W_{n+1}$.

**(c)** $(2W_0 - 3W_1 + W_2)(4W_0 - 4W_1 + W_2)H_n = (10W_0 - 11W_1 + 3W_2)W_{n+2} + 2(18W_1 - 16W_0 - 5W_2)W_{n+1} + 4(6W_0 - 7W_1 + 2W_2)W_n$.

**(d)** $(2W_0 - 3W_1 + W_2)(4W_0 - 4W_1 + W_2)H_n = (18W_0 - 19W_1 + 5W_2)W_{n+1} + 4(15W_1 - 14W_0 - 4W_2)W_n + 4(10W_0 - 11W_1 + 3W_2)W_{n-1}$.

**(e)** $(2W_0 - 3W_1 + W_2)(4W_0 - 4W_1 + W_2)H_n = (34W_0 - 35W_1 + 9W_2)W_n + 4(27W_1 - 26W_0 - 7W_2)W_{n-1} + 4(18W_0 - 19W_1 + 5W_2)W_{n-2}$.

Now, we give a few basic relations between $\{W_n\}$ and $\{R_n\}$.

**Lemma 4.11** *The following equalities are true:*

**(a)** $8W_n = (42W_1 - 39W_0 - 11W_2)R_{n+4} + (151W_0 - 161W_1 + 42W_2)R_{n+3} + (151W_1 - 144W_0 - 39W_2)R_{n+2}$.

**(b)** $8W_n = (49W_1 - 44W_0 - 13W_2)R_{n+3} + (168W_0 - 185W_1 + 49W_2)R_{n+2} + 4(42W_1 - 39W_0 - 11W_2)R_{n+1}$.

**(c)** $2W_n = (15W_1 - 13W_0 - 4W_2)R_{n+2} + (49W_0 - 56W_1 + 15W_2)R_{n+1} + (49W_1 - 44W_0 - 13W_2)R_n$.

**(d)** $2W_n = (19W_1 - 16W_0 - 5W_2)R_{n+1} + (60W_0 - 71W_1 + 19W_2)R_n + 4(15W_1 - 13W_0 - 4W_2)R_{n-1}$.

**(e)** $W_n = (12W_1 - 10W_0 - 3W_2)R_n + 2(19W_0 - 23W_1 + 6W_2)R_{n-1} + 2(19W_1 - 16W_0 - 5W_2)R_{n-2}$.

**(f)** $2(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2R_n = (-12W_0^2 + 36W_0W_1 - 13W_0W_2 - 26W_1^2 + 18W_1W_2 - 3W_2^2)W_{n+4} + (52W_0^2 + 108W_1^2 + 12W_2^2 - 152W_0W_1 + 53W_0W_2 - 73W_1W_2)W_{n+3} + (-48W_0^2 + 140W_0W_1 - 48W_0W_2 - 100W_1^2 + 67W_1W_2 - 11W_2^2)W_{n+2}$.

**(g)** $2(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2R_n = (-8W_0^2 + 28W_0W_1 - 12W_0W_2 - 22W_1^2 + 17W_1W_2 - 3W_2^2)W_{n+3} + (48W_0^2 + 108W_1^2 + 13W_2^2 - 148W_0W_1 + 56W_0W_2 - 77W_1W_2)W_{n+2} + 4(-12W_0^2 + 36W_0W_1 - 13W_0W_2 - 26W_1^2 + 18W_1W_2 - 3W_2^2)W_{n+1}$.

**(h)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2R_n = (4W_0^2 - W_1^2 - W_2^2 - 4W_0W_1 - 2W_0W_2 + 4W_1W_2)W_{n+2} + 2(4W_0^2 + 18W_1^2 + 3W_2^2 - 20W_0W_1 + 11W_0W_2 - 16W_1W_2)W_{n+1} + 2(-8W_0^2 + 28W_0W_1 - 12W_0W_2 - 22W_1^2 + 17W_1W_2 - 3W_2^2)W_n$.

**(i)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2R_n = (28W_0^2 + 31W_1^2 + W_2^2 - 60W_0W_1 + 12W_0W_2 - 12W_1W_2)W_{n+1} + 2(-24W_0^2 + 44W_0W_1 - 4W_0W_2 - 18W_1^2 + W_1W_2 + W_2^2)W_n + 4(4W_0^2 - W_1^2 - W_2^2 - 4W_0W_1 - 2W_0W_2 + 4W_1W_2)W_{n-1}$.

**(j)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 R_n = (92W_0^2 + 119W_1^2 + 7W_2^2 - 212W_0W_1 + 52W_0W_2 - 58W_1W_2)W_n + 4(-52W_0^2 + 116W_0W_1 - 26W_0W_2 - 63W_1^2 + 28W_1W_2 - 3W_2^2)W_{n-1} + 4(28W_0^2 + 31W_1^2 + W_2^2 - 60W_0W_1 + 12W_0W_2 - 12W_1W_2)W_{n-2}$.

Next, we present a few basic relations between $\{W_n\}$ and $\{C_n\}$.

**Lemma 4.12** *The following equalities are true:*

**(a)** $8W_n = (25W_0 - 22W_1 + 5W_2)C_{n+4} + (95W_1 - 105W_0 - 22W_2)C_{n+3} + (112W_0 - 105W_1 + 25W_2)C_{n+2}$.

**(b)** $8W_n = (20W_0 - 15W_1 + 3W_2)C_{n+3} + (71W_1 - 88W_0 - 15W_2)C_{n+2} + 4(25W_0 - 22W_1 + 5W_2)C_{n+1}$.

**(c)** $2W_n = (3W_0 - W_1)C_{n+2} + (8W_1 - 15W_0 - W_2)C_{n+1} + (20W_0 - 15W_1 + 3W_2)C_n$.

**(d)** $2W_n = (3W_1 - W_2)C_{n+1} + (3W_2 - 7W_1 - 4W_0)C_n + 4(3W_0 - W_1)C_{n-1}$.

**(e)** $W_n = (4W_1 - 2W_0 - W_2)C_n + 2(3W_0 - 7W_1 + 2W_2)C_{n-1} + 2(3W_1 - W_2)C_{n-2}$.

**(f)** $2(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 C_n = (4W_0^2 + 10W_1^2 + W_2^2 - 12W_0W_1 + 3W_0W_2 - 6W_1W_2)W_{n+4} + (-12W_0^2 + 40W_0W_1 - 11W_0W_2 - 36W_1^2 + 23W_1W_2 - 4W_2^2)W_{n+3} + (16W_0^2 + 44W_1^2 + 5W_2^2 - 52W_0W_1 + 16W_0W_2 - 29W_1W_2)W_{n+2}$.

**(g)** $2(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 C_n = (8W_0^2 + 14W_1^2 + W_2^2 - 20W_0W_1 + 4W_0W_2 - 7W_1W_2)W_{n+3} + (-16W_0^2 + 44W_0W_1 - 8W_0W_2 - 36W_1^2 + 19W_1W_2 - 3W_2^2)W_{n+2} + 4(4W_0^2 + 10W_1^2 + W_2^2 - 12W_0W_1 + 3W_0W_2 - 6W_1W_2)W_{n+1}$.

**(h)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 C_n = (12W_0^2 + 17W_1^2 + W_2^2 - 28W_0W_1 + 6W_0W_2 - 8W_1W_2)W_{n+2} + 2(-12W_0^2 + 28W_0W_1 - 5W_0W_2 - 18W_1^2 + 8W_1W_2 - W_2^2)W_{n+1} + 2(8W_0^2 + 14W_1^2 + W_2^2 - 20W_0W_1 + 4W_0W_2 - 7W_1W_2)W_n$.

**(i)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 C_n = (36W_0^2 + 49W_1^2 + 3W_2^2 - 84W_0W_1 + 20W_0W_2 - 24W_1W_2)W_{n+1} + 2(-40W_0^2 + 92W_0W_1 - 20W_0W_2 - 54W_1^2 + 25W_1W_2 - 3W_2^2)W_n + 4(12W_0^2 + 17W_1^2 + W_2^2 - 28W_0W_1 + 6W_0W_2 - 8W_1W_2)W_{n-1}$.

**(j)** $(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 C_n = (100W_0^2 + 137W_1^2 + 9W_2^2 - 236W_0W_1 + 60W_0W_2 - 70W_1W_2)W_n + 4(-60W_0^2 + 140W_0W_1 - 34W_0W_2 - 81W_1^2 + 40W_1W_2 - 5W_2^2)W_{n-1} + 4(36W_0^2 + 49W_1^2 + 3W_2^2 - 84W_0W_1 + 20W_0W_2 - 24W_1W_2)W_{n-2}$.

Now, we give a few basic relations between $\{G_n\}$ and $\{H_n\}$.

**Lemma 4.13** *The following equalities are true:*

$$\begin{aligned}
4H_n &= 5G_{n+4} - 19G_{n+3} + 18G_{n+2},\\
2H_n &= 3G_{n+3} - 11G_{n+2} + 10G_{n+1},\\
H_n &= 2G_{n+2} - 7G_{n+1} + 6G_n,\\
H_n &= 3G_{n+1} - 10G_n + 8G_{n-1},\\
H_n &= 5G_n - 16G_{n-1} + 12G_{n-2}.
\end{aligned}$$

Next, we present a few basic relations between $\{G_n\}$ and $\{R_n\}$.

**Lemma 4.14** *The following equalities are true:*

$$\begin{aligned}
8G_n &= -13R_{n+4} + 49R_{n+3} - 44R_{n+2},\\
2G_n &= -4R_{n+3} + 15R_{n+2} - 13R_{n+1},\\
2G_n &= -5R_{n+2} + 19R_{n+1} - 16R_n,\\
G_n &= -3R_{n+1} + 12R_n - 10R_{n-1},\\
G_n &= -3R_n + 14R_{n-1} - 12R_{n-2},
\end{aligned}$$

*and*

$$\begin{aligned}
8R_n &= -11G_{n+4} + 43G_{n+3} - 40G_{n+2},\\
2R_n &= -3G_{n+3} + 12G_{n+2} - 11G_{n+1},\\
2R_n &= -3G_{n+2} + 13G_{n+1} - 12G_n,\\
R_n &= -G_{n+1} + 6G_n - 6G_{n-1},\\
R_n &= G_n + 2G_{n-1} - 4G_{n-2}.
\end{aligned}$$

Now, we give a few basic relations between $\{G_n\}$ and $\{C_n\}$.

**Lemma 4.15** *The following equalities are true:*

$$\begin{aligned}
8G_n &= 3C_{n+4} - 15C_{n+3} + 20C_{n+2}, \\
2G_n &= -C_{n+2} + 3C_{n+1}, \\
G_n &= -C_{n+1} + 4C_n - 2C_{n-1}, \\
G_n &= -C_n + 6C_{n-1} - 4C_{n-2},
\end{aligned}$$

*and*

$$\begin{aligned}
8C_n &= 5G_{n+4} - 21G_{n+3} + 24G_{n+2}, \\
2C_n &= G_{n+3} - 4G_{n+2} + 5G_{n+1}, \\
2C_n &= G_{n+2} - 3G_{n+1} + 4G_n, \\
C_n &= G_{n+1} - 2G_n + 2G_{n-1}, \\
C_n &= 3G_n - 6G_{n-1} + 4G_{n-2}.
\end{aligned}$$

Next, we present a few basic relations between $\{H_n\}$ and $\{R_n\}$.

**Lemma 4.16** *The following equalities are true:*

$$\begin{aligned}
4H_n &= -3R_{n+4} + 13R_{n+3} - 14R_{n+2}, \\
2H_n &= -R_{n+3} + 5R_{n+2} - 6R_{n+1}, \\
H_n &= R_{n+1} - 2R_n, \\
H_n &= 3R_n - 8R_{n-1} + 4R_{n-2}.
\end{aligned}$$

Now, we give a few basic relations between $\{H_n\}$ and $\{C_n\}$.

**Lemma 4.17** *The following equalities are true:*

$$\begin{aligned}
4H_n &= 5C_{n+4} - 19C_{n+3} + 18C_{n+2}, \\
2H_n &= 3C_{n+3} - 11C_{n+2} + 10C_{n+1}, \\
H_n &= 2C_{n+2} - 7C_{n+1} + 6C_n, \\
H_n &= 3C_{n+1} - 10C_n + 8C_{n-1}, \\
H_n &= 5C_n - 16C_{n-1} + 12C_{n-2}.
\end{aligned}$$

Next, we present a few basic relations between $\{R_n\}$ and $\{C_n\}$.

**Lemma 4.18** *The following equalities are true:*

$$\begin{aligned}
4R_n &= -6C_{n+4} + 23C_{n+3} - 21C_{n+2},\\
4R_n &= -7C_{n+3} + 27C_{n+2} - 24C_{n+1},\\
R_n &= -2C_{n+2} + 8C_{n+1} - 7C_n,\\
R_n &= -2C_{n+1} + 9C_n - 8C_{n-1},\\
R_n &= -C_n + 8C_{n-1} - 8C_{n-2},
\end{aligned}$$

*and*

$$\begin{aligned}
4C_n &= -6R_{n+4} + 23R_{n+3} - 21R_{n+2},\\
4C_n &= -7R_{n+3} + 27R_{n+2} - 24R_{n+1},\\
C_n &= -2R_{n+2} + 8R_{n+1} - 7R_n,\\
C_n &= -2R_{n+1} + 9R_n - 8R_{n-1},\\
C_n &= -R_n + 8R_{n-1} - 8R_{n-2}.
\end{aligned}$$

## 4.4 ON THE RECURRENCE PROPERTIES OF GENERALIZED WOODALL SEQUENCE

Taking $r = 5, s = -8, t = 4$ in Theorem 4.5, we obtain the following Proposition.

**Proposition 4.19** *For $n \in \mathbb{Z}$, generalized triangular numbers (the case $r = 5, s = -8, t = 4$) have the following identity:*

$$W_{-n} = 4^{-n}(W_{2n} - H_n W_n + \frac{1}{2}(H_n^2 - H_{2n})W_0)$$

*where*

$$H_n = \frac{((10W_0 - 11W_1 + 3W_2)W_{n+2} - 2(16W_0 - 18W_1 + 5W_2)W_{n+1} + 4(6W_0 - 7W_1 + 2W_2)W_n)}{(2W_0 - 3W_1 + W_2)(4W_0 - 4W_1 + W_2)} \tag{4.16}$$

Note that if we take $r = 5, s = -8, t = 4$ in Lemma 4.6 (or using Lemma 4.10 (c)) we get (4.16).

From the above Proposition and Corollary 4.2, we have the following corollary which gives the connection between the special cases of generalized triangular sequence at the positive index and the negative index: for modified Woodall, modified Cullen, Woodall and Cullen numbers: take $W_n = G_n$ with $G_0 = 0, G_1 = 1, G_2 = 5$, take $W_n = H_n$ with

$H_0 = 3, H_1 = 5, H_2 = 9$, $W_n = R_n$ with $R_0 = -1, R_1 = 1, R_2 = 7$ and $W_n = C_n$ with $C_0 = 1, C_1 = 3, C_2 = 9$, respectively. Note that in this case $H_n = H_n$.

**Corollary 4.5** *For $n \in \mathbb{Z}$, we have the following recurrence relations:*

**(a)** *Modified Woodall sequence:*

$$G_{-n} = 4^{-n}(-6G_n^2 + G_{2n} - 2G_{n+2}G_n + 7G_{n+1}G_n).$$

**(b)** *Modified Cullen sequence:*

$$H_{-n} = 2^{-2n-1}\left(H_n^2 - H_{2n}\right).$$

**(c)** *Woodall sequence:*

$$R_{-n} = 2^{-2n-1}(-R_{n+1}^2 + R_{2n+1} + 2R_{n+1}R_n).$$

**(d)** *Cullen sequence:*

$$\begin{aligned} C_{-n} &= 2^{-2n-1}(4C_{n+2}^2 + 49C_{n+1}^2 + 24C_n^2 - 2C_{2n+2} + 7C_{2n+1} - 4C_{2n} - 28C_{n+1}C_{n+2} \\ &\quad +20C_nC_{n+2} - 70C_nC_{n+1}). \end{aligned}$$

## 4.5 SUM FORMULAS

The following Theorem presents some formulas of of generalized Woodall numbers numbers with indices in arithmetic progression.

**Theorem 4.20** *For all integers $m$ and $j$, we have the following sum formula:*

$$\sum_{k=0}^{n} W_{mk+j} = \frac{1}{2\left(2^m - 1\right)^2}\Gamma$$

*where*

$\Gamma = ((j + mn - 2)2^{mn+2m+j} - (j + m + mn - 2)2^{mn+m+j} + (m - j + 2)2^{m+j} + (j - 2)2^j + 2(n + 1)(2^m - 1)^2)W_2 + (-(3j + 3mn - 8)2^{mn+2m+j} + (3j + 3m + 3mn - 8)2^{mn+m+j} + (3j - 3m - 8)2^{m+j} - (3j - 8)2^j - 8(n + 1)(2^m - 1)^2)W_1 + 2((j + mn - 3)2^{mn+2m+j} - (j + m + mn - 3)2^{mn+m+j} + (m - j + 3)2^{m+j} + (j - 3)2^j + 4(n + 1)(2^m - 1)^2)W_0.$

Proof. Use the Binet's formula of generalized Woodall numbers, i.e.,

$$W_n = ((-W_2 + 4W_1 - 3W_0) + \frac{W_2 - 3W_1 + 2W_0}{2} n) \times 2^n + (W_2 - 4W_1 + 4W_0). \quad \square$$

The following proposition presents some formulas of generalized Woodall numbers numbers with positive subscripts.

**Proposition 4.21** *For $n \geq 0$, we have the following formulas:*

**(a)** $\sum_{k=0}^{n} W_k = ((n-3)2^n+n+3)W_2-((3n-11)2^n+4n+11)W_1+((n-4)2^{n+1}+4n+9)W_0$.

**(b)** $\sum_{k=0}^{n} W_{2k} = \frac{1}{9}(((3n-4)2^{2n+2} + 9n + 16)W_2 - 12((3n-5)2^{2n} + 3n + 5)W_1 + ((6n - 11)2^{2n+2} + 36n + 53)W_0)$.

**(c)** $\sum_{k=0}^{n} W_{2k+1} = \frac{1}{9}(((6n-5)2^{2n+2} + 9n + 20)W_2 - 3((6n-7)2^{2n+2} + 12n + 25)W_1 + 4((3n-4)2^{2n+2} + 9n + 16)W_0)$.

Proof. Take $m = 1, j = 0$; $m = 2, j = 0$ and $m = 2, j = 1$, respectively, in Theorem 4.20. $\square$

From Theorem 4.20, we have the following corollary.

**Corollary 4.6** *For all integers $m$ and $j$, we have the following sum formulas:*

**(a)** $\sum_{k=0}^{n} G_{mk+j} = \frac{1}{(2^m-1)^2}((j + mn - 1)2^{mn+2m+j} - (j + m + mn - 1)2^{mn+m+j} + (n + 1)2^{2m} - (n + 1)2^{m+1} - (j - m - 1)2^{m+j} + (j - 1)2^j + n + 1)$.

**(b)** $\sum_{k=0}^{n} H_{mk+j} = \frac{1}{(2^m-1)}(2^{mn+m+j+1} + (n + 1)2^m - 2^{j+1} - n - 1)$.

**(c)** $\sum_{k=0}^{n} R_{mk+j} = \frac{1}{(2^m-1)^2}((j + mn)2^{mn+2m+j} - (j + m + mn)2^{mn+m+j} - (n + 1)2^{2m} + (n + 1)2^{m+1} + (m - j)\,2^{m+j} + 2^j j - n - 1)$.

**(d)** $\sum_{k=0}^{n} C_{mk+j} = \frac{1}{(2^m-1)^2}((j + mn)2^{mn+2m+j} - (j + m + mn)2^{mn+m+j} + (n + 1)2^{2m} - (n + 1)2^{m+1} + (m - j)2^{m+j} + 2^j j + n + 1)$.

From the last Proposition 4.21 (or using Corollary 4.6), we have the following corollary which gives sum formulas of modified Woodall numbers (take $W_n = G_n$ with $G_0 = 0, G_1 = 1, G_2 = 5$).

**Corollary 4.7** *For $n \geq 0$ we have the following formulas:*

**(a)** $\sum_{k=0}^{n} G_k = (n-2)\,2^{n+1} + n + 4$.

**(b)** $\sum_{k=0}^{n} G_{2k} = \frac{1}{9}((6n-5)2^{2n+2} + 9n + 20)$.

**(c)** $\sum_{k=0}^{n} G_{2k+1} = \frac{1}{9}((3n-1)2^{2n+4} + 9n + 25)$.

Taking $W_n = H_n$ with $H_0 = 3, H_1 = 5, H_2 = 9$ in the last Proposition 4.21 (or using Corollary 4.6), we have the following corollary which presents sum formulas of modified Cullen numbers.

**Corollary 4.8** *For $n \geq 0$ we have the following formulas:*

**(a)** $\sum_{k=0}^{n} H_k = 2^{n+2} + n - 1$.

**(b)** $\sum_{k=0}^{n} H_{2k} = \frac{1}{3}(2^{2n+3} + 3n + 1)$.

**(c)** $\sum_{k=0}^{n} H_{2k+1} = \frac{1}{3}(2^{2n+4} + 3n - 1)$.

From the last Proposition 4.21 (or using Corollary 4.6), we have the following corollary which gives sum formulas of Woodall numbers (take $W_n = R_n$ with $R_0 = -1, R_1 = 1, R_2 = 7$).

**Corollary 4.9** *For $n \geq 0$ we have the following formulas:*

**(a)** $\sum_{k=0}^{n} R_k = (n-1)(2^{n+1} - 1)$.

**(b)** $\sum_{k=0}^{n} R_{2k} = \frac{1}{9}((3n-1)2^{2n+3} - 9n - 1)$.

**(c)** $\sum_{k=0}^{n} R_{2k+1} = \frac{1}{9}((6n+1)2^{2n+3} - 9n + 1)$.

Taking $W_n = C_n$ with $C_0 = 1, C_1 = 3, C_2 = 9$ in the last Proposition, we have the following corollary which presents sum formulas of Cullen numbers.

**Corollary 4.10** *For $n \geq 0$ we have the following formulas:*

**(a)** $\sum_{k=0}^{n} C_k = (n-1)2^{n+1} + n + 3$.

**(b)** $\sum_{k=0}^{n} C_{2k} = \frac{1}{9}((3n-1)2^{2n+3} + 9n + 17)$.

**(c)** $\sum_{k=0}^{n} C_{2k+1} = \frac{1}{9}((6n+1)2^{2n+3} + 9n + 19)$.

## 4.6 MATRICES RELATED WITH GENERALIZED WOODALL NUMBERS

We define the square matrix $A$ of order 3 as:

$$A = \begin{pmatrix} 5 & -8 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

such that $\det A = 4$. From (4.10) we have

$$\begin{pmatrix} W_{n+2} \\ W_{n+1} \\ W_n \end{pmatrix} = \begin{pmatrix} 5 & -8 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} W_{n+1} \\ W_n \\ W_{n-1} \end{pmatrix} \tag{4.17}$$

and from (4.6) (or using (4.17) and induction) we have

$$\begin{pmatrix} W_{n+2} \\ W_{n+1} \\ W_n \end{pmatrix} = \begin{pmatrix} 5 & -8 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n \begin{pmatrix} W_2 \\ W_1 \\ W_0 \end{pmatrix}.$$

If we take $W = G$ in (4.17) we have

$$\begin{pmatrix} G_{n+2} \\ G_{n+1} \\ G_n \end{pmatrix} = \begin{pmatrix} 5 & -8 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} G_{n+1} \\ G_n \\ G_{n-1} \end{pmatrix}.$$

We also define

$$B_n = \begin{pmatrix} G_{n+1} & -8G_n + 4G_{n-1} & 4G_n \\ G_n & -8G_{n-1} + 4G_{n-2} & 4G_{n-1} \\ G_{n-1} & -8G_{n-2} + 4G_{n-3} & 4G_{n-2} \end{pmatrix}$$

and

$$C_n = \begin{pmatrix} W_{n+1} & -8W_n + 4W_{n-1} & 4W_n \\ W_n & -8W_{n-1} + 4W_{n-2} & 4W_{n-1} \\ W_{n-1} & -8W_{n-2} + 4W_{n-3} & 4W_{n-2} \end{pmatrix}$$

**Theorem 4.22** *For all integer $m, n \geq 0$, we have*

**(a)** $B_n = A^n$

**(b)** $C_1 A^n = A^n C_1$

**(c)** $C_{n+m} = C_n B_m = B_m C_n$.

Proof. Take $r = 5, s = -8, t = 4$ in Soykan [22, Theorem 5.1.]. □

Some properties of matrix $A^n$ can be given as

$$A^n = 5A^{n-1} - 8A^{n-1} + 4A^{n-3}$$

and

$$A^{n+m} = A^n A^m = A^m A^n$$

and

$$\det(A^n) = 4^n$$

for all integer $m$ and $n$.

**Corollary 4.11** *For all integers $n$, we have the following formulas for the modified Woodall, Woodall and Cullen numbers.*

**(a)** *Modified Woodall Numbers.*

$$\begin{aligned} A^n &= \begin{pmatrix} 5 & -8 & 4 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n = \begin{pmatrix} G_{n+1} & -8G_n + 4G_{n-1} & 4G_n \\ G_n & -8G_{n-1} + 4G_{n-2} & 4G_{n-1} \\ G_{n-1} & -8G_{n-2} + 4G_{n-3} & 4G_{n-2} \end{pmatrix} \\ &= \begin{pmatrix} 2^{n+1}n + 1 & 4 \times 2^n - 6 \times 2^n n - 4 & 4 \times 2^n n - 4 \times 2^n + 4 \\ 2^n n - 2^n + 1 & 5 \times 2^n - 3 \times 2^n n - 4 & 2 \times 2^n n - 4 \times 2^n + 4 \\ \frac{1}{2}2^n n - 2^n + 1 & 2^{n+2} - \frac{3}{2}2^n n - 4 & 2^n n - 3 \times 2^n + 4 \end{pmatrix}. \end{aligned}$$

**(b)** *Woodall Numbers.*

$$A^n = \frac{1}{2}\begin{pmatrix} -5R_{n+3} + 19R_{n+2} - 16R_{n+1} & 24R_{n+2} - 92R_{n+1} + 76R_n & 4(-5R_{n+2} + 19R_{n+1} - 16R_n) \\ -5R_{n+2} + 19R_{n+1} - 16R_n & 24R_{n+1} - 92R_n + 76R_{n-1} & 4(-5R_{n+1} + 19R_n - 16R_{n-1}) \\ -5R_{n+1} + 19R_n - 16R_{n-1} & 24R_n - 92R_{n-1} + 76R_{n-2} & 4(-5R_n + 19R_{n-1} - 16R_{n-2}) \end{pmatrix}.$$

**(c)** *Cullen Numbers.*

$$A^n = \begin{pmatrix} -C_{n+2} + 4C_{n+1} - 2C_n & 6C_{n+1} - 26C_n + 16C_{n-1} & 4(-C_{n+1} + 4C_n - 2C_{n-1}) \\ -C_{n+1} + 4C_n - 2C_{n-1} & 6C_n - 26C_{n-1} + 16C_{n-2} & 4(-C_n + 4C_{n-1} - 2C_{n-2}) \\ -C_n + 4C_{n-1} - 2C_{n-2} & 6C_{n-1} - 26C_{n-2} + 16C_{n-3} & 4(-C_{n-1} + 4C_{n-2} - 2C_{n-3}) \end{pmatrix}.$$

Proof.

**(a)** It is given in Theorem 4.22 (a).

**(b)** Note that, from Lemma 4.14, we have

$$2G_n = -5R_{n+2} + 19R_{n+1} - 16R_n.$$

Using the last equation and (a), we get required result.

**(c)** Note that, from Lemma 4.15, we have

$$G_n = -C_{n+1} + 4C_n - 2C_{n-1}.$$

Using the last equation and (a), we get required result. □

**Theorem 4.23** *For all integers $m, n$, we have*

$$\begin{aligned} W_{n+m} &= W_n G_{m+1} + W_{n-1}(-8G_m + 4G_{m-1}) + 4W_{n-2}G_m \\ &= W_n G_{m+1} + (-8W_{n-1} + 4W_{n-2})\, G_m + 4W_{n-1}G_{m-1} \end{aligned} \tag{4.18}$$

Proof. Take $r = 5, s = -8, t = 4$ in Soykan [22, Theorem 5.2.]. □

By Lemma 4.9, we know that

$$\begin{aligned} (4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 G_m &= (4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{m+2} \\ &\quad +(W_2^2 - 4W_0W_1 + 8W_0W_2 - 5W_1W_2)W_{m+1} \\ &\quad +4(W_1^2 - W_0W_2)W_m. \end{aligned}$$

so (4.18) can be written in the following form

$$\begin{aligned} &(4W_0 - 4W_1 + W_2)(2W_0 - 3W_1 + W_2)^2 W_{n+m} \\ = \;& W_n((4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{m+3} \\ &+(W_2^2 - 4W_0W_1 + 8W_0W_2 - 5W_1W_2)W_{m+2} + 4(W_1^2 - W_0W_2)W_{m+1}) \\ &+ (-8W_{n-1} + 4W_{n-2})\,((4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{m+2} \\ &+(W_2^2 - 4W_0W_1 + 8W_0W_2 - 5W_1W_2)W_{m+1} + 4(W_1^2 - W_0W_2)W_m) \\ &+4W_{n-1}((4W_0^2 + 5W_1^2 - 8W_0W_1 - W_1W_2)W_{m+1} \\ &+(W_2^2 - 4W_0W_1 + 8W_0W_2 - 5W_1W_2)W_m + 4(W_1^2 - W_0W_2)W_{m-1}). \end{aligned}$$

**Corollary 4.12** *For all integers $m, n$, we have*

$$\begin{aligned}
G_{n+m} &= G_nG_{m+1} + G_{n-1}(-8G_m + 4G_{m-1}) + 4G_{n-2}G_m,\\
H_{n+m} &= H_nG_{m+1} + H_{n-1}(-8G_m + 4G_{m-1}) + 4H_{n-2}G_m,\\
R_{n+m} &= R_nG_{m+1} + R_{n-1}(-8G_m + 4G_{m-1}) + 4R_{n-2}G_m,\\
C_{n+m} &= C_nG_{m+1} + C_{n-1}(-8G_m + 4G_{m-1}) + 4C_{n-2}G_m,
\end{aligned}$$

*and*

$$\begin{aligned}
2R_{m+n} &= -5R_nR_{m+3} + (19R_n + 40R_{n-1} - 20R_{n-2})\,R_{m+2}\\
&\quad +4(-4R_n - 43R_{n-1} + 19R_{n-2})R_{m+1} + 4(51R_{n-1} - 16R_{n-2})R_m - 64R_{n-1}R_{m-1},\\
2C_{m+n} &= -C_nC_{m+3} + (3C_n + 8C_{n-1} - 4C_{n-2})C_{m+2}\\
&\quad +4(-7C_{n-1} + 3C_{n-2})C_{m+1} + 12C_{n-1}C_m.
\end{aligned}$$

Taking $m = n$ in the last corollary we obtain the following identities:

$$\begin{aligned}
G_{2n} &= 4G_{n-1}^2 + (G_{n+1} - 8G_{n-1} + 4G_{n-2})G_n,\\
H_{2n} &= H_nG_{n+1} - 4\,(2H_{n-1} - H_{n-2})\,G_n + 4H_{n-1}G_{n-1},\\
R_{2n} &= R_nG_{n+1} - 4\,(2R_{n-1} - R_{n-2})\,G_n + 4R_{n-1}G_{n-1},\\
C_{2n} &= C_nG_{n+1} - 4\,(2C_{n-1} - C_{n-2})\,G_n + 4C_{n-1}G_{n-1},
\end{aligned}$$

and

$$\begin{aligned}
2R_{2n} &= -5R_nR_{n+3} + (19R_n + 40R_{n-1} - 20R_{n-2})\,R_{n+2}\\
&\quad +4(-4R_n - 43R_{n-1} + 19R_{n-2})R_{n+1}\\
&\quad +4(51R_{n-1} - 16R_{n-2})R_n - 64R_{n-1}R_{n-1},\\
2C_{2n} &= -C_nC_{n+3} + (3C_n + 8C_{n-1} - 4C_{n-2})C_{n+2}\\
&\quad +4(-7C_{n-1} + 3C_{n-2})C_{n+1} + 12C_{n-1}C_n.
\end{aligned}$$

## CHAPTER 5

## CRYPTOGRAPHY USING FIBONACCI AND LUCAS NUMBERS

In this chapter we introduce a new coding/decoding algorithm using Fibonacci $Q$-matrix and $R$-matrix. We put our message in a matrix of even size adding point between two words and zero end of the message until we obtain the size of the message matrix is even. Dividing the message square matrix $S$ of size $2m$ into the block matrices, named $B_i$ $(1 \leq i \leq m^2)$ of size $2 \times 2$, from left to right, we construct a new coding method.
The symbols of our coding method:

$$B_i = \begin{bmatrix} b_{i,1} & b_{i,2} \\ b_{i,3} & b_{i,4} \end{bmatrix}, E_i = \begin{bmatrix} e_{i,1} & e_{i,2} \\ e_{i,3} & e_{i,4} \end{bmatrix}, Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} q_1 & q_2 \\ q_3 & q_4 \end{bmatrix}, R = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}$$

$$\text{and } R_{n,p} = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}^p . \begin{bmatrix} q_1 & q_2 \\ q_3 & q_4 \end{bmatrix} = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}.$$

The number of the block matrices $B_i$ is denoted by $s$. According to $s$, we choose the numbers which are $n$ and $p$ as follows:

$$n = \begin{cases} s & , \quad s < 4 \\ \left[\left|\frac{s}{2}\right|\right] + 1 & , \quad s \geq 4 \end{cases},$$

$$p = \begin{cases} 3 & , \quad s < 4 \\ \text{the first prime number bigger than } \left[\left|\frac{s}{2}\right|\right] + 1 & , \quad s \geq 4 \end{cases}$$

Using the chosen $n$ and $p$, we write the following character table according to mod 45. This table can be extended according to the used characters in the message matrix. Lower cases can be added to this table. The order of the characters doesn't matter. We can order the characters as we want.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H |
| n+p | n+p+1 | n+p+2 | n+p+3 | n+p+4 | n+p+5 | n+p+6 | n+p+7 |
| I | J | K | L | M | N | O | P |
| n+p+8 | n+p+9 | n+p+10 | n+p+11 | n+p+12 | n+p+13 | n+p+14 | n+p+15 |
| Q | R | S | T | U | V | W | X |
| n+p+16 | n+p+17 | n+p+18 | n+p+19 | n+p+20 | n+p+21 | n+p+22 | n+p+23 |
| Y | Z | 0 | 1 | 2 | 3 | 4 | 5 |
| n+p+24 | n+p+25 | n+p+26 | n+p+27 | n+p+28 | n+p+29 | n+p+30 | n+p+31 |
| 6 | 7 | 8 | 9 | . | , | ! | ? |
| n+p+32 | n+p+33 | n+p+34 | n+p+35 | n+p+36 | n+p+37 | n+p+38 | n+p+39 |
| - | + | × | ÷ | = | | | |
| n+p+40 | n+p+41 | n+p+42 | n+p+43 | n+p+44 | | | |

**Coding Algorithm**

**Step 1**. Divide the matrix $S$ into blocks $B_i$ $(1 \leq i \leq m^2)$.

**Step 2**. Choose $n$ and $p$.

**Step 3**. Determine $b_{i,j}$ $(1 \leq j \leq 4)$.

**Step 4**. Compute $\det(B_i) = d_i$

**Step 5**. Construct $V = [b_{i,k}, d_i]_{k \in \{2,3,4\}}$.

**Step 6**. Transmit $(n, p, V)$.

**Decoding Algorithm**

**Step 1**. Compute $R_{n,p}$.

**Step 2**. Determine $r_k$ $(1 \leq k \leq 4)$.

**Step 3**. Compute $r_1 b_{i,3} + r_3 b_{i,4} \longrightarrow e_{i,3}$ $(1 \leq i \leq m^2)$.

**Step 4**. Compute $r_2 b_{i,3} + r_4 b_{i,4} \longrightarrow e_{i,4}$.

**Step 5**. Solve $5^p \times (-1)^{n+p} \times d_i = e_{i,4}(r_1 x_i + r_3 b_{i,2}) - e_{i,3}(r_2 x_i + r_4 b_{i,2})$.

**Step 6**. Substitute for $x_i = b_{i,1}$

**Step 7**. Construct $B_i$.

**Step 8**. Construct $S$.

**Step 9**. End of algorithm.

**Example 5.1** *Let us consider the message matrix for the message text "CODING ALGORITHM"*

$$S = \begin{bmatrix} C & O & D & I \\ N & G & . & A \\ L & G & O & R \\ I & T & H & M \end{bmatrix}_{4\times 4}$$

***Coding Algorithm***

***Step 1.***

$$B_1 = \begin{bmatrix} C & O \\ N & G \end{bmatrix},\ B_2 = \begin{bmatrix} D & I \\ . & A \end{bmatrix},\ B_3 = \begin{bmatrix} L & G \\ I & T \end{bmatrix},\ B_4 = \begin{bmatrix} O & R \\ H & M \end{bmatrix}$$

***Step 2.*** *Since* $s = 4 \geq 4$, *we calculate* $n = \left[\left|\frac{s}{2}\right|\right] + 1 = 3$, $p = 5$.

| $C$ | $O$ | $D$ | $I$ | $N$ | $G$ | $.$ | $A$ |
|---|---|---|---|---|---|---|---|
| 10 | 22 | 11 | 16 | 21 | 14 | 44 | 8 |
| $L$ | $G$ | $O$ | $R$ | $I$ | $T$ | $H$ | $M$ |
| 19 | 14 | 22 | 25 | 16 | 27 | 15 | 20 |

***Step 3***. *We have the elements of the blocks* $B_i$ $(1 \leq i \leq 4)$ *as follows:*

$b_{1,1} = 10 \quad b_{1,2} = 22 \quad b_{1,3} = 21 \quad b_{1,4} = 14$

$b_{2,1} = 11 \quad b_{2,2} = 16 \quad b_{2,3} = 44 \quad b_{2,4} = 8$

$b_{3,1} = 19 \quad b_{3,2} = 14 \quad b_{3,3} = 16 \quad b_{3,4} = 27$

$b_{4,1} = 22 \quad b_{4,2} = 25 \quad b_{4,3} = 15 \quad b_{4,4} = 20$

***Step 4***. *We calculate the* $\det(B_i) = d_i$.

$d_1 = -322$

$d_2 = -616$

$d_3 = 289$

$d_4 = 65$

***Step 5***. *Now we obtain the following matrix* $V$*:*

$$V = \begin{bmatrix} 22 & 21 & 14 & -322 \\ 16 & 44 & 8 & -616 \\ 14 & 16 & 27 & 289 \\ 25 & 15 & 20 & 65 \end{bmatrix}$$

***Step 6.*** *Transmit* $(3, 5, \begin{bmatrix} 22 & 21 & 14 & -322 \\ 16 & 44 & 8 & -616 \\ 14 & 16 & 27 & 289 \\ 25 & 15 & 20 & 65 \end{bmatrix})$.

***Decoding Algorithm***

***Step 1***.

$$R_{3,5} = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}^5 . \begin{bmatrix} F_4 & F_3 \\ F_3 & F_2 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}^5 . \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 175 & 100 \\ 100 & 75 \end{bmatrix}$$

***Step 2***. $r_1 = 175$, $r_2 = 100$, $r_3 = 100$, $r_4 = 75$.

***Step 3***. $r_1 b_{i,3} + r_3 b_{i,4} \longrightarrow e_{i,3}$

$175.21 + 100.14 = 5075 = e_{1,3}$

$175.44 + 100.8 = 8500 = e_{2,3}$

$175.16 + 100.27 = 5500 = e_{3,3}$

$175.15 + 100.20 = 4625 = e_{4,3}$

***Step 4***. $r_2 b_{i,3} + r_4 b_{i,4} \longrightarrow e_{i,4}$

$100.21 + 75.14 = 3150 = e_{1,4}$

$100.44 + 75.8 = 5000 = e_{2,4}$

$100.16 + 75.27 = 3625 = e_{3,4}$

$100.15 + 75.20 = 3000 = e_{4,4}$

***Step 5***. *We calculate the elements* $x_i$.

$5^p \times (-1)^{n+p} \times d_i = e_{i,4}(r_1 x_i + r_3 b_{i,2}) - e_{i,3}(r_2 x_i + r_4 b_{i,2})$

$5^5 \times (-1)^8 \times (-322) = 3150(175.x_1 + 100.22) - 5075(100.x_1 + 75.22) \Longrightarrow x_1 = 10$

$5^5 \times (-1)^8 \times (-616) = 5000(175.x_2 + 100.16) - 8500(100.x_2 + 75.16) \Longrightarrow x_2 = 11$

$5^5 \times (-1)^8 \times (289) = 3625(175.x_3 + 100.14) - 5500(100.x_3 + 75.14) \Longrightarrow x_3 = 19$

$5^5 \times (-1)^8 \times (65) = 3000(175.x_4 + 100.25) - 4625(100.x_4 + 75.25) \Longrightarrow x_4 = 22$

***Step 6***. $x_i = b_{i,1}$

$x_1 = b_{1,1} = 10$, $x_2 = b_{2,1} = 11$, $x_3 = b_{3,1} = 19$, $x_4 = b_{4,1} = 22$.

***Step 7***. *We construct the block matrices* $B_i$*:*

$$B_1 = \begin{bmatrix} 10 & 22 \\ 21 & 14 \end{bmatrix}, B_2 = \begin{bmatrix} 11 & 16 \\ 44 & 8 \end{bmatrix}, B_3 = \begin{bmatrix} 19 & 14 \\ 16 & 27 \end{bmatrix}, B_4 = \begin{bmatrix} 22 & 25 \\ 15 & 20 \end{bmatrix}.$$

***Step 8***. *We obtain the message matrix $S$:*

$$S = \begin{bmatrix} 10 & 22 & 11 & 16 \\ 21 & 14 & 44 & 8 \\ 19 & 14 & 22 & 25 \\ 16 & 27 & 15 & 20 \end{bmatrix} = \begin{bmatrix} C & O & D & I \\ N & G & . & A \\ L & G & O & R \\ I & T & H & M \end{bmatrix}.$$

***Step 9***. *End of algorithm.*

## CHAPTER 6

## PADOVAN MATRICES IN CODING THEORY

In this chapter, we investigate Padovan numbers $P_n$ $(n \geq 0)$. Also we develop a new coding theory on Padovan matrices.

Introducing the square matrix $A$ of order 3 as:

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} P_{-1} & P_0 & P_{-2} \\ P_{-2} & P_{-1} & P_{-3} \\ P_{-3} & P_{-2} & P_{-4} \end{pmatrix} \tag{6.1}$$

such that $\det A = 1$.

The inverse of $A$ is as:

$$\begin{aligned} A^{-1} &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} P_{-1}P_{-4} - P_{-2}P_{-3} & P_{-2}^2 - P_0P_{-4} & P_0P_{-3} - P_{-1}P_{-2} \\ P_{-3}^2 - P_{-2}P_{-4} & P_{-1}P_{-4} - P_{-2}P_{-3} & P_{-2}^2 - P_{-1}P_{-3} \\ P_{-2}^2 - P_{-1}P_{-3} & P_0P_{-3} - P_{-1}P_{-2} & P_{-1}^2 - P_0P_{-2} \end{pmatrix} \end{aligned} \tag{6.2}$$

such that $\det A^{-1} = 1$.

Also

$$A^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_{-1} \\ P_{-1} & P_0 & P_{-2} \\ P_{-2} & P_{-1} & P_{-3} \end{pmatrix} \tag{6.3}$$

such that $\det A^2 = 1$ and

$$A^{-2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{pmatrix} \tag{6.4}$$

$$= \begin{pmatrix} P_0P_{-3} - P_{-1}P_{-2} & P_{-1}^2 - P_1P_{-3} & P_0P_{-1} - P_1P_{-2} \\ P_{-2}^2 - P_{-1}P_{-3} & P_0P_{-3} - P_{-1}P_{-2} & P_{-1}^2 - P_0P_{-2} \\ P_{-1}^2 - P_0P_{-2} & P_0P_{-1} - P_1P_{-2} & P_0^2 - P_1P_{-1} \end{pmatrix}$$

such that $\det A^{-2} = 1$.

**Theorem 6.1**

$$A^n = \begin{pmatrix} P_{n-2} & P_{n-1} & P_{n-3} \\ P_{n-3} & P_{n-2} & P_{n-4} \\ P_{n-4} & P_{n-3} & P_{n-5} \end{pmatrix} \quad \textit{where } A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Proof. The proof can be given by mathematical induction. □

**Theorem 6.2**

$$A^{-n} = \begin{pmatrix} P_{n-2}P_{n-5} - P_{n-3}P_{n-4} & P_{n-1}P_{n-5} - P_{n-3}^2 & P_{n-1}P_{n-4} - P_{n-2}P_{n-3} \\ P_{n-3}P_{n-5} - P_{n-4}^2 & P_{n-2}P_{n-5} - P_{n-3}P_{n-4} & P_{n-2}P_{n-4} - P_{n-3}^2 \\ P_{n-2}P_{n-4} - P_{n-3}^2 & P_{n-1}P_{n-4} - P_{n-2}P_{n-3} & P_{n-1}P_{n-3} - P_{n-2}^2 \end{pmatrix}$$

$$\textit{where } A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Proof. The proof can be given by mathematical induction. □

## 6.1 SOME PROPERTIES OF $A^n$ MATRIX

(1) $A^n = A^{n-2} + A^{n-3}$.

$$\begin{pmatrix} P_{n-2} & P_{n-1} & P_{n-3} \\ P_{n-3} & P_{n-2} & P_{n-4} \\ P_{n-4} & P_{n-3} & P_{n-5} \end{pmatrix} = \begin{pmatrix} P_{n-4}+P_{n-5} & P_{n-3}+P_{n-4} & P_{n-5}+P_{n-6} \\ P_{n-5}+P_{n-6} & P_{n-4}+P_{n-5} & P_{n-6}+P_{n-7} \\ P_{n-6}+P_{n-7} & P_{n-5}+P_{n-6} & P_{n-7}+P_{n-8} \end{pmatrix} \tag{6.5}$$

$$= \begin{pmatrix} P_{n-4} & P_{n-3} & P_{n-5} \\ P_{n-5} & P_{n-4} & P_{n-6} \\ P_{n-6} & P_{n-5} & P_{n-7} \end{pmatrix} + \begin{pmatrix} P_{n-5} & P_{n-4} & P_{n-6} \\ P_{n-6} & P_{n-5} & P_{n-7} \\ P_{n-7} & P_{n-6} & P_{n-8} \end{pmatrix}$$

$$= A^{n-2} + A^{n-3}.$$

(2) $A^n A^m = A^m A^n = A^{n+m}$ $(m, n = 0, \pm 1, \pm 2, \pm 3 \ldots)$.

(3) $\det A^n = 1$.

## 6.2 PADOVAN CODING/DECODING METHOD

In this section, we define a new coding theory called Padovan coding theory. Let us represent the initial message in the form of the square matrix $M$ of order 3. We take the Padovan matrix $A^n$ of order 3 as a coding matrix and its inverse matrix $A^{-n}$ as a decoding matrix for any value of $n$. We name the transformation $M \times A^n = E$ as Padovan coding, the transformation $E \times A^{-n} = M$ as Padovan decoding and define $E$ as code matrix.

**Determinant of The Code Matrix** $E$

$E = M \times A^n$

$$\det E = \det(M \times A^n) = \det M \times \det A^n = \det M \times 1 = \det M. \tag{6.6}$$

**Example of Padovan Coding/Decoding Method**

Let us represent the initial message in form of square matrix of order 3 as

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}. \tag{6.7}$$

Let us assume that all elements of the matrix are nonnegative integer i.e., $m_i \geq 0$ $(i = 1, 2, \ldots, 9)$. Let us now select for any value of $n$, the Padovan matrix as the coding matrix. We simply write for $n = 8$.

$$A^8 = \begin{pmatrix} P_6 & P_7 & P_5 \\ P_5 & P_6 & P_4 \\ P_4 & P_5 & P_3 \end{pmatrix} = \begin{pmatrix} 4 & 5 & 3 \\ 3 & 4 & 2 \\ 2 & 3 & 2 \end{pmatrix}. \tag{6.8}$$

The inverse of $A^8$ is given by

$$A^{-8} = \begin{pmatrix} P_3P_6 - P_4P_5 & P_5^2 - P_3P_7 & P_4P_7 - P_5P_6 \\ P_4^2 - P_3P_5 & P_3P_6 - P_4P_5 & P_5^2 - P_4P_6 \\ P_5^2 - P_4P_6 & P_4P_7 - P_5P_6 & P_6^2 - P_5P_7 \end{pmatrix}$$
$$= \begin{pmatrix} 2 & -1 & -2 \\ -2 & 2 & 1 \\ 1 & -2 & 1 \end{pmatrix}.$$

$$M \times A^8 = E \tag{6.9}$$

$$\begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \begin{pmatrix} 4 & 5 & 3 \\ 3 & 4 & 2 \\ 2 & 3 & 2 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix}$$

$$e_1 = 4m_1 + 3m_2 + 2m_3 \quad , \quad e_2 = 5m_1 + 4m_2 + 3m_3 \quad , \quad e_3 = 3m_1 + 2m_2 + 2m_3$$
$$e_4 = 4m_4 + 3m_5 + 2m_6 \quad , \quad e_5 = 5m_4 + 4m_5 + 3m_6 \quad , \quad e_6 = 3m_4 + 2m_5 + 2m_6$$
$$e_7 = 4m_7 + 3m_8 + 2m_9 \quad , \quad e_8 = 5m_7 + 4m_8 + 3m_9 \quad , \quad e_9 = 3m_7 + 2m_8 + 2m_9.$$

Solving these we have,

$$m_1 = 2e_1 - 2e_2 + e_3 \quad , \quad m_2 = 2e_2 - e_1 - 2e_3 \quad , \quad m_3 = e_2 - 2e_1 + e_3$$
$$m_4 = 2e_4 - 2e_5 + e_6 \quad , \quad m_5 = 2e_5 - e_4 - 2e_6 \quad , \quad m_6 = e_5 - 2e_4 + e_6$$
$$m_7 = 2e_7 - 2e_8 + e_9 \quad , \quad m_8 = 2e_8 - e_7 - 2e_9 \quad , \quad m_9 = e_8 - 2e_7 + e_9.$$

Then the code matrix $E$ is sent to a channel. The decoding of the code message $E$ given by (6.9) is performed by the following manner,

$$E \times A^{-8} = M$$
$$\begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} \begin{pmatrix} 2 & -1 & -2 \\ -2 & 2 & 1 \\ 1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 2e_1 - 2e_2 + e_3 & 2e_2 - e_1 - 2e_3 & e_2 - 2e_1 + e_3 \\ 2e_4 - 2e_5 + e_6 & 2e_5 - e_4 - 2e_6 & e_5 - 2e_4 + e_6 \\ 2e_7 - 2e_8 + e_9 & 2e_8 - e_7 - 2e_9 & e_8 - 2e_7 + e_9 \end{pmatrix}$$
$$= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}.$$

### 6.2.1 Relations Among The Code Matrix Elements

In this subsection, we develop the relations among the code matrix elements. We write the code matrix $E$ and the initial message $M$ as:

$$\begin{aligned} E &= M \times A^n = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \begin{pmatrix} P_{n-2} & P_{n-1} & P_{n-3} \\ P_{n-3} & P_{n-2} & P_{n-4} \\ P_{n-4} & P_{n-3} & P_{n-5} \end{pmatrix} \\ &= \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix}. \end{aligned}$$

We choose $n$ in such a manner that $e_i > 0$ for $i = 1, 2, 3, \ldots, 9$.

$$\begin{aligned} M &= E \times A^{-n} = \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} \begin{pmatrix} P_{n-2} & P_{n-1} & P_{n-3} \\ P_{n-3} & P_{n-2} & P_{n-4} \\ P_{n-4} & P_{n-3} & P_{n-5} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix} \\ &\quad \times \begin{pmatrix} P_{n-2}P_{n-5} - P_{n-3}P_{n-4} & P_{n-1}P_{n-5} - P_{n-3}^2 & P_{n-1}P_{n-4} - P_{n-2}P_{n-3} \\ P_{n-3}P_{n-5} - P_{n-4}^2 & P_{n-2}P_{n-5} - P_{n-3}P_{n-4} & P_{n-2}P_{n-4} - P_{n-3}^2 \\ P_{n-2}P_{n-4} - P_{n-3}^2 & P_{n-1}P_{n-4} - P_{n-2}P_{n-3} & P_{n-1}P_{n-3} - P_{n-2}^2 \end{pmatrix} \\ &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}. \end{aligned}$$

Also,

$$\det A^n = P_{n-5}P_{n-2}^2 - 2P_{n-2}P_{n-3}P_{n-4} + P_{n-3}^3 - P_{n-1}P_{n-5}P_{n-3} + P_{n-1}P_{n-4}^2 \tag{6.10}$$

$$\begin{aligned} \det A^n &= P_{n-2}(P_{n-5}P_{n-2} - P_{n-3}P_{n-4}) + P_{n-1}(-P_{n-5}P_{n-3} + P_{n-4}^2) + P_{n-3}(P_{n-3}^2 - P_{n-2}P_{n-4}) \\ &= 1 \end{aligned}$$

Since $m_i \geq 0$ $(i = 1, 2, \ldots, 9)$, we have

$$m_1 = e_3\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_2\left(P_{n-3}P_{n-5} - P_{n-4}^2\right) + e_1\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0$$

(6.11)

$$m_2 = e_1\left(P_{n-1}P_{n-5} - P_{n-3}^2\right) + e_3\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) + e_2\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0 \tag{6.12}$$

$$m_3 = e_3\left(P_{n-1}P_{n-3} - P_{n-2}^2\right) + e_2\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_1\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) \geq 0 \tag{6.13}$$

$$m_4 = e_6\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_5\left(P_{n-3}P_{n-5} - P_{n-4}^2\right) + e_4\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0 \tag{6.14}$$

$$m_5 = e_4\left(P_{n-1}P_{n-5} - P_{n-3}^2\right) + e_6\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) + e_5\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0 \tag{6.15}$$

$$m_6 = e_6\left(P_{n-1}P_{n-3} - P_{n-2}^2\right) + e_5\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_4\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) \geq 0 \tag{6.16}$$

$$m_7 = e_9\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_8\left(P_{n-3}P_{n-5} - P_{n-4}^2\right) + e_7\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0 \tag{6.17}$$

$$m_8 = e_7\left(P_{n-1}P_{n-5} - P_{n-3}^2\right) + e_9\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) + e_8\left(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}\right) \geq 0 \tag{6.18}$$

$$m_9 = e_9\left(P_{n-1}P_{n-3} - P_{n-2}^2\right) + e_8\left(P_{n-2}P_{n-4} - P_{n-3}^2\right) + e_7\left(P_{n-1}P_{n-4} - P_{n-2}P_{n-3}\right) \geq 0 \tag{6.19}$$

From (6.11), we have

$$e_3P_{n-2}P_{n-4} + e_2P_{n-3}P_{n-5} + e_1P_{n-2}P_{n-5} \geq e_3P_{n-3}^2 + e_2P_{n-4}^2 + e_1P_{n-3}P_{n-4} \tag{6.20}$$

From (6.12), we have

$$e_1P_{n-1}P_{n-5} + e_3P_{n-1}P_{n-4} + e_2P_{n-2}P_{n-5} \geq e_1P_{n-3}^2 + e_3P_{n-2}P_{n-3} + e_2P_{n-3}P_{n-4} \tag{6.21}$$

From (6.22), we have

$$e_3P_{n-1}P_{n-3} + e_2P_{n-2}P_{n-4} + e_1P_{n-1}P_{n-4} \geq e_3P_{n-2}^2 + e_2P_{n-3}^2 + e_1P_{n-2}P_{n-3}. \tag{6.22}$$

Dividing both sides by $e_1P_{n-3}P_{n-4}$ $(> 0)$ of (6.20), $e_1P_{n-3}^2$ $(> 0)$ of (6.21) and $e_1P_{n-2}P_{n-3}$ $(> 0)$ of (6.22), we have

$$\frac{e_3}{e_1}(P_{n-2}P_{n-4} - P_{n-3}^2) \geq \frac{e_2}{e_1}(P_{n-4}^2 - P_{n-3}P_{n-5}) + (P_{n-3}P_{n-4} - P_{n-2}P_{n-5}) \tag{6.23}$$

$$\frac{e_3}{e_1}(P_{n-2}P_{n-3} - P_{n-1}P_{n-4}) \leq \frac{e_2}{e_1}(P_{n-2}P_{n-5} - P_{n-3}P_{n-4}) + (P_{n-1}P_{n-5} - P_{n-3}^2) \tag{6.24}$$

$$\frac{e_3}{e_1}(P_{n-1}P_{n-3} - P_{n-2}^2) \geq \frac{e_2}{e_1}(P_{n-3}^2 - P_{n-3}P_{n-4}) + (P_{n-2}P_{n-3} - P_{n-1}P_{n-4}) \tag{6.25}$$

Let $a = (P_{n-2}P_{n-4} - P_{n-3}^2)$, $b = (P_{n-2}P_{n-3} - P_{n-1}P_{n-4})$, $c = (P_{n-1}P_{n-3} - P_{n-2}^2)$.

Now $3^3 = 27$ cases arise for $a >=< 0$, $b >=< 0$, $c >=< 0$.

**Case 1.** When $a > 0$, $b > 0$, $c > 0$. Then from (6.23), we have

$$\frac{e_3}{e_1} \geq v, \text{ where } v = \frac{e_2}{e_1}\left(\frac{P_{n-4}^2 - P_{n-3}P_{n-5}}{P_{n-2}P_{n-4} - P_{n-3}^2}\right) + \frac{P_{n-3}P_{n-4} - P_{n-2}P_{n-5}}{P_{n-2}P_{n-4} - P_{n-3}^2} \tag{6.26}$$

From (6.24), we have

$$\frac{e_3}{e_1} \leq y, \text{ where } y = \frac{e_2}{e_1}\left(\frac{P_{n-2}P_{n-5} - P_{n-3}P_{n-4}}{P_{n-2}P_{n-3} - P_{n-1}P_{n-4}}\right) + \frac{P_{n-1}P_{n-5} - P_{n-3}^2}{P_{n-2}P_{n-3} - P_{n-1}P_{n-4}} \tag{6.27}$$

From (6.25), we have

$$\frac{e_3}{e_1} \geq z, \text{ where } z = \frac{e_2}{e_1}\left(\frac{P_{n-3}^2 - P_{n-3}P_{n-4}}{P_{n-1}P_{n-3} - P_{n-2}^2}\right) + \frac{P_{n-2}P_{n-3} - P_{n-1}P_{n-4}}{P_{n-1}P_{n-3} - P_{n-2}^2}. \tag{6.28}$$

From (6.26) and (6.27), we have

$$\frac{e_1}{e_2} \geq \min\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\}, \text{using (6.10).} \tag{6.29}$$

From (6.27) and (6.28), we have

$$\frac{e_1}{e_2} \leq \max\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\}, \text{using (6.10).} \tag{6.30}$$

From (6.29) and (6.30), we have

$$\min\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\} \leq \frac{e_1}{e_2} \leq \max\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\}. \tag{6.31}$$

Similarly, we have

$$\min\left\{\frac{P_{n-1}}{P_{n-3}}, \frac{P_{n-2}}{P_{n-4}}, \frac{P_{n-3}}{P_{n-5}}\right\} \leq \frac{e_2}{e_3} \leq \max\left\{\frac{P_{n-1}}{P_{n-3}}, \frac{P_{n-2}}{P_{n-4}}, \frac{P_{n-3}}{P_{n-5}}\right\}$$

and

$$\min\left\{\frac{P_{n-2}}{P_{n-3}},\frac{P_{n-3}}{P_{n-4}},\frac{P_{n-4}}{P_{n-5}}\right\}\leq\frac{e_1}{e_3}\leq\max\left\{\frac{P_{n-2}}{P_{n-3}},\frac{P_{n-3}}{P_{n-4}},\frac{P_{n-4}}{P_{n-5}}\right\}.$$

**Case 2.** When $a=0$, $b>0$, $c>0$. From (6.23), we have

$$\frac{e_1}{e_2}\geq\min\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\},\text{ since } a=0. \tag{6.32}$$

From (6.24) and (6.25), we have

$$\frac{e_1}{e_2}\leq\max\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\},\text{using (6.10) and } a=0. \tag{6.33}$$

From (6.32) and (6.33), we have

$$\min\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\}\leq\frac{e_1}{e_2}\leq\max\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\}. \tag{6.34}$$

**Case 2.** When $a<0$, $b<0$, $c<0$, then from

$$\frac{e_3}{e_1}\leq v,\text{ where } v=\frac{e_2}{e_1}\left(\frac{P_{n-4}^2-P_{n-3}P_{n-5}}{P_{n-2}P_{n-4}-P_{n-3}^2}\right)+\frac{P_{n-3}P_{n-4}-P_{n-2}P_{n-5}}{P_{n-2}P_{n-4}-P_{n-3}^2}. \tag{6.35}$$

From (6.24), we have

$$\frac{e_3}{e_1}\geq y,\text{ where } y=\frac{e_2}{e_1}\left(\frac{P_{n-2}P_{n-5}-P_{n-3}P_{n-4}}{P_{n-2}P_{n-3}-P_{n-1}P_{n-4}}\right)+\frac{P_{n-1}P_{n-5}-P_{n-3}^2}{P_{n-2}P_{n-3}-P_{n-1}P_{n-4}}. \tag{6.36}$$

From (6.25), we have

$$\frac{e_3}{e_1}\geq z,\text{ where } z=\frac{e_2}{e_1}\left(\frac{P_{n-3}^2-P_{n-3}P_{n-4}}{P_{n-1}P_{n-3}-P_{n-2}^2}\right)+\frac{P_{n-2}P_{n-3}-P_{n-1}P_{n-4}}{P_{n-1}P_{n-3}-P_{n-2}^2}. \tag{6.37}$$

From (6.35) and (6.36), we have

$$\frac{e_1}{e_2}\leq\max\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\},\text{using (6.10)}. \tag{6.38}$$

From (6.36) and (6.37), we have

$$\frac{e_1}{e_2}\geq\min\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\},\text{using (6.10)}. \tag{6.39}$$

From (6.38) and (6.39), we have

$$\min\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\}\leq\frac{e_1}{e_2}\leq\max\left\{\frac{P_{n-2}}{P_{n-1}},\frac{P_{n-3}}{P_{n-2}},\frac{P_{n-4}}{P_{n-3}}\right\}. \tag{6.40}$$

Similarly, we have

$$\min\left\{\frac{P_{n-1}}{P_{n-3}},\frac{P_{n-2}}{P_{n-4}},\frac{P_{n-3}}{P_{n-5}}\right\}\leq\frac{e_2}{e_3}\leq\max\left\{\frac{P_{n-1}}{P_{n-3}},\frac{P_{n-2}}{P_{n-4}},\frac{P_{n-3}}{P_{n-5}}\right\}$$

and

$$\min\left\{\frac{P_{n-2}}{P_{n-3}}, \frac{P_{n-3}}{P_{n-4}}, \frac{P_{n-4}}{P_{n-5}}\right\} \leq \frac{e_1}{e_3} \leq \max\left\{\frac{P_{n-2}}{P_{n-3}}, \frac{P_{n-3}}{P_{n-4}}, \frac{P_{n-4}}{P_{n-5}}\right\}.$$

Similarly it can be proved for the rest cases.

Hence, we have

$$\min\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\} \leq \frac{e_1}{e_2} \leq \max\left\{\frac{P_{n-2}}{P_{n-1}}, \frac{P_{n-3}}{P_{n-2}}, \frac{P_{n-4}}{P_{n-3}}\right\}$$

$$\min\left\{\frac{P_{n-1}}{P_{n-3}}, \frac{P_{n-2}}{P_{n-4}}, \frac{P_{n-3}}{P_{n-5}}\right\} \leq \frac{e_2}{e_3} \leq \max\left\{\frac{P_{n-1}}{P_{n-3}}, \frac{P_{n-2}}{P_{n-4}}, \frac{P_{n-3}}{P_{n-5}}\right\} \tag{6.41}$$

$$\min\left\{\frac{P_{n-2}}{P_{n-3}}, \frac{P_{n-3}}{P_{n-4}}, \frac{P_{n-4}}{P_{n-5}}\right\} \leq \frac{e_1}{e_3} \leq \max\left\{\frac{P_{n-2}}{P_{n-3}}, \frac{P_{n-3}}{P_{n-4}}, \frac{P_{n-4}}{P_{n-5}}\right\}. \tag{6.42}$$

Therefore, for large value of $n$ we arrive at

$$\frac{e_1}{e_2} \approx \frac{1}{\alpha}, \frac{e_2}{e_3} \approx \alpha^2 \text{ and } \frac{e_1}{e_3} \approx \alpha, \text{ where } \alpha = 1.32471795724. \tag{6.43}$$

Similarly, we have

$$\frac{e_4}{e_5} \approx \frac{1}{\alpha}, \frac{e_5}{e_6} \approx \alpha^2 \text{ and } \frac{e_4}{e_6} \approx \alpha \tag{6.44}$$

and

$$\frac{e_7}{e_8} \approx \frac{1}{\alpha}, \frac{e_8}{e_9} \approx \alpha^2 \text{ and } \frac{e_7}{e_9} \approx \alpha. \tag{6.45}$$

**Remark 6.1** *The relationships between the code matrix elements can also be given as follows:*

$$\begin{aligned} E &= M \times A^n = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \begin{pmatrix} P_{n-2} & P_{n-1} & P_{n-3} \\ P_{n-3} & P_{n-2} & P_{n-4} \\ P_{n-4} & P_{n-3} & P_{n-5} \end{pmatrix} \\ &= \begin{pmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} \lim_{n\longrightarrow\infty} \frac{e_1}{e_2} &= \lim_{n\longrightarrow\infty} \frac{m_1P_{n-2} + m_2P_{n-3} + m_3P_{n-4}}{m_1P_{n-1} + m_2P_{n-2} + m_3P_{n-3}} = \frac{1}{\alpha}, \\ \lim_{n\longrightarrow\infty} \frac{e_2}{e_3} &= \lim_{n\longrightarrow\infty} \frac{m_1P_{n-1} + m_2P_{n-2} + m_3P_{n-3}}{m_1P_{n-3} + m_2P_{n-4} + m_3P_{n-5}} = \alpha^2, \\ \lim_{n\longrightarrow\infty} \frac{e_1}{e_3} &= \lim_{n\longrightarrow\infty} \frac{m_1P_{n-2} + m_2P_{n-3} + m_3P_{n-4}}{m_1P_{n-3} + m_2P_{n-4} + m_3P_{n-5}} = \alpha. \end{aligned}$$

*Similarly, we have*

$$\lim_{n\longrightarrow\infty}\frac{e_4}{e_5}=\frac{1}{\alpha},\ \lim_{n\longrightarrow\infty}\frac{e_5}{e_6}=\alpha^2\ \textit{and}\ \lim_{n\longrightarrow\infty}\frac{e_4}{e_6}=\alpha$$

*and*

$$\lim_{n\longrightarrow\infty}\frac{e_7}{e_8}=\frac{1}{\alpha},\ \lim_{n\longrightarrow\infty}\frac{e_8}{e_9}=\alpha^2\ \textit{and}\ \lim_{n\longrightarrow\infty}\frac{e_7}{e_9}=\alpha.$$

### 6.2.2 Error Detection and Correction

If we have single error in the code matrix $E$, it is clear that there are nine variants of single error in the code matrix $E$:

$$(1)\begin{pmatrix} x_1 & e_2 & e_3\\ e_4 & e_5 & e_6\\ e_7 & e_8 & e_9\end{pmatrix},\ (2)\begin{pmatrix} e_1 & x_2 & e_3\\ e_4 & e_5 & e_6\\ e_7 & e_8 & e_9\end{pmatrix},\ (3)\begin{pmatrix} e_1 & e_2 & x_3\\ e_4 & e_5 & e_6\\ e_7 & e_8 & e_9\end{pmatrix},$$

$$(4)\begin{pmatrix} e_1 & e_2 & e_3\\ x_4 & e_5 & e_6\\ e_7 & e_8 & e_9\end{pmatrix},\ (5)\begin{pmatrix} e_1 & e_2 & e_3\\ e_4 & x_5 & e_6\\ e_7 & e_8 & e_9\end{pmatrix},\ (6)\begin{pmatrix} e_1 & e_2 & e_3\\ e_4 & e_5 & x_6\\ e_7 & e_8 & e_9\end{pmatrix}$$

$$(7)\begin{pmatrix} e_1 & e_2 & e_3\\ e_4 & e_5 & e_6\\ x_7 & e_8 & e_9\end{pmatrix},\ (8)\begin{pmatrix} e_1 & e_2 & e_3\\ e_4 & e_5 & e_6\\ e_7 & x_8 & e_9\end{pmatrix},\ (9)\begin{pmatrix} e_1 & e_2 & e_3\\ e_4 & e_5 & e_6\\ e_7 & e_8 & x_9\end{pmatrix},$$

where $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$ are possible destroyed elements. For checking the hypotheses $(1)-(9)$, we write the following algebraic equations based on relations (6.6):

$$x_1(e_5e_9-e_6e_8)+e_2(e_6e_7-e_4e_9)+e_3(e_4e_8-e_5e_7)=detP, \tag{6.46}$$

$$e_1(e_5e_9-e_6e_8)+x_2(e_6e_7-e_4e_9)+e_3(e_4e_8-e_5e_7)=detP, \tag{6.47}$$

$$e_1(e_5e_9-e_6e_8)+e_2(e_6e_7-e_4e_9)+x_3(e_4e_8-e_5e_7)=detP, \tag{6.48}$$

$$x_4(e_3e_8-e_2e_9)+e_5(e_1e_9-e_3e_7)+e_6(e_2e_7-e_1e_8)=detP, \tag{6.49}$$

$$e_4(e_3e_8-e_2e_9)+x_5(e_1e_9-e_3e_7)+e_6(e_2e_7-e_1e_8)=detP, \tag{6.50}$$

$$e_4(e_3e_8-e_2e_9)+e_5(e_1e_9-e_3e_7)+x_6(e_2e_7-e_1e_8)=detP, \tag{6.51}$$

$$x_7(e_2e_6-e_3e_5)+e_8(e_3e_4-e_1e_6)+e_9(e_1e_5-e_2e_4)=detP, \tag{6.52}$$

$$e_7(e_2e_6-e_3e_5)+x_8(e_3e_4-e_1e_6)+e_9(e_1e_5-e_2e_4)=detP, \tag{6.53}$$

$$e_7(e_2e_6 - e_3e_5) + e_8(e_3e_4 - e_1e_6) + x_9(e_1e_5 - e_2e_4) = detP. \tag{6.54}$$

It follows from (15.1)-(6.54) nine variants of calculations of possible single errors:

$$x_1 = \frac{detP - e_2(e_6e_7 - e_4e_9) - e_3(e_4e_8 - e_5e_7)}{e_5e_9 - e_6e_8}, \tag{6.55}$$

$$x_2 = \frac{detP - e_1(e_5e_9 - e_6e_8) - e_3(e_4e_8 - e_5e_7)}{e_6e_7 - e_4e_9}, \tag{6.56}$$

$$x_3 = \frac{detP - e_1(e_5e_9 - e_6e_8) - e_2(e_6e_7 - e_4e_9)}{e_4e_8 - e_5e_7}, \tag{6.57}$$

$$x_4 = \frac{detP - e_5(e_1e_9 - e_3e_7) - e_6(e_2e_7 - e_1e_8)}{e_3e_8 - e_2e_9}, \tag{6.58}$$

$$x_5 = \frac{detP - e_4(e_3e_8 - e_2e_9) - e_6(e_2e_7 - e_1e_8)}{e_1e_9 - e_3e_7}, \tag{6.59}$$

$$x_6 = \frac{detP - e_4(e_3e_8 - e_2e_9) - e_5(e_1e_9 - e_3e_7)}{e_2e_7 - e_1e_8}, \tag{6.60}$$

$$x_7 = \frac{detP - e_8(e_3e_4 - e_1e_6) - e_9(e_1e_5 - e_2e_4)}{e_2e_6 - e_3e_5}, \tag{6.61}$$

$$x_8 = \frac{detP - e_7(e_2e_6 - e_3e_5) - e_9(e_1e_5 - e_2e_4)}{e_3e_4 - e_1e_6}, \tag{6.62}$$

$$x_9 = \frac{detP - e_7(e_2e_6 - e_3e_5) - e_8(e_3e_4 - e_1e_6)}{e_1e_5 - e_2e_4}. \tag{6.63}$$

The formulas (6.55)-(6.63) give nine possible variants of single error but we have to choose the correct variant only among the cases of the integer solutions $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$; which satisfies relations (6.43), (6.44) and (6.45). If the calculations by the formulas (6.55)-(6.63) do not give an integer result, we have to conclude that our hypothesis about single error is incorrect or we have more than single error in the checking element $\det P$. For the latter case, we use the approximate equalities (6.43), (6.44) and (6.45) for checking a correctness of the code matrix $E$.

By analogy, we check all hypotheses of double errors in the code matrix $E$. As example, let us consider the following case of double errors in the code matrix $E$:

$$\begin{pmatrix} x & y & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{pmatrix}. \tag{6.64}$$

Using relation (6.6), we write the algebraic equation for matrix (6.64)

$$x(e_5e_9 - e_6e_8) + y(e_6e_7 - e_4e_9) = e_3(e_5e_7 - e_4e_8) + detP. \tag{6.65}$$

According to relation (6.43) there is the following relation between $x$ and $y$:

$$x \approx \frac{1}{\alpha} y. \tag{6.66}$$

Equation (6.65) is "Diophantine". As the "Diophantine" equation (6.65) has many solutions, we have to choose such solutions $x, y$, which satisfy relation (6.66).

It is clear that there are $\begin{pmatrix} 9 \\ 2 \end{pmatrix} = 36$ variants of double errors in the code matrix $E$ and by using similar approach we correct all double errors in the code matrix $E$. Hence there are

$$\begin{pmatrix} 9 \\ 1 \end{pmatrix} + \begin{pmatrix} 9 \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} 9 \\ 8 \end{pmatrix} + \begin{pmatrix} 9 \\ 9 \end{pmatrix} = 511$$

cases of errors in the code matrix $E$.

Similarly, we show by using this approach that there is a possibility to correct all possible triple-fold, four-fold, . . . , eight-fold errors in the code matrix $E$.

Hence the possibility to correct eight cases of this method is $\frac{510}{511} = 0,9980 = 99,80\%$ since the nine-fold error of the code matrix is not correctable.

# CHAPTER 7

# AN APPLICATION OF THIRD ORDER JACOBSTHAL NUMBERS TO CRYPTOGRAPHY

Today, many different encryptions have been developed for information security. Shift and Affine encryption, Hill encryption, RSA, ElGamal are some of them, see [78].
Private key and public key have an important place in cryptosystems. Because cryptosystems have been attempted to be strengthened with key exchange algorithms based on private and public keys, and significant research has been conducted in this field. ElGamal technique is one of them. T. ElGamal introduced a key exchange technique based on private and public keys in 1984. This technique is closely related to the Deffie-Hellman technique [78,79].
In this chapter, we propose a new encryption-decryption algorithm using the third order Jacobsthal **J** matrix and ElGamal technique, the algorithm depends on dividing the message matrix into the block matrices each is of size $3 \times 3$. We use different numbered alphabet for each message, so we get a more reliable encryption method. The alphabet is determined by the number of block matrices of the message matrix and $k$ number.

## 7.1 KEY EXCHANGE ALGORITHM (ELGAMAL TECHNIQUE)

Let us remind you again of the ElGamal technique, which will be used in the algorithm we will create in this section.

1. $p$ is prime.

2. $D$ is a private key, where $1 < D < \phi(p)$.

3. Select a primitive root of $p$, say $\alpha$.

4. Assign $E_1 = \alpha$ and $E_2 \equiv E_1^D (\mathrm{mod}\, p)$.

5. Make $(p, E_1, E_2)$ as public key and keep $D$ as secret key.

Let's say that Bob and Alice wish to exchange keys. Alice produces signature $k$ using the public key $(p, E_1, E_2)$ mentioned above by computing $k = E_1^e (\mathrm{mod}\, p)$, where $e$ is a random integer with $1 < e < \phi(p)$, and secret key $\lambda = E_2^e (\mathrm{mod}\, p)$. As a result, Alice can send an encrypted message $(k, C)$ using their secret key $\lambda$ if she has access to Bob's public key .

Bob discovers the secret key after getting $(k, C)$ from Alice by using their secret key $D$ as follows:

$$\lambda = k^D = (E_1^e)^D = (E_1^D)^e \equiv (E_2)^e (\mathrm{mod}\, p).$$

As a result, Bob successfully finds the secret key $\lambda$ and uses it to decrypt the ciphertext $C$ and obtain the original plaintext $P$.

## 7.2 THE ENCRYPTION AND DECRYPTION ALGORITHMS

At first, we put our message in a matrix $M$ of size $3m \times 3m$ leaving space between two words. Dividing the message square matrix $M$ of size $3m \times 3m$ into the matrices, named $B_i$ of size $3 \times 3$. $(1 \leq i \leq m^2)$

$$B_i = \begin{pmatrix} b_1^i & b_2^i & b_3^i \\ b_4^i & b_5^i & b_6^i \\ b_7^i & b_8^i & b_9^i \end{pmatrix}, E_i = \begin{pmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{pmatrix}, \mathbf{J}^\lambda = \begin{pmatrix} j_1 & j_2 & j_3 \\ j_4 & j_5 & j_6 \\ j_7 & j_8 & j_9 \end{pmatrix}.$$

**Encryption Algorithm**

The number of the block matrices is denoted by $s$. According to $s$ and $k$, we choose the number $n$ as follows. Suppose that $[|k/s|] = y$,

$$n = \begin{cases} 5 & , \quad y \leq 1 \\ y & , \quad y > 1 \end{cases}$$

.

We will use the following table according to $(\mathrm{mod}\, 41)$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ |
| $n$ | $n+1$ | $n+2$ | $n+3$ | $n+4$ | $n+5$ | $n+6$ | $n+7$ | $n+8$ |
| $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ |
| $n+9$ | $n+10$ | $n+11$ | $n+12$ | $n+13$ | $n+14$ | $n+15$ | $n+16$ | $n+17$ |
| $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 |
| $n+18$ | $n+19$ | $n+20$ | $n+21$ | $n+22$ | $n+23$ | $n+24$ | $n+25$ | $n+26$ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $n+27$ | $n+28$ | $n+29$ | $n+30$ | $n+31$ | $n+32$ | $n+33$ | $n+34$ | $n+35$ |
| | . | , | ! | ? | | | | |
| $n+36$ | $n+37$ | $n+38$ | $n+39$ | $n+40$ | | | | |

1. Choose $n$
2. Determine $b_j^i$ $(1 \leq j \leq 9)$
3. Compute $\det(B_i) = d_i$
4. Construct $C = [b_k^i, d_i]_{k \in \{1,2,3,5,6,7,8,9\}}$
5. Transmit $(k, n, C)$

**Decryption Algorithm**

1. Compute $\lambda$
2. Compute $\mathbf{J}^\lambda$
3. Compute

$$j_1 b_1^i + j_3 b_7^i = e_1^i \quad j_1 b_2^i + j_2 b_5^i + j_3 b_8^i = e_2^i \quad j_1 b_3^i + j_2 b_6^i + j_3 b_9^i = e_3^i$$
$$j_4 b_1^i + j_6 b_7^i = e_4^i \quad j_4 b_2^i + j_5 b_5^i + j_6 b_8^i = e_5^i \quad j_4 b_3^i + j_5 b_6^i + j_6 b_9^i = e_6^i$$
$$j_7 b_1^i + j_9 b_7^i = e_7^i \quad j_7 b_2^i + j_8 b_5^i + j_9 b_8^i = e_8^i \quad j_7 b_3^i + j_8 b_6^i + j_9 b_9^i = e_9^i$$

4. Solve $2^\lambda . d_i = (e_1^i + j_2 x_i)(e_5^i e_9^i - e_6^i e_8^i) + (e_4^i + j_5 x_i)(e_3^i e_8^i - e_2^i e_9^i) + (e_7^i + j_8 x_i)(e_2^i e_6^i - e_3^i e_5^i)$
5. Substitute for $x_i = b_4^i$
6. Construct $B_i$

7. Construct $M$

**Example 7.1** *(Public key calculation) Consider* $p = 41$ *and Bob's private key is* $D = 23$. *Bob choose primitive root of* $p$, *say* $\alpha = 17$. *Bob assign* $E_1 = \alpha = 17$ *and compute* $E_2 \equiv E_1^D (\mathrm{mod}\, p) \equiv 17^{23} (\mathrm{mod}\, 41) = 7$. *Thus, Bob's public key* $pk(p, E_1, E_2)$ *is* $pk(41, 17, 7)$ *and secret key is* $D = 23$.
*For encryption, choose* $e = 18$ *such that* $1 < e < \phi(p)$. *Calculating signature* $k = E_1^e \equiv 17^{18} (\mathrm{mod}\, 41) = 20$.

**Example 7.2** *Consider the message "HELLO BOB CODING DECODING ALGORITHM."*

$$M = \begin{pmatrix} H & E & L & L & O & \\ B & O & B & & C & O \\ D & I & N & G & & D \\ E & C & O & D & I & N \\ G & & A & L & G & O \\ R & I & T & H & M & . \end{pmatrix}$$

***Encryption***

$m = 2$ *and* $s = 4$

$$B_1 = \begin{pmatrix} H & E & L \\ B & O & B \\ D & I & N \end{pmatrix}, B_2 = \begin{pmatrix} L & O & \\ & C & O \\ G & & D \end{pmatrix},$$

$$B_3 = \begin{pmatrix} E & C & O \\ G & & A \\ R & I & T \end{pmatrix}, B_4 = \begin{pmatrix} D & I & N \\ L & G & O \\ H & M & . \end{pmatrix}$$

1. $[|20/4|] = 5 \Longrightarrow n = 5$

2. $B_1 = \begin{pmatrix} 12 & 9 & 16 \\ 6 & 19 & 6 \\ 8 & 13 & 18 \end{pmatrix}$, $B_2 = \begin{pmatrix} 16 & 19 & 0 \\ 0 & 7 & 19 \\ 11 & 0 & 8 \end{pmatrix}$, $B_3 = \begin{pmatrix} 9 & 7 & 19 \\ 11 & 0 & 5 \\ 22 & 13 & 24 \end{pmatrix}$, $B_4 = \begin{pmatrix} 8 & 13 & 18 \\ 16 & 11 & 19 \\ 12 & 17 & 1 \end{pmatrix}$

3. $d_1 = 1444$, $d_2 = 4867$, $d_3 = 1054$, $d_4 = 2780$

4. $C = \begin{pmatrix} 12 & 9 & 16 & 19 & 6 & 8 & 13 & 18 & 1444 \\ 16 & 19 & 0 & 7 & 19 & 11 & 0 & 8 & 4867 \\ 9 & 7 & 19 & 0 & 5 & 22 & 13 & 24 & 1054 \\ 8 & 13 & 18 & 11 & 19 & 12 & 17 & 1 & 2780 \end{pmatrix}$

5. $(20, 5, \begin{pmatrix} 12 & 9 & 16 & 19 & 6 & 8 & 13 & 18 & 1444 \\ 16 & 19 & 0 & 7 & 19 & 11 & 0 & 8 & 4867 \\ 9 & 7 & 19 & 0 & 5 & 22 & 13 & 24 & 1054 \\ 8 & 13 & 18 & 11 & 19 & 12 & 17 & 1 & 2780 \end{pmatrix})$

***Decryption***

1. $\lambda = k^D = 20^{23} (\mathrm{mod}\, 41) = 5$

2. $\mathbf{J}^\lambda = \begin{pmatrix} 18 & 19 & 18 \\ 9 & 9 & 10 \\ 5 & 4 & 4 \end{pmatrix}$

3. *For* $B_1$

$$e_1^1 = 360 \quad e_2^1 = 757 \quad e_3^1 = 726$$
$$e_4^1 = 188 \quad e_5^1 = 382 \quad e_6^1 = 378$$
$$e_7^1 = 92 \quad e_8^1 = 173 \quad e_9^1 = 176$$

4. $2^5.d_1 = (e_1^1 + j_2 x_1)(e_5^1 e_9^1 - e_6^1 e_8^1) + (e_4^1 + j_5 x_1)(e_3^1 e_8^1 - e_2^1 e_9^1) + (e_7^1 + j_8 x_1)(e_2^1 e_6^1 - e_3^1 e_5^1)$

$32.1444 = (360 + 19x_1).1838 + (188 + 9x_1).(-7634) + (92 + 4x_1).8814$

$\Longrightarrow x_1 = 6$

5. $x_1 = b_4^1 = 6$

6. $B_1 = \begin{pmatrix} 12 & 9 & 16 \\ 6 & 19 & 6 \\ 8 & 13 & 18 \end{pmatrix}$.

*The same process steps are done for the* $B_2, B_3, B_4$.

7. $M = \begin{pmatrix} 12 & 9 & 16 & 16 & 19 & 0 \\ 6 & 19 & 6 & 0 & 7 & 19 \\ 8 & 13 & 18 & 11 & 0 & 8 \\ 9 & 7 & 19 & 8 & 13 & 18 \\ 11 & 0 & 5 & 16 & 11 & 19 \\ 22 & 13 & 24 & 12 & 17 & 1 \end{pmatrix} = \begin{pmatrix} H & E & L & L & O & \\ B & O & B & & C & O \\ D & I & N & G & & D \\ E & C & O & D & I & N \\ G & & A & L & G & O \\ R & I & T & H & M & . \end{pmatrix}$

# CHAPTER 8

## CRYPTOGRAPHY USING $\lambda$-STEP PELL NUMBERS WITH AFFINE-HILL CIPHER

Today, the widespread use of computers and the emergence of the internet have necessitated the sending of financial and other sensitive information through public channels. This has initiated an intensive development of mathematical cryptography, both symmetric and public key. In sophisticated cryptosystems, the public and private keys are crucial. Important research on the public key and the private key have been undertaken in order to eliminate insecure situations. One of them is its application to linear Diophantine equations. Lin Chang and Lie presented Diophantine equation-based cryptography in 1995. Hary Yosh suggested cryptography based on nonlinear Diophantine equations and specific operators whose security is dependent on the difficulty of finding a solution to the equation in [80]. An application of linear Diophantine equations to cryptography was given in [7] by Kameswari, P. A., and et al. For more information, see [81, 82]. Furthermore, the Hill cipher [78, 83, 84] is one of the important encryption methods developed by mathematician Lester Hill in 1929, see [85-88] for Hill's Cipher.

**Remark 8.1** *In this study, we will take the smallest positive integer with respect to* $(\mathrm{mod}\, 41)$ *of any given number. For example* $\frac{19}{645}(\mathrm{mod}\, 41) = 2$. *Because*

$$645x = 19(\mathrm{mod}\, 41)$$

$$\Rightarrow \quad x = \frac{19 + 41n}{645}$$
$$\Rightarrow \quad n = 3,\ x = 2.$$

In this chapter, we develop a public key cryptosystem using key exchange based on $n$-variable linear Diophantine equations and the Affine-Hill Cipher with $\lambda$-step Pell numbers.

## 8.1 KEY EXCHANGE ALGORITHM [7] (SOLUTION OF LINEAR DIOPHANTINE EQUATIONS WITH $n$-VARIABLES TECHNIQUE)

1. Sender generates public key.

   - A linear Diophantine equation $g(x_1, x_2, \ldots, x_n)$ is considered by the sender.
   - The sender generates the operator on the Diophantine equation given as for $T_i = T_{[p_i,q_i]}(g) = (g + p_i)q_i$, where $p_i, q_i$ parameters and $p_i \in \mathbb{R}$, $q_i > 0$ $\forall i = 1, 2, \ldots, m$.
   - The sender generates the public key by taking key as $T = T_m \circ T_{m-1} \circ \cdots \circ T_1$ and computes $T(g)$ as

   $$\begin{aligned} T(g) &= T_m.T_{m-1}.\cdots.T_1(g(x_1, x_2, \ldots, x_n)) \\ &= (((g(x_1, x_2, \ldots, x_n) + p_1)q_1 + p_2)q_2 \ldots + p_m)q_m \\ &= h(x_1, x_2, \ldots, x_n). \end{aligned}$$

   - The sender makes the Diophantine equations $h(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ public.

2. Recipient generates public key and private key.

   - A linear Diophantine equation $f(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ in $n$ variables for $n > 2$ such that $\gcd(a_1, a_2, \ldots, a_n)$ divides $b$ is considered by the sender.
   - The recipient selects a random solution $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the linear Diophantine equation $f(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$.
   - The recipient on receiving the public key Diophantine equations evaluates $h(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ evaluates $h(\alpha_1, \alpha_2, \ldots, \alpha_n) = k$, $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = \lambda$.
   - The recipient keeps the evaluated value $\lambda$ as secret key and makes $u$ public key.

3. The sender recovers the secret key.

- The sender recovers the secret key $\lambda$ from public key $k$ by applying the inverse of operators $T_i$ where for $T_i$ we have $T_i^{-1} = T_{[p_i,q_i]}^{-1}$ with $T_{[p_i,q_i]}^{h} = (h)\frac{1}{q_i} - p_i$.
- The sender from $T_i^{-1}$ the inverse of $T_i$ recovers $\lambda$ from $k$ by

  $(T_m \circ T_{m-1} \circ \cdots \circ T_1)^{-1}(u) = T_1^{-1} \circ T_2^{-1} \circ \ldots \circ T_{m-1}^{-1} \circ T_m^{-1}$.

4. The secret key $\lambda$ evaluated by both sender and receiver is used as the key for key exchange.

## 8.2 ALGORITHMS

Encryption Algorithm:

1. $X$ chooses Diophantine equation $g$ and generates $h$
2. $X$ recovers the secret key $\lambda$
3. Key Matrix: $\boldsymbol{P}_\lambda^k \longrightarrow K$, where $\boldsymbol{P}_\lambda^k$ is multinacci matrix of order $\lambda \times \lambda$
4. Encryption: $Enc(M) : C_i \equiv (M_i K + B)(\mathrm{mod}\, p)$
5. Transmit $(k, C)$ to $Y$.

Decryption Algorithm:
$Y$, after receiving $(k, C)$.

1. Key Matrix: $\boldsymbol{P}_\lambda^k \longrightarrow K$
2. Decryption: $Dec(C) : M_i \equiv (C_i - B)K^{-1}(\mathrm{mod}\, p)$

Note that $B$ is an $(1 \times \lambda)$ row vector called shifting vector.
Suppose $X$ wants to send message to $Y$. After calculating key matrix $K$ he will encrypt plaintext $M$ with $K$ using proposed algorithm above.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 | 1 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ! | ? | | |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

**Example 8.1** *(Public key calculation) X chooses a linear Diophantine equation* $g(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 - 1$ *and constructs the public key* $h(x_1, x_2, x_3, x_4)$ *using the operators* $T_1 = T_{[1,2]}$, $T_2 = T_{[-4,3]}$, $T_3 = T_{[-5,1]}$

$$\begin{aligned} h(x_1, x_2, x_3, x_4) &= T_3 \circ T_2 \circ T_1(g(x_1, x_2, x_3, x_4)) \\ &= T_3 \circ T_2 \circ T_1(x_1 + x_2 + x_3 + x_4 - 1) \\ &= T_3 \circ T_2(2x_1 + 2x_2 + 2x_3 + 2x_4) \\ &= T_3((2x_1 + 2x_2 + 2x_3 + 2x_4 - 4).3) \\ &= T_3(6x_1 + 6x_2 + 6x_3 + 6x_4 - 12) \\ &= 6x_1 + 6x_2 + 6x_3 + 6x_4 - 17. \end{aligned}$$

*X makes*

$$\begin{cases} x_1 + x_2 + x_3 + x_4 - 1 \\ -6x_1 + 6x_2 + 6x_3 + 6x_4 - 17 \end{cases}$$

*public.*

*Y considers the linear Diophantine equation* $f(x_1, x_2, x_3, x_4) = x_1 + 3x_2 - 2x_3 + x_4 - 3$ *picks a solution* $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1, 1, 1, 1)$ *and keeps it private.*

*Y evaluates*

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 7 \\ g(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 3. \end{aligned}$$

*Y keeps* $\lambda = g(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 3$ *as secret key, makes* $k = h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 7$ *as public key.*

*X recovers secrete key* $\lambda$ *from the private key* $h(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ *by applying*

$$\begin{aligned} (T_3 \circ T_2 \circ T_1)^{-1}(k) &= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(7) \\ &= T_1^{-1} \circ T_2^{-1}(\frac{7}{1} + 5) \\ &= T_1^{-1} \circ T_2^{-1}(12) \\ &= T_1^{-1}(\frac{12}{3} + 4) \\ &= T_1^{-1}(8) \\ &= \frac{8}{2} - 1 \\ &= 3 \\ &= \lambda \end{aligned}$$

**Example 8.2** *(Encryption-Decryption) Suppose plaintext $M$ is $SECRET$, and shifting vector $B$ is $(25, 13, 17)$.*

**Solution 8.1** *For encryption, signature $k = 7$ and secret key $\lambda = 3$ construct the key matrix $K = \boldsymbol{P}_{\lambda}^{k} = \boldsymbol{P}_{3}^{7}$ using $\lambda = 3rd$ order generalized Pell matrix. Generalized Pell sequence for $\lambda = 3$ is given by*

| *Index* | ... | $-3$ | $-2$ | $-1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Pell numbers* | ... | $-1$ | 1 | 0 | 0 | 1 | 2 | 5 | 13 | 33 | 84 | 214 | 545 | ... |

*we have*

$$K = \begin{pmatrix} P_8 & P_7 + P_6 & P_7 \\ P_7 & P_6 + P_5 & P_6 \\ P_6 & P_5 + P_4 & P_5 \end{pmatrix} = \begin{pmatrix} 545 & 298 & 214 \\ 214 & 117 & 84 \\ 84 & 46 & 33 \end{pmatrix},$$

$$K(\text{mod}\,41) = \begin{pmatrix} 12 & 11 & 9 \\ 9 & 35 & 2 \\ 2 & 5 & 33 \end{pmatrix}.$$

*The plaintext $M = SECRET$ is divided into blocks each of size $\lambda$ and obtain numerical values*

$M_1 = (S\ E\ C) = (\ 18\ \ 4\ \ 2\ )$ *and* $M_2 = (R\ E\ T) = (\ 17\ \ 4\ \ 19\ )$.

*Encryption:* $C \equiv (MK + B)(\text{mod}\,41)$.

*Then we get*

$$C_1 = (M_1K + B) \equiv [(\ 18\ \ 4\ \ 2\ ) \begin{pmatrix} 12 & 11 & 9 \\ 9 & 35 & 2 \\ 2 & 5 & 33 \end{pmatrix} + (\ 25\ \ 13\ \ 17\ )](\text{mod}\,41)$$

$$\equiv \begin{pmatrix} 281 & 361 & 253 \end{pmatrix} (\text{mod}\,41)$$

$\equiv (\ 35\ \ 33\ \ 7\ ) \sim (9\ 7\ H)$,

*and*

$$C_2 = (M_2K + B) \equiv [(\ 17\ \ 4\ \ 19\ ) \begin{pmatrix} 12 & 11 & 9 \\ 9 & 35 & 2 \\ 2 & 5 & 33 \end{pmatrix} + \begin{pmatrix} 25 & 13 & 17 \end{pmatrix}](\text{mod}\,41)$$

$$\equiv \begin{pmatrix} 303 & 435 & 805 \end{pmatrix} (\text{mod}\,41)$$

$\equiv (\ 16\ \ 25\ \ 26\ ) \sim (Q\ Z\ 0)$. *Cipher-text* $C = (C_1C_2) = (97HQZ0)$ *and hence* $M$ : $SECRET \longrightarrow C : 97HQZ0$. *$X$ send this cipher-text $C$ to $Y$ along with her signature $k$.*

*Decryption: Receiving ciphertext $C$ along with signature $k$, $Y$ will calculate decryption key $K^{-1} = \boldsymbol{J}_{\lambda}^{-k} = \boldsymbol{J}_{3}^{-7}$ where $\lambda = 3$. Then we obtain*

$$K^{-1}(\text{mod}\,41) = \begin{pmatrix} \frac{1145}{10\,292} & -\frac{159}{5146} & -\frac{293}{10\,292} \\ -\frac{293}{10\,292} & \frac{189}{5146} & \frac{57}{10\,292} \\ -\frac{25}{10\,292} & -\frac{19}{5146} & \frac{321}{10\,292} \end{pmatrix} (\text{mod}\,41)$$

$$= \begin{pmatrix} 38 & 10 & 35 \\ 35 & 9 & 16 \\ 16 & 3 & 34 \end{pmatrix}$$

*and*

$$\begin{pmatrix} 12 & 11 & 9 \\ 9 & 35 & 2 \\ 2 & 5 & 33 \end{pmatrix} \times \begin{pmatrix} 38 & 10 & 35 \\ 35 & 9 & 16 \\ 16 & 3 & 34 \end{pmatrix} = \begin{pmatrix} 985 & 246 & 902 \\ 1599 & 411 & 943 \\ 779 & 164 & 1272 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (\text{mod}\,41).$$

*Decryption takes place as* $P_i \equiv (C_i - B)K^{-1}(\text{mod}\,41)$.

*Then*

$$M_1 = (C_1 - B)K^{-1} = [(\ 35 \quad 33 \quad 7\ ) - (\ 25 \quad 13 \quad 17\ )] \begin{pmatrix} 38 & 10 & 35 \\ 35 & 9 & 16 \\ 16 & 3 & 34 \end{pmatrix} (\text{mod}\,41)$$

$$\equiv \begin{pmatrix} 920 & 250 & 330 \end{pmatrix} (\text{mod}\,41) \equiv (\ 18 \quad 4 \quad 2\ ) \sim (S\ E\ C),$$

*and*

$$M_2 = (C_2 - B)K^{-1} = [(\ 16 \quad 25 \quad 26\ ) - (\ 25 \quad 13 \quad 17\ )] \begin{pmatrix} 38 & 10 & 35 \\ 35 & 9 & 16 \\ 16 & 3 & 34 \end{pmatrix} (\text{mod}\,41)$$

$$\equiv \begin{pmatrix} 222 & 45 & 183 \end{pmatrix} (\text{mod}\,41) \equiv (\ 17 \quad 4 \quad 19\ ) \sim (R\ E\ T).$$

*Thus, $Y$ recovered the plaintext $SECRET$ sent by $X$ successfully.*

## 8.3 COMPLEXITY ANALYSIS AND STRENGTH

Because it requires performing matrix multiplications of a $(\lambda \times \lambda)$ matrix $\boldsymbol{P}_{\lambda}$ into $k$ times and inverse computations for the invader, obtaining key matrices $K = \boldsymbol{P}_{\lambda}^{k}$ or $K^{-1} = \boldsymbol{P}_{\lambda}^{-k}$ is quite challenging. However, the computations for matrix multiplication and finding its inverse are made easier since the key matrices for X and Y can be easily created from the terms of the $\lambda$-th order generalized Pell sequence.

**Security Strength and Analysis**

**Example 8.3** *To create all conceivable matrices is one approach for an adversary (let's say X) to defeat our suggested method using a brute force attack [18]. Since we are working with $J_p$(where $p > 26$ must be a prime number), X must examine the $p^{\lambda^2}$ matrices.*
*If $p = 41$ and $\lambda = 30$, then X need to check $p^{\lambda^2} = 41^{30^2} = 41^{900}$ matrices, which is equivalent to $3.2023660177 \times 10^{1451}$.*
*However, we are aware that*

$$|GL_\lambda(J_p)| = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2}) \dots (p^\lambda - p^1)(p^\lambda - 1) \tag{8.1}$$

*determines the order of the General Linear group $GL_\lambda$, which consists of all invertible matrices with order over $\lambda \times \lambda$ over $\boldsymbol{P}_p$. Thus, for $p = 41$ and $\lambda = 30$ we get $|GL_{30}(P_{41})| = (41^{30} - 41^{29})(41^{30} - 41^{28}) \dots (41^{30} - 41^1)(41^{30} - 1) = 3.1223551 \times 10^{1451}$.*
*Therefore, it is extremely difficult to reconstruct the key matrix in both circumstances. The strength of the system using the suggested key matrix $\boldsymbol{P}_\lambda^k$ over $P_{41}$ is demonstrated in the list below.*

| $\lambda$ | $k$ | $\lvert GL_\lambda(P_p)\rvert = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2}) \dots (p^\lambda - p^1)(p^\lambda - 1)$ |
|---|---|---|
| 1 | 1 | $\boldsymbol{P}_1^1 = \lvert GL_1(P_{41})\rvert = 40$ |
| | 2 | $\boldsymbol{P}_1^2 = \lvert GL_1(P_{41})\rvert = 40$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{P}_1^k = \lvert GL_1(P_{41})\rvert = 40$ |
| 2 | 1 | $\boldsymbol{P}_2^1 = \lvert GL_2(P_{41})\rvert = 2.755\,2 \times 10^6$ |
| | 2 | $\boldsymbol{P}_2^2 = \lvert GL_2(P_{41})\rvert = 2.755\,2 \times 10^6$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{P}_2^k = \lvert GL_2(P_{41})\rvert = 2.755\,2 \times 10^6$ |
| 3 | 1 | $\boldsymbol{P}_3^1 = \lvert GL_3(P_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| | 2 | $\boldsymbol{P}_3^2 = \lvert GL_3(P_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{P}_3^k = \lvert GL_3(P_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $\lambda$ | $k$ | $\boldsymbol{P}_\lambda^k = \lvert GL_\lambda(P_{41})\rvert = (41^\lambda - 41^{\lambda-1})(41^\lambda - 41^{\lambda-2}) \dots (41^\lambda - 41^1)(41^\lambda - 1)$ |

*It is clear from the table above that making prime p too large makes it nearly unbreakable. Additionally, we noticed that it is independent of k and that if the size of the key matrix is increased for a fixed p, then $|GL_\lambda(P_p)| \longrightarrow \infty$. Therefore, it is impractical to breach a system via a brute-force assault if the key space is huge. The adversary might then*

*attempt to analyze the ciphertext by running various statistical tests on it.*

**Complexity Analysis**

The amount of computing power required to crack an encryption technique determines how strong it is. An algorithm's time complexity is a measure of how long it takes to execute, see [49]. Big $O$ notation is typically used to indicate an algorithm's computational complexity. It is commonly known that when multiplying matrices, the complexity in the worst case is $O(n^3)$, which makes large-scale matrix multiplications more time-consuming. However, this temporal complexity is reduced to $O(n)$ in the case of generalized Pell matrices, see (2.18).

# CHAPTER 9

# CRYPTOSYSTEM USING ELGAMAL TECHNIQUE AND THE AFFINE-HILL CIPHER WITH $\lambda$-STEP JACOBSTHAL NUMBERS

The use of different number sequences in this area makes it difficult to solve the generated cryptography. For this reason, we have applied different number sequences to cryptography. In this chapter, we develop a public key cryptosystem using ElGamal technique and the Affine-Hill cipher with $\lambda$-step Jacobsthal numbers.

## 9.1 KEY EXCHANGE ALGORITHM (ELGAMAL TECHNIQUE)

1. $p$ is prime.
2. $D$ is a private key, where $1 < D < \phi(p)$.
3. Select a primitive root of $p$, say $\alpha$.
4. Assign $E_1 = \alpha$ and $E_2 \equiv E_1^D (\mathrm{mod}\, p)$.
5. Make $(p, E_1, E_2)$ as public key and keep $D$ as secret key.

Suppose entity Vedat and Mehmet want to exchange keys. Vedat produces signature $k$ using the public key $(p, E_1, E_2)$ mentioned above by computing $k = E_1^e (\mathrm{mod}\, p)$, where $e$ is a random integer with $1 < e < \phi(p)$, and secret key $\lambda = E_2^e (\mathrm{mod}\, p)$. Mehmet's public key makes it possible for Vedat to encrypt messages using their secret key and send them $(k, C)$.

Mehmet recovers secret key by utilizing their secret key $D$ as follows after getting $(k, C)$ from Vedat:

$\lambda = k^D = (E_1^e)^D = (E_1^D)^e \equiv (E_2)^e (\mathrm{mod}\, p)$.

As a result, Mehmet successfully locates the secret key and uses it to decrypt the ciphertext $C$ and obtain the original plaintext $P$.

## 9.2 ALGORITHMS

Encryption Algorithm:

1. Vedat selects the secret number $e$ so that it is $1 < e < \phi(p)$
2. Signature: $E_1^e (\mathrm{mod}\, p) \longrightarrow k$
3. Secret key: $E_2^e (\mathrm{mod}\, p) \longrightarrow \lambda$
4. Key Matrix: $\boldsymbol{J}_\lambda^k \longrightarrow K$, where $\boldsymbol{J}_\lambda^k$ is matrix of order $\lambda \times \lambda$
5. Encryption: $Enc(P) : C_i \equiv (P_i K + B)(\mathrm{mod}\, p)$
6. Transmit $(k, C)$ to Mehmet.

Decryption Algorithm:
Mehmet, after receiving $(k, C)$.

1. Secret key: $k^D (\mathrm{mod}\, p) \longrightarrow \lambda$, ($D$ is Mehmet's secret key.)
2. Key Matrix: $\boldsymbol{J}_\lambda^k \longrightarrow K$
3. Decryption: $Dec(C) : P_i \equiv (C_i - B)K^{-1} (\mathrm{mod}\, p)$

It should be noted that $B$ is a $(1 \times \lambda)$ row vector known as a shifting vector.
Assume Vedat wishes to communicate with Mehmet. He will encrypt plaintext $P$ with $K$ using the proposed algorithm above after calculating key matrix $K$.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 | 1 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ! | ? | | |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

**Example 9.1** *(Public key calculation) Let's* $p = 41$ *and Mehmet's private key is* $D = 25$. *Further Mehmet choose primitive root of* $p$, *say* $\alpha = 35$.
*(primitive roots of* $p = \{6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35\}$*).*
*Mehmet assign* $E_1 = \alpha = 35$ *and compute* $E_2 = E_1^D (\mathrm{mod}\, p) = 35^{25} (\mathrm{mod}\, 41) = 27$. *Mehmet's public key* $pk(p, E_1, E_2)$ *is* $pk(41, 35, 27)$ *and secret key is* $D = 25$.

**Example 9.2** *(Encryption-Decryption) Suppose plaintext* $P$ *is* $CODING$, *public key is* $pk(41, 35, 27)$ *and shifting vector* $B$ *is* $(29, 11, 19)$.

**Solution 9.1** *For encryption, choose* $e = 19$ *such that* $1 < e < \phi(p)$. *Calculating signature* $k = E_1^e = 35^{19} (\mathrm{mod}\, 41) \equiv 7$ *and secret key* $\lambda = E_2^e = 27^{19} (\mathrm{mod}\, 41) \equiv 3$ *construct the key matrix* $K = \boldsymbol{J}_\lambda^k = \boldsymbol{J}_3^7$ *using* $\lambda = 3rd$ *order generalized Jacobsthal matrix. Generalized Jacobsthal sequence for* $\lambda = 3$ *is given by*

| *Index* | $\ldots$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ | $8$ | $\ldots$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Jacobsthal numbers* | $\ldots$ | $-\frac{1}{4}$ | $\frac{1}{2}$ | $0$ | $0$ | $1$ | $1$ | $2$ | $5$ | $9$ | $18$ | $37$ | $73$ | $\ldots$ |

*we have*

$$K = \begin{pmatrix} J_8 & J_7 + 2J_6 & 2J_7 \\ J_7 & J_6 + 2J_5 & 2J_6 \\ J_6 & J_5 + 2J_4 & 2J_5 \end{pmatrix} = \begin{pmatrix} 73 & 73 & 74 \\ 37 & 36 & 36 \\ 18 & 19 & 18 \end{pmatrix}$$

$$K(\mathrm{mod}\, 41) = \begin{pmatrix} 32 & 32 & 33 \\ 37 & 36 & 36 \\ 18 & 19 & 18 \end{pmatrix}.$$

*The plaintext* $P = CODING$ *is divided into blocks each of size* $\lambda$ *and obtain numerical values*

$P_1 = (COD) = (\ 2 \quad 14 \quad 3\ )$ *and* $P_2 = (ING) = (\ 8 \quad 13 \quad 6\ )$.

*Encryption:* $C \equiv (PK + B)(\mathrm{mod}\, 41)$

$$\begin{aligned} C_1 &= (P_1 K + B) \\ &\equiv [(\ 2 \quad 14 \quad 3\ ) \begin{pmatrix} 32 & 32 & 33 \\ 37 & 36 & 36 \\ 18 & 19 & 18 \end{pmatrix} + (\ 29 \quad 11 \quad 19\ )](\mathrm{mod}\, 41) \\ &\equiv (\ 665 \quad 636 \quad 643\ )(\mathrm{mod}\, 41) \\ &\equiv (\ 9 \quad 21 \quad 28\ ) \sim (J92), \end{aligned}$$

*and*

$$\begin{aligned} C_2 &= (P_2K + B) \\ &\equiv [(\ 8 \quad 13 \quad 6\ ) \begin{pmatrix} 32 & 32 & 33 \\ 37 & 36 & 36 \\ 18 & 19 & 18 \end{pmatrix} + (\ 29 \quad 11 \quad 19\ )](\mathrm{mod}\, 41) \\ &\equiv (\ 874 \quad 849 \quad 859\ )(\mathrm{mod}\, 41) \\ &\equiv (\ 13 \quad 29 \quad 39\ ) \sim (N3?). \end{aligned}$$

*Cipher-text* $C = (C_1C_2) = (J92N3?)$ *and hence* $P : CODING \longrightarrow C : J92N3?$. *Vedat encrypts this message* $C$ *and transmits it to Mehmet with her signature* $k$.
*Decryption: Mehmet will determine the decryption key* $K^{-1} = \boldsymbol{J}_\lambda^{-k} = \boldsymbol{J}_3^{-7}$ *after receiving the ciphertext* $C$ *and the signature* $k$, *where* $\lambda = k^D(\mathrm{mod}\, 41) = 7^{25}(\mathrm{mod}\, 41) \equiv 3$ *is obtained using the secret key* $D$. *So we get*

$$\begin{aligned} K^{-1}(\mathrm{mod}\, 41) &= \begin{pmatrix} -\frac{12}{29} & \frac{17}{29} & -\frac{12}{29} \\ -\frac{6}{29} & -\frac{6}{29} & \frac{23}{29} \\ \frac{55}{87} & -\frac{32}{87} & -\frac{32}{87} \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 1 & 2 & 1 \\ 21 & 21 & 22 \\ 11 & 10 & 10 \end{pmatrix}, \end{aligned}$$

*and*

$$\begin{pmatrix} 32 & 32 & 33 \\ 37 & 36 & 36 \\ 18 & 19 & 18 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 21 & 21 & 22 \\ 11 & 10 & 10 \end{pmatrix} = \begin{pmatrix} 1067 & 1066 & 1066 \\ 1189 & 1190 & 1189 \\ 615 & 615 & 616 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (\mathrm{mod}\, 41).$$

*Decryption takes place as* $P_i \equiv (C_i - B)K^{-1}(\mathrm{mod}\, 41)$. *Then we have*

$$\begin{aligned} P_1 &= (C_1 - B)K^{-1} \\ &= [(\ 9 \quad 21 \quad 28\ ) - (\ 29 \quad 11 \quad 19\ )] \begin{pmatrix} 1 & 2 & 1 \\ 21 & 21 & 22 \\ 11 & 10 & 10 \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 289 & 260 & 290 \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv (\ 2 \quad 14 \quad 3\ ) \sim (COD), \end{aligned}$$

*and*

$$\begin{aligned} P_2 &= (C_2 - B)K^{-1} \\ &= [(\ 13 \quad 29 \quad 39\ ) - (\ 29 \quad 11 \quad 19\ )] \begin{pmatrix} 1 & 2 & 1 \\ 21 & 21 & 22 \\ 11 & 10 & 10 \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 582 & 546 & 580 \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv (\ 8 \quad 13 \quad 6\ ) \sim (ING). \end{aligned}$$

*Mehmet was able to successfully obtain the plaintext CODING that Vedat had sent.*

## 9.3 COMPLEXITY ANALYSIS AND STRENGTH

It is extremely difficult to obtain key matrices $K = \boldsymbol{J}_\lambda^k$ or $K^{-1} = \boldsymbol{J}_\lambda^{-k}$ because it requires matrix multiplications of a $(\lambda \times \lambda)$ matrix $\boldsymbol{J}_\lambda$ in to $k$ times and calculations of its inverse for the intruder. However, for Vedat and Mehmet, it is quite simple to construct key matrices from the terms of the $\lambda$ th order generalized Jacobsthal sequence, which simplifies matrix multiplication and inverse calculations.

**Security Strength and Analysis**

**Example 9.3** *To create all conceivable matrices is one approach for an adversary (let's say X) to defeat our suggested method using a brute force attack [18]. Since we are working with $J_p$(where $p > 26$ must be a prime number), X must examine the $p^{\lambda^2}$ matrices.*
*If $p = 41$ and $\lambda = 30$, then X need to check $p^{\lambda^2} = 41^{30^2} = 41^{900}$ matrices, which is equivalent to $3.2023660177 \times 10^{1451}$ (too large).*
*However, we are aware that*

$$|GL_\lambda(J_p)| = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2}) \ldots (p^\lambda - p^1)(p^\lambda - 1) \tag{9.1}$$

*determines the order of the General Linear group $GL_\lambda$, which consists of all invertible matrices with order over $\lambda \times \lambda$ over $\boldsymbol{J}_p$. Thus, for $p = 41$ and $\lambda = 30$ we get $|GL_{30}(J_{41})| = (41^{30} - 41^{29})(41^{30} - 41^{28}) \ldots (41^{30} - 41^1)(41^{30} - 1) = 3.1223551 \times 10^{1451}$.*
*Therefore, it is extremely difficult to reconstruct the key matrix in both circumstances. The strength of the system using the suggested key matrix $\boldsymbol{J}_\lambda^k$ over $J_{41}$ is demonstrated in the list below.*

| $\lambda$ | $k$ | $\lvert GL_\lambda(J_p)\rvert = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2})\dots(p^\lambda - p^1)(p^\lambda - 1)$ |
|---|---|---|
| 1 | 1 | $\boldsymbol{J}_1^1 = \lvert GL_1(J_{41})\rvert = 40$ |
| | 2 | $\boldsymbol{J}_1^2 = \lvert GL_1(J_{41})\rvert = 40$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{J}_1^k = \lvert GL_1(J_{41})\rvert = 40$ |
| 2 | 1 | $\boldsymbol{J}_2^1 = \lvert GL_2(J_{41})\rvert = 2.755\,2 \times 10^6$ |
| | 2 | $\boldsymbol{J}_2^2 = \lvert GL_2(J_{41})\rvert = 2.755\,2 \times 10^6$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{J}_2^k = \lvert GL_2(J_{41})\rvert = 2.755\,2 \times 10^6$ |
| 3 | 1 | $\boldsymbol{J}_3^1 = \lvert GL_3(J_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| | 2 | $\boldsymbol{J}_3^2 = \lvert GL_3(J_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| | $\vdots$ | $\vdots$ |
| | $k$ | $\boldsymbol{J}_3^k = \lvert GL_3(J_{41})\rvert = 3.19\,202\,373\,504 \times 10^{14}$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $\lambda$ | $k$ | $\boldsymbol{J}_\lambda^k = \lvert GL_\lambda(J_{41})\rvert = (41^\lambda - 41^{\lambda-1})(41^\lambda - 41^{\lambda-2})\dots(41^\lambda - 41^1)(41^\lambda - 1)$ |

*It is clear from the table above that making prime p too large makes it nearly unbreakable. Additionally, we noticed that it is independent of k and that if the size of the key matrix is increased for a fixed p, then* $\lvert GL_\lambda(J_p)\rvert \longrightarrow \infty$. *Therefore, it is impractical to breach a system via a brute-force assault if the key space is huge. The adversary might then attempt to analyze the ciphertext by running various statistical tests on it.*

**Complexity Analysis**

The amount of computing power required to crack an encryption technique determines how strong it is. An algorithm's time complexity is a measure of how long it takes to execute, see [49]. Big $O$ notation is typically used to indicate an algorithm's computational complexity. It is commonly known that when multiplying matrices, the complexity in the worst case is $O(n^3)$, which makes large-scale matrix multiplications more time-consuming. However, this temporal complexity is reduced to $O(n)$ in the case of generalized Jacobsthal matrices, see (2.14).

# CHAPTER 10

# ON THE ROLE OF THE THIRD ORDER PELL NUMBERS AND LINEAR DIOPHANTINE EQUATIONS IN CRYPTOGRAPHY

In this chapter, we propose a new encryption-decryption algorithm using solutions of linear Diophantine equations with $n-$variables and the third order Pell $\mathbf{P}$ matrix, the algorithm depends on dividing the message matrix into the block matrices each is of size $3 \times 3$. We use different numbered alphabet for each message, so we get a more reliable encryption method. The alphabet is determined by the number of block matrices of the message matrix and the number $u$ that we use in the public key algorithm.

## 10.1 KEY EXCHANGE ALGORITHM [7] (SOLUTION OF LINEAR DIOPHANTINE EQUATIONS WITH $n$-VARIABLES TECHNIQUE)

1. Sender generates public key.

   - A linear Diophantine equation $g(x_1, x_2, \ldots, x_n)$ is considered by the sender.
   - The sender generates the operator on the Diophantine equation given as for $T_i = T_{[p_i,q_i]}(g) = (g + p_i)q_i$, where $p_i, q_i$ parameters and $p_i \geq 0$, $q_i > 0$ $\forall i = 1, 2, \ldots, m$.
   - The sender generates the public key by taking key as $T = T_m \circ T_{m-1} \circ \cdots \circ T_1$ and computes $T(g)$ as

   $$\begin{aligned} T(g) &= T_m.T_{m-1}.\cdots.T_1(g(x_1, x_2, \ldots, x_n)) \\ &= (((g(x_1, x_2, \ldots, x_n) + p_1)q_1 + p_2)q_2 \ldots + p_m)q_m \\ &= h(x_1, x_2, \ldots, x_n). \end{aligned}$$

   - The sender makes the Diophantine equations $h(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ public.

2. Recipient generates public key and private key.

   - A linear Diophantine equation $f(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ in $n$ variables for $n > 2$ such that $\gcd(a_1, a_2, \ldots, a_n)$ divides $b$ is considered by the sender.
   - The recipient selects a random solution $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the linear Diophantine equation $f(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$.
   - The recipient on receiving the public key Diophantine equations evaluates $h(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ evaluates $h(\alpha_1, \alpha_2, \ldots, \alpha_n) = u$, $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = v$.
   - The recipient keeps the evaluated value $v$ as secret key and makes $u$ public key.

3. The sender recovers the secret key.

   - The sender recovers the secret key $v$ from public key $u$ by applying the inverse of operators $T_i$ where for $T_i$ we have $T_i^{-1} = T_{[p_i,q_i]}^{-1}$ with $T_{[p_i,q_i]}^{h} = (h)\frac{1}{q_i} - p_i$.
   - Sender from $T_i^{-1}$ the inverse of $T_i$ recovers $v$ from $u$ by

     $$(T_m \circ T_{m-1} \circ \cdots \circ T_1)^{-1}(u) = T_1^{-1} \circ T_2^{-1} \circ \ldots \circ T_{m-1}^{-1} \circ T_m^{-1}.$$

4. The secret key $v$ evaluated by both sender and receiver is used as the key for key exchange.

## 10.2 THE ENCRYPTION AND DECRYPTION ALGORITHMS

First, we put our message in a matrix $M$ of size $3m \times 3m$ leaving space between two words. Divide the square $M$ message matrix of the size 3m in the matrices, named $B_i$ of the size $3 \times 3$. $(1 \leq i \leq m^2)$

$$B_i = \begin{pmatrix} b_1^i & b_2^i & b_3^i \\ b_4^i & b_5^i & b_6^i \\ b_7^i & b_8^i & b_9^i \end{pmatrix}, E_i = \begin{pmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{pmatrix}, \mathbf{P}^\lambda = \begin{pmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{pmatrix}.$$

**Encryption Algorithm**

The number of the block matrices is denoted by $s$. According to $s$ and $u$, we choose the number $n$ as follows. Let's accept $\left[\left|\frac{u}{s}+1\right|\right]=y$,

$$n=\begin{cases} 2 & , \ y\leq 2 \\ y-3 & , \ y>2 \end{cases}.$$

We will use the following table according to (mod 41)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ |
| $n$ | $n+1$ | $n+2$ | $n+3$ | $n+4$ | $n+5$ | $n+6$ | $n+7$ | $n+8$ |
| $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ |
| $n+9$ | $n+10$ | $n+11$ | $n+12$ | $n+13$ | $n+14$ | $n+15$ | $n+16$ | $n+17$ |
| $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 |
| $n+18$ | $n+19$ | $n+20$ | $n+21$ | $n+22$ | $n+23$ | $n+24$ | $n+25$ | $n+26$ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $n+27$ | $n+28$ | $n+29$ | $n+30$ | $n+31$ | $n+32$ | $n+33$ | $n+34$ | $n+35$ |
| | . | , | ! | ? | | | | |
| $n+36$ | $n+37$ | $n+38$ | $n+39$ | $n+40$ | | | | |

1. Choose $n$.
2. Determine $b_j^i$ $(1\leq j\leq 9)$.
3. Compute $\det(B_i)=d_i$.
4. Construct $C=[b_k^i,d_i]_{k\in\{1,2,3,4,6,7,8,9\}}$.
5. Transmit $(u,n,C)$.

**Decryption Algorithm**

1. Compute $v$.
2. Compute $\mathbf{P}^v$.
3. Compute

$$\begin{array}{lll} p_1b_1^i+p_2b_4^i+p_3b_7^i=e_1^i & p_1b_2^i+p_3b_8^i=e_2^i & p_1b_3^i+p_2b_6^i+p_3b_9^i=e_3^i, \\ p_4b_1^i+p_5b_4^i+p_6b_7^i=e_4^i & p_4b_2^i+p_6b_8^i=e_5^i & 4_4b_3^i+p_5b_6^i+p_6b_9^i=e_6^i, \\ p_7b_1^i+p_8b_4^i+p_9b_7^i=e_7^i & p_7b_2^i+p_9b_8^i=e_8^i & p_7b_3^i+p_8b_6^i+p_9b_9^i=e_9^i. \end{array}$$

4. Solve $1^{\lambda}.d_i = -(e_2^i + p_2 x_i)(e_4^i e_9^i - e_6^i e_7^i) + (e_5^i + p_5 x_i)(e_1^i e_9^i - e_3^i e_7^i) - (e_8^i + p_8 x_i)(e_1^i e_6^i - e_3^i e_4^i)$.

5. Substitute for $x_i = b_5^i$.

6. Construct $B_i$.

7. Construct $M$.

**Example 10.1** *(Public key calculation) The sender considers a linear Diophantine equation* $g(x_1, x_2, x_3) = 5x_1 - 3x_2 + x_3 + 1$. *Let* $T_1 = T_{[2,1]}$, $T_2 = T_{[3,4]}$

$$\begin{aligned} h(x_1, x_2, x_3) &= T_2 \circ T_1(g(x_1, x_2, x_3)) \\ &= T_2 \circ T_1(5x_1 - 3x_2 + x_3 + 1) \\ &= T_{[3,4]}.T_{[2,1]}(5x_1 - 3x_2 + x_3 + 1) \\ &= T_{[3,4]}((5x_1 - 3x_2 + x_3 + 1 + 2).1) \\ &= T_{[3,4]}(5x_1 - 3x_2 + x_3 + 3) \\ &= ((5x_1 - 3x_2 + x_3 + 3) + 3).4 \\ &= 20x_1 - 12x_2 + 4x_3 + 24. \end{aligned}$$

*Sender makes*

$$\begin{cases} 5x_1 - 3x_2 + x_3 + 1 \\ 20x_1 - 12x_2 + 4x_3 + 24 \end{cases}$$

*public.*

*The recipient consider the linear Diophantine equation* $f(x_1, x_2, x_3) = 2x_1 + 3x_2 + 4x_3 - 10$. *Let* $(\alpha_1, \alpha_2, \alpha_3) = (2, 2, 0)$ *and keeps it private. Recipient evaluates*

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3) &= 20.2 - 12.2 + 4.0 + 24 \\ &= 40 \\ g(\alpha_1, \alpha_2, \alpha_3) &= 5.2 - 3.2 + 0 + 1 \\ &= 5. \end{aligned}$$

*The recipient keeps* $v = 5$ *as secret key and makes* $u = 40$ *as public key. The sender recovers secret key* $v$.

**Example 10.2** *Consider the message "OPERATORS CODING DECODING ALGORITHM."*

$$M = \begin{pmatrix} O & P & E & R & A & T \\ O & R & S & & C & O \\ D & I & N & G & & D \\ E & C & O & D & I & N \\ G & & A & L & G & O \\ R & I & T & H & M & . \end{pmatrix}$$

***Encryption***

*We get the following calculations.*

$m = 2$ *and* $s = 4$

$$B_1 = \begin{pmatrix} O & P & E \\ O & R & S \\ D & I & N \end{pmatrix}, B_2 = \begin{pmatrix} R & A & T \\ & C & O \\ G & & D \end{pmatrix},$$

$$B_3 = \begin{pmatrix} E & C & O \\ G & & A \\ R & I & T \end{pmatrix}, B_4 = \begin{pmatrix} D & I & N \\ L & G & O \\ H & M & . \end{pmatrix}.$$

1. $\left[\left|\frac{40}{4} + 1\right|\right] = 11 = y \Longrightarrow n = 11 - 3 = 8.$

2. $B_1 = \begin{pmatrix} 22 & 23 & 12 \\ 22 & 25 & 26 \\ 11 & 16 & 21 \end{pmatrix}$, $B_2 = \begin{pmatrix} 25 & 8 & 27 \\ 3 & 10 & 22 \\ 14 & 3 & 11 \end{pmatrix}$, $B_3 = \begin{pmatrix} 12 & 10 & 22 \\ 14 & 3 & 8 \\ 25 & 16 & 27 \end{pmatrix}$, $B_4 = \begin{pmatrix} 11 & 16 & 21 \\ 19 & 14 & 22 \\ 15 & 20 & 4 \end{pmatrix}$.

3. $d_1 = -726$, $d_2 = -237$, $d_3 = 934$, $d_4 = 3410$.

4. $C = \begin{pmatrix} 22 & 23 & 12 & 22 & 26 & 11 & 16 & 21 & -726 \\ 25 & 8 & 27 & 3 & 22 & 14 & 3 & 11 & -237 \\ 12 & 10 & 22 & 14 & 8 & 25 & 16 & 27 & 934 \\ 11 & 16 & 21 & 19 & 22 & 15 & 20 & 4 & 3410 \end{pmatrix}$.

5. $(40, 8, \begin{pmatrix} 22 & 23 & 12 & 22 & 26 & 11 & 16 & 21 & -726 \\ 25 & 8 & 27 & 3 & 22 & 14 & 3 & 11 & -237 \\ 12 & 10 & 22 & 14 & 8 & 25 & 16 & 27 & 934 \\ 11 & 16 & 21 & 19 & 22 & 15 & 20 & 4 & 3410 \end{pmatrix})$.

***Decryption***

*We have the following calculations.*

1.

$$\begin{aligned}(T_2 \circ T_1)^{-1}(u) &= T_{[2,1]}^{-1} \circ T_{[3,4]}^{-1}(40) \\ &= T_{[2,1]}^{-1}(40.\frac{1}{4} - 3) \\ &= T_{[2,1]}^{-1}(7) \\ &= (7.\frac{1}{1} - 2) \\ &= 5 \\ &= v.\end{aligned}$$

2. $\mathbf{P}^v = \begin{pmatrix} 84 & 46 & 33 \\ 33 & 18 & 13 \\ 13 & 7 & 5 \end{pmatrix}$.

3. *For* $B_1$

$$\begin{aligned} e_1^1 = 3223 \quad e_2^1 = 2460 \quad e_3^1 = 2897, \\ e_4^1 = 1265 \quad e_5^1 = 967 \quad e_6^1 = 1137, \\ e_7^1 = 495 \quad e_8^1 = 379 \quad e_9^1 = 443. \end{aligned}$$

4. $1^5.d_1 = -(e_2^1 + p_2x_1)(e_4^1e_9^1 - e_6^1e_7^1) + (e_5^1 + p_5x_1)(e_1^1e_9^1 - e_3^1e_7^1) - (e_8^1 + p_8x_1)(e_1^1e_6^1 - e_3^1e_4^1)$

$-726 = (2460 + 46x_1).(-2420) + (967 + 18x_1).(-6226) + (379 + 7x_1).(-154)$

$\Longrightarrow x_1 = 25.$

5. $x_1 = b_5^1 = 25.$

6. $B_1 = \begin{pmatrix} 22 & 23 & 12 \\ 22 & 25 & 26 \\ 11 & 16 & 21 \end{pmatrix}$.

*The same process steps are done for the* $B_2, B_3, B_4$.

$$B_2 = \begin{pmatrix} 25 & 8 & 27 \\ 3 & 10 & 22 \\ 14 & 3 & 11 \end{pmatrix}, B_3 = \begin{pmatrix} 12 & 10 & 22 \\ 14 & 3 & 8 \\ 25 & 16 & 27 \end{pmatrix}, B_4 = \begin{pmatrix} 11 & 16 & 21 \\ 19 & 14 & 22 \\ 15 & 20 & 4 \end{pmatrix}.$$

7. $M = \begin{pmatrix} 22 & 23 & 12 & 25 & 8 & 27 \\ 22 & 25 & 26 & 3 & 10 & 22 \\ 11 & 16 & 21 & 14 & 3 & 11 \\ 12 & 10 & 22 & 11 & 16 & 21 \\ 14 & 3 & 8 & 19 & 14 & 22 \\ 25 & 16 & 27 & 15 & 20 & 4 \end{pmatrix} = \begin{pmatrix} O & P & E & R & A & T \\ O & R & S & & C & O \\ D & I & N & G & & D \\ E & C & O & D & I & N \\ G & & A & L & G & O \\ R & I & T & H & M & . \end{pmatrix}$.

# CHAPTER 11

## AN APPLICATION TO CODING THEORY USING $3-PRIMES$ CIRCULANT MATRICES WITH AFFINE-HILL CIPHER

There are two types of cryptosystems, the symmetric key cryptosystem using a single key in both encryption and decryption, and the asymmetric key cryptosystem using different keys. The asymmetric key cryptosystem includes the public key and the private key. The public key and private key are critical in advanced cryptosystems. Important studies on the public key and the private key have been conducted in order to reduce insecure situations. Application to linear Diophantine equations is one of them. In this chapter, we develop a public key cryptosystem using key exchange based on the relationship between $n$-variable linear Diophantine equations and linear operators and the Affine-Hill cipher with 3-primes circulant matrices.

**Remark 11.1** *In this study, we will take the smallest positive integer with respect to* $(\mathrm{mod}\, 41)$ *of any given number. For example* $\frac{19}{645}(\mathrm{mod}\, 41) = 2$. *Because* $645x = 19(\mathrm{mod}\, 41)$

$$\Rightarrow \quad x = \frac{19 + 41n}{645}$$

$$\Rightarrow \quad n = 3,\ x = 2.$$

### 11.1 KEY EXCHANGE ALGORITHM BASED ON THE RELATIONSHIP BETWEEN $n$-VARIABLE LINEAR DIOPHANTINE EQUATIONS AND LINEAR MAPPINGS

In this section, we will construct a key exchange algorithm based on the relationship between linear diophantine equations with $n$-variables and linear mappings.
Generating the public key by the message sender;

1. The message sender creates the linear Diophantine equation $g(x_1, x_2, \ldots, x_j)$ and the linear mapping $T$ given as $T_k = T_{[m_k,n_k]}(g) = (1 + m_k)g + n_k$ by thinking about it, where $m_k, n_k$ are parameters and $m_k \geq 0$, $n_k \geq 0$. $\forall k = 1, 2, \ldots, s$.

2. Public key $h(x_1, x_2, \ldots, x_j)$ is generated as

$$\underbrace{T \circ T \circ \ldots \circ T}_{s-times}(g) \quad = \quad h(x_1, x_2, \ldots, x_j).$$

3. After the sender creates the $h$ and $g$ equations, they are sent to the person who will receive the message.

Generating the public key and private key by the person receiving the message

1. The receiver creates a linear Diophantine equation $f(x_1, x_2, \ldots, x_j) = a_1x_1 + a_2x_2 + \ldots + a_jx_j = b$ in $n$-variables for $n > 2$ such that $\gcd(a_1, a_2, \ldots, a_j)$ divides $b$ and selects a random solution $(\alpha_1, \alpha_2, \ldots, \alpha_j)$ of the linear Diophantine equation $f(x_1, x_2, \ldots, x_j) = a_1x_1 + a_2x_2 + \ldots + a_jx_j = b$.

2. The receiver calculates the expressions $h(\alpha_1, \alpha_2, \ldots, \alpha_j) = u$ and $g(\alpha_1, \alpha_2, \ldots, \alpha_j) = v$ according to the $h(x_1, x_2, \ldots, x_j)$ and $g(x_1, x_2, \ldots, x_j)$ public key Diophantine equations.

3. The receiver of the message makes $u$ the public key and $v$ the private key.

Resolution of the private key by the sender.

1. The sender decrypts the private key $v$ from the public key $u$ by applying the inverse of the $T$ linear mapping, where $T^{-1} = \frac{1}{1+m_k}(h - n_k)$.

2. Solve $v$ from $u$ with the expression $(T \circ T \circ \ldots \circ T)^{-1}(u) = T^{-1} \circ T^{-1} \circ \ldots \circ T^{-1}(u)$.

Key exchange

1. $v$ secret key calculated by both sender and receiver can be used as key for key exchange.

## 11.2 A NEW ALGORITHM USING $3-PRIMES$ CIRCULANT MATRICES WITH AFFINE-HILL CIPHER

**Algorithms**

Encryption Algorithm:

1. $X$ chooses Diophantine equation $g$ and generates $h$
2. $X$ recovers the secret key $v$
3. Key Matrix: $\boldsymbol{C}_v(W) \longrightarrow K$, where $\boldsymbol{C}_v(W)$ is $3-primes$ circulant matrice of order $v \times v$
4. Encryption: $Enc(M) : C_i \equiv (M_iK + B)(\mathrm{mod}\, p)$
5. Transmit $(C)$ to $Y$.

Decryption Algorithm:
$Y$, after receiving $(C)$.

1. Key Matrix: $\boldsymbol{C}_v(W) \longrightarrow K$
2. Decryption: $Dec(C) : M_i \equiv (C_i - B)K^{-1}(\mathrm{mod}\, p)$

Note that $B$ is an $(1 \times v)$ row vector called shifting vector. Also $B = (W_0, W_0 + W_1, \ldots, W_0 + W_1 + \cdots + W_{v-1})$.
Suppose that $X$ wants to send a message to $Y$. After calculating key matrix $K$, he will encrypt plaintext $M$ with $K$ using the proposed algorithm above.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 | 1 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ! | ? | | |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

**Example 11.1** *The sender* $(X)$ $g(x_1, x_2, x_3) = 3x_1 + 6x_2 + 2x_3 - 4$ *take the linear Diophantine equation and let* $T_1 = T_{[2,5]}$, $T_2 = T_{[3,7]}$.

$$\begin{aligned} h(x_1, x_2, x_3) &= T_2 \circ T_1(g(x_1, x_2, x_3)) \\ &= T_2 \circ T_1(3x_1 + 6x_2 + 2x_3 - 4) \\ &= T_2(9x_1 + 18x_2 + 6x_3 - 7) \\ &= 36x_1 + 72x_2 + 24x_3 - 21. \end{aligned}$$

$$\begin{cases} g(x_1, x_2, x_3) = 3x_1 + 6x_2 + 2x_3 - 4 \\ h(x_1, x_2, x_3) = 36x_1 + 72x_2 + 24x_3 - 21 \end{cases}$$

*system is created.*

*The receiver* $(Y)$ *considers the linear Diophantine equation* $f(x_1, x_2, x_3) = 2x_1 - 3x_2 + x_3 + 2$ *and its solution* $(\alpha_1, \alpha_2, \alpha_3) = (0, 1, 1)$.

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3) &= 75 = u \\ g(\alpha_1, \alpha_2, \alpha_3) &= 4 = v. \end{aligned}$$

*The receiver* $(Y)$ *makes* $v$ *the private key and* $u$ *the public key.*

*The sender* $(X)$ *solves* $v$ *from* $u$.

$$\begin{aligned} (T_2 \circ T_1)^{-1}(h(\alpha_1, \alpha_2, \alpha_3)) &= T_1^{-1} \circ T_2^{-1}(h(\alpha_1, \alpha_2, \alpha_3)) \\ &= T_1^{-1} \circ T_2^{-1}(75) \\ &= T_1^{-1}(\frac{1}{1+3}(75 - 7)) \\ &= T_1^{-1}(17) \\ &= \frac{1}{1+2}(17 - 5) \\ &= 4 \\ &= v \end{aligned}$$

*So* $v$ *public secret key can be used as key for key exchange.*

**Example 11.2** *(Encryption-Decryption) Suppose that plaintext* $M$ *is* $TEACHER$.

**Solution 11.1** *For encryption, secret key* $v = 4$ *construct the key matrix* $K = \boldsymbol{C}_4(W)$

*using $v = 4th$ order $3-primes$ circulant matrix.*

$$K = \boldsymbol{C}_4(W) = \begin{pmatrix} 0 & 1 & 2 & 7 \\ 7 & 0 & 1 & 2 \\ 2 & 7 & 0 & 1 \\ 1 & 2 & 7 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 1 & 3 & 10 \end{pmatrix}$$

*The plaintext $M = TEACHER.$ is divided into blocks each of size $v$ and obtain numerical values*

$M_1 = (TEAC) = \begin{pmatrix} 19 & 4 & 0 & 2 \end{pmatrix}$ *and* $M_2 = (HER.) = \begin{pmatrix} 7 & 4 & 17 & 36 \end{pmatrix}$.

*Encryption:* $C \equiv (MK + B)(\mathrm{mod}\, 41)$

$$\begin{aligned} C_1 &\equiv (M_1K + B)(\mathrm{mod}\, 41) \\ &\equiv [(\ 19 \quad 4 \quad 0 \quad 2\ ) \begin{pmatrix} 0 & 1 & 2 & 7 \\ 7 & 0 & 1 & 2 \\ 2 & 7 & 0 & 1 \\ 1 & 2 & 7 & 0 \end{pmatrix} + (\ 0 \quad 1 \quad 3 \quad 10\ )](\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 30 & 24 & 59 & 151 \end{pmatrix} (\mathrm{mod}\, 41) \\ &= (\ 30 \quad 24 \quad 18 \quad 28\ ) \sim (4YS2). \end{aligned}$$

*The $C_1$ password corresponding to the $M_1$ block plaintext is $(4YS2)$.*

$$\begin{aligned} C_2 &\equiv (M_2K + B)(\mathrm{mod}\, 41) \\ &\equiv [(\ 7 \quad 4 \quad 17 \quad 36\ ) \begin{pmatrix} 0 & 1 & 2 & 7 \\ 7 & 0 & 1 & 2 \\ 2 & 7 & 0 & 1 \\ 1 & 2 & 7 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 3 & 10 \end{pmatrix}](\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 98 & 199 & 273 & 84 \end{pmatrix} (\mathrm{mod}\, 41) \\ &= (\ 16 \quad 35 \quad 27 \quad 2\ ) \sim (Q91C). \end{aligned}$$

*The $C_2$ password corresponding to the $M_2$ block plaintext is $(Q91C)$.*

*Cipher-text $C = (C_1C_2) = (4YS2Q91C)$ and hence $M : TEACHER. \longrightarrow C : 4YS2Q91C.$*

*$X$ send this cipher-text $C$ to $Y$.*

*Decryption: Receiving ciphertext $C$, $Y$ will calculate decryption key $K^{-1} = \boldsymbol{C}_4^{-1}(W)$ where $v = 4$.*

$$K^{-1}(\mathrm{mod}\,41) \equiv \begin{pmatrix} -\frac{1}{24} & \frac{17}{120} & \frac{1}{120} & -\frac{1}{120} \\ -\frac{1}{120} & -\frac{1}{24} & \frac{17}{120} & \frac{1}{120} \\ \frac{1}{120} & -\frac{1}{120} & -\frac{1}{24} & \frac{17}{120} \\ \frac{17}{120} & \frac{1}{120} & -\frac{1}{120} & -\frac{1}{24} \end{pmatrix} (\mathrm{mod}\,41)$$

$$= \begin{pmatrix} 29 & 8 & 27 & 14 \\ 14 & 29 & 8 & 27 \\ 27 & 14 & 29 & 8 \\ 8 & 27 & 14 & 29 \end{pmatrix}$$

*It is seen that*

$$\begin{pmatrix} 0 & 1 & 2 & 7 \\ 7 & 0 & 1 & 2 \\ 2 & 7 & 0 & 1 \\ 1 & 2 & 7 & 0 \end{pmatrix} \begin{pmatrix} 29 & 8 & 27 & 14 \\ 14 & 29 & 8 & 27 \\ 27 & 14 & 29 & 8 \\ 8 & 27 & 14 & 29 \end{pmatrix} (\mathrm{mod}\,41)$$

$$\equiv \begin{pmatrix} 124 & 246 & 164 & 246 \\ 246 & 124 & 246 & 164 \\ 164 & 246 & 124 & 246 \\ 246 & 164 & 246 & 124 \end{pmatrix} (\mathrm{mod}\,41)$$

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

*Decryption takes place as* $P_i \equiv (C_i - B)K^{-1}(\mathrm{mod}\,41)$

$$M_1 \equiv (C_1 - B)K^{-1}(\mathrm{mod}\,41)$$

$$= [(\ 30 \quad 24 \quad 18 \quad 28\ ) - (\ 0 \quad 1 \quad 3 \quad 10\ )] \begin{pmatrix} 29 & 8 & 27 & 14 \\ 14 & 29 & 8 & 27 \\ 27 & 14 & 29 & 8 \\ 8 & 27 & 14 & 29 \end{pmatrix} (\mathrm{mod}\,41)$$

$$\equiv \begin{pmatrix} 1741 & 1603 & 1681 & 1683 \end{pmatrix} (\mathrm{mod}\,41)$$

$$= \begin{pmatrix} 19 & 4 & 0 & 2 \end{pmatrix} \sim (TEAC).$$

*The $M_1$ plaintext corresponding to the $C_1$ password is $(TEAC)$.*

$$\begin{aligned} M_2 &\equiv (C_2 - B)K^{-1} (\mathrm{mod}\, 41) \\ &= [(\ 16 \quad 35 \quad 27 \quad 2\ ) - (\ 0 \quad 1 \quad 3 \quad 10\ )] \begin{pmatrix} 29 & 8 & 27 & 14 \\ 14 & 29 & 8 & 27 \\ 27 & 14 & 29 & 8 \\ 8 & 27 & 14 & 29 \end{pmatrix} (\mathrm{mod}\, 41) \\ &\equiv \begin{pmatrix} 1524 & 1234 & 1288 & 1102 \end{pmatrix} (\mathrm{mod}\, 41) \\ &= \begin{pmatrix} 7 & 4 & 17 & 36 \end{pmatrix} \sim (HER.)\,. \end{aligned}$$

*The $M_2$ plaintext corresponding to the $C_2$ password is $(HER.)$.*
*Thus, $Y$ recovered the plaintext $TEACHER.$ sent by $X$ successfully.*

Let's increase the number of operators to three in the next example and make it a little more difficult. Thus, the precaution taken against those who want to intercept the message will be increased.

**Example 11.3** *The sender $(X)$ $g(x_1, x_2, x_3, x_4) = 2x_1 - x_2 + 3x_3 + 4x_4 - 1$ take the linear Diophantine equation and let $T_1 = T_{[3,2]}$, $T_2 = T_{[1,4]}$ and $T_3 = T_{[2,6]}$.*

$$\begin{aligned} h(x_1, x_2, x_3, x_4) &= T_3 \circ T_2 \circ T_1(g(x_1, x_2, x_3, x_4)) \\ &= T_3 \circ T_2 \circ T_1(2x_1 - x_2 + 3x_3 + 4x_4 - 1) \\ &= T_3 \circ T_2(8x_1 - 4x_2 + 12x_3 + 16x_4 - 2) \\ &= T_3(16x_1 - 8x_2 + 24x_3 + 32x_4) \\ &= 48x_1 - 24x_2 + 72x_3 + 96x_4 + 6. \end{aligned}$$

$$\begin{cases} g(x_1, x_2, x_3, x_4) = 2x_1 - x_2 + 3x_3 + 4x_4 - 1 \\ h(x_1, x_2, x_3, x_4) = 48x_1 - 24x_2 + 72x_3 + 96x_4 + 6 \end{cases}$$

*system is created.*
*The receiver $(Y)$ considers the linear Diophantine equation $f(x_1, x_2, x_3, x_4) = 4x_1 + 5x_2 - 7x_3 + 2x_4 - 6$ and its solution $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (2, 1, 1, 0)$.*

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 150 = u \\ g(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 5 = v. \end{aligned}$$

*The receiver $(Y)$ makes $v$ the private key and $u$ the public key.*

*The sender $(X)$ solves $v$ from $u$.*

$$\begin{aligned}
(T_3 \circ T_2 \circ T_1)^{-1}(h(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) &= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(h(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) \\
&= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(150) \\
&= T_1^{-1} \circ T_2^{-1}(\frac{1}{1+2}(150-6)) \\
&= T_1^{-1} \circ T_2^{-1}(48) \\
&= T_1^{-1}(\frac{1}{1+1}(48-4)) \\
&= T_1^{-1}(22) \\
&= \frac{1}{1+3}(22-2) \\
&= 5 \\
&= v
\end{aligned}$$

*So $v$ public secret key can be used as key for key exchange.*

**Example 11.4** *(Encryption-Decryption) Suppose that plaintext $M$ is $CRYPTOLOGY$.*

**Solution 11.2** *For encryption, secret key $v = 5$ construct the key matrix $K = \boldsymbol{C}_5(W)$ using $v = 5th$ order $3-$primes circulant matrix.*

$$K = \boldsymbol{C}_5(W) = \begin{pmatrix} 0 & 1 & 2 & 7 & 25 \\ 25 & 0 & 1 & 2 & 7 \\ 7 & 25 & 0 & 1 & 2 \\ 2 & 7 & 25 & 0 & 1 \\ 1 & 2 & 7 & 25 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} 0 & 1 & 3 & 10 & 35 \end{pmatrix}$$

*The plaintext $M = CRYPTOLOGY$ is divided into blocks each of size $v$ and obtain numerical values*

$M_1 = (CRYPT) = \begin{pmatrix} 2 & 17 & 24 & 15 & 19 \end{pmatrix}$ *and*

$M_2 = (OLOGY) = \begin{pmatrix} 14 & 11 & 14 & 6 & 24 \end{pmatrix}$.

*Encryption:* $C \equiv (MK + B)(\text{mod}\, 41)$

$$
\begin{aligned}
C_1 &= (M_1K + B)(\text{mod}\, 41) \\
&\equiv [\begin{pmatrix} 2 & 17 & 24 & 15 & 19 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 7 & 25 \\ 25 & 0 & 1 & 2 & 7 \\ 7 & 25 & 0 & 1 & 2 \\ 2 & 7 & 25 & 0 & 1 \\ 1 & 2 & 7 & 25 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 3 & 10 & 35 \end{pmatrix}](\text{mod}\, 41) \\
&= \begin{pmatrix} 27 & 8 & 40 & 24 & 21 \end{pmatrix} \sim (1I \;\; YV).
\end{aligned}
$$

*The $C_1$ password corresponding to the $M_1$ block plaintext is* $(1I \;\; YV)$.

$$
\begin{aligned}
C_2 &\equiv (M_2K + B)(\text{mod}\, 41) \\
&\equiv [\begin{pmatrix} 14 & 11 & 14 & 6 & 24 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 7 & 25 \\ 25 & 0 & 1 & 2 & 7 \\ 7 & 25 & 0 & 1 & 2 \\ 2 & 7 & 25 & 0 & 1 \\ 1 & 2 & 7 & 25 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 3 & 10 & 35 \end{pmatrix}](\text{mod}\, 41) \\
&= \begin{pmatrix} 40 & 4 & 32 & 6 & 4 \end{pmatrix} \sim (\ 46GE).
\end{aligned}
$$

*The $C_2$ password corresponding to the $M_2$ block plaintext is* $(\ 46GE)$.

*Cipher-text* $C = (C_1C_2) = (1I \;\; YV \;\; 46GE)$ *and hence* $M : CRYPTOLOGY \longrightarrow C :$ $1I \;\; YV \;\; 46GE$. *$X$ send this cipher-text $C$ to $Y$.*

*Decryption: Receiving ciphertext $C$, $Y$ will calculate decryption key* $K^{-1} = \boldsymbol{C}_5^{-1}(W)$,

*where* $v = 5$.

$$
\begin{aligned}
& K^{-1} \pmod{41} \\
\equiv & \begin{pmatrix}
-\frac{109\,449}{9780\,925} & \frac{390\,036}{9780\,925} & \frac{6296}{9780\,925} & -\frac{6619}{9780\,925} & -\frac{809}{9780\,925} \\
-\frac{809}{9780\,925} & -\frac{109\,449}{9780\,925} & \frac{390\,036}{9780\,925} & \frac{6296}{9780\,925} & -\frac{6619}{9780\,925} \\
-\frac{6619}{9780\,925} & -\frac{809}{9780\,925} & -\frac{109\,449}{9780\,925} & \frac{390\,036}{9780\,925} & \frac{6296}{9780\,925} \\
\frac{6296}{9780\,925} & -\frac{6619}{9780\,925} & -\frac{809}{9780\,925} & -\frac{109\,449}{9780\,925} & \frac{390\,036}{9780\,925} \\
\frac{390\,036}{9780\,925} & \frac{6296}{9780\,925} & -\frac{6619}{9780\,925} & -\frac{809}{9780\,925} & -\frac{109\,449}{9780\,925}
\end{pmatrix} \pmod{41} \\
= & \begin{pmatrix}
24 & 21 & 38 & 38 & 36 \\
36 & 24 & 21 & 38 & 38 \\
38 & 36 & 24 & 21 & 38 \\
38 & 38 & 36 & 24 & 21 \\
21 & 38 & 38 & 36 & 24
\end{pmatrix}
\end{aligned}
$$

*It can easily be seen that*

$$
\begin{aligned}
& \begin{pmatrix}
0 & 1 & 2 & 7 & 25 \\
25 & 0 & 1 & 2 & 7 \\
7 & 25 & 0 & 1 & 2 \\
2 & 7 & 25 & 0 & 1 \\
1 & 2 & 7 & 25 & 0
\end{pmatrix}
\begin{pmatrix}
24 & 21 & 38 & 38 & 36 \\
36 & 24 & 21 & 38 & 38 \\
38 & 36 & 24 & 21 & 38 \\
38 & 38 & 36 & 24 & 21 \\
21 & 38 & 38 & 36 & 24
\end{pmatrix} \pmod{41} \\
\equiv & \begin{pmatrix}
903 & 1312 & 1271 & 1148 & 861 \\
861 & 903 & 1312 & 1271 & 1148 \\
1148 & 861 & 903 & 1312 & 1271 \\
1271 & 1148 & 861 & 903 & 1312 \\
1312 & 1271 & 1148 & 861 & 903
\end{pmatrix} \pmod{41} \\
= & \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}
\end{aligned}
$$

*Decryption takes place as* $P_i \equiv (C_i - B)K^{-1} (\mathrm{mod}\, 41)$

$$
\begin{aligned}
M_1 &\equiv (C_1 - B)K^{-1} (\mathrm{mod}\, 41) \\
&\equiv [\begin{pmatrix} 27 & 8 & 40 & 24 & 21 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 3 & 10 & 35 \end{pmatrix}] \begin{pmatrix} 24 & 21 & 38 & 38 & 36 \\ 36 & 24 & 21 & 38 & 38 \\ 38 & 36 & 24 & 21 & 38 \\ 38 & 38 & 36 & 24 & 21 \\ 21 & 38 & 38 & 36 & 24 \end{pmatrix} (\mathrm{mod}\, 41) \\
&= \begin{pmatrix} 2 & 17 & 24 & 15 & 19 \end{pmatrix} \sim (CRYPT).
\end{aligned}
$$

*The* $M_1$ *plaintext corresponding to the* $C_1$ *password is* $(CRYPT)$.

$$
\begin{aligned}
M_2 &\equiv (C_2 - B)K^{-1} (\mathrm{mod}\, 41) \\
&\equiv [\begin{pmatrix} 40 & 4 & 32 & 6 & 4 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 3 & 10 & 35 \end{pmatrix}] \begin{pmatrix} 24 & 21 & 38 & 38 & 36 \\ 36 & 24 & 21 & 38 & 38 \\ 38 & 36 & 24 & 21 & 38 \\ 38 & 38 & 36 & 24 & 21 \\ 21 & 38 & 38 & 36 & 24 \end{pmatrix} (\mathrm{mod}\, 41) \\
&= \begin{pmatrix} 14 & 11 & 14 & 6 & 24 \end{pmatrix} \sim (OLOGY).
\end{aligned}
$$

*The* $C_2$ *password corresponding to the* $M_2$ *block plaintext is* $(OLOGY)$.
*Thus,* $Y$ *recovered the plaintext* $CRYPTOLOGY$ *sent by* $X$ *successfully.*

## 11.3 COMPLEXITY ANALYSIS AND SECURITY STRENGTH

To compute the common secret key either $v$ or the $2s$ parameters $m_k, n_k$ for all $k = 1, 2, \ldots, s$ in key exchange algorithm and to abtain key matrices $K$ and calculations of $MK + B$ and $(C - B)K^{-1}$ are very difficult. However for X and Y it is quite easy to construct key matrices from $v$-th order $3 - primes$ circulant matrix.

One of the most common attacks in the context of security strength analysis is the Brute force attack [18, 84].

In Example (11.2) , $p = 41$ and $v = 4$, then intruder need to check $41^{16}$ matrices, which is equivalent to $6.3\,759\,030\,914\,653\,054\,346\,432\,641 \times 10^{25}$.

However, we know that

$$|GL_m(W_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \ldots (p^m - p^1)(p^m - 1) \tag{11.1}$$

gives the order of the General Linear group $GL_m$, which consists of all invertible matrices of order $m \times m$ over $W_p$. Our key matrices are invertible. We get

$$\begin{aligned} |GL_4(K_{41})| &= (41^4 - 41^3)(41^4 - 41^2)(41^4 - 41^1)(41^4 - 1) \\ &= 6.2\,166\,004\,473\,116\,489\,379\,84 \times 10^{25}. \end{aligned}$$

In Example (11.4) , $p = 41$ and $v = 5$, then intruder need to check $41^{25}$ matrices, which is equivalent to $2.0\,873\,554\,875\,923\,477\,449\,109\,855\,954\,682\,643\,681\,001 \times 10^{40}$.
Our key matrices are invertible. We get

$$\begin{aligned} |GL_5(K_{41})| &= (41^5 - 41^4)(41^5 - 41^3)(41^5 - 41^2)(41^5 - 41^1)(41^5 - 1) \\ &= 2.0\,352\,026\,622\,286\,237\,622\,737\,800\,936\,665\,088 \times 10^{40}\,. \end{aligned}$$

It is obvious that by making prime $p$ too large, it becomes nearly unbreakable. Also, if we increase the size of key matrix for fixed $p$, then $|GL_m(W_p)| \longrightarrow \infty$, i.e. it depends on $v$ and $p$. The difficulty in obtaining the key matrices is highlighted by this. Furthermore, the method's difficulty makes cracking the password difficult.

# CHAPTER 12

# A NEW APPLICATION TO CRYPTOLOGY USING GENERALIZED FIBONACCI MATRICES, INNER PRODUCT AND SELF-ADJOINT OPERATOR

Recent developments in the field of cryptology have made it an important discipline in both mathematics and computer science and engineering. In mathematics, cryptology is applied in different sub-fields such as algebra, number theory, graph theory, algebraic geometry, probability, and statistics. Analysis of cryptographic security has led to the use of theoretical computer science and complexity theory in particular. Because an important aspect of encryption protocols is their security. That is the ability to withstand attacks. Since modern cryptography is done on a computer, cryptographic security uses on computer science and complexity theory. For more information on complexity theory, see [89].

Most coding algorithms use modular arithmetic. Because in this way, it provides the transformation of the $n$-letter. This shows that cryptography is closely related to number theory. For this see [78,90,91]. For example, Hill-Affine encryption is used a lot with modular arithmetic [78,83-88].

Using the same ideas in Diffie-Hellman and RSA, algebraic geometry began to be used in cryptography to reduce the key space size. Elliptic curves over finite fields and their related groups were suggested as potential cryptographic building blocks by Neil Koblitz [92] in 1985. The majority of the time, these techniques have produced quicker encryption and fewer key gaps than conventional RSA techniques. They have been highly effective. Therefore, significant studies has been done on the application of elliptic curves to cryptology after 1985, see for more information [8,78,93].

In 1995, Lin Chang and Lie proposed the application of Diophantine equations in cryptography. Afterwards, Hary Yosh did cryptography studies on nonlinear Diophantine equations. For studies in this area, see [7,80-82].

In this chapter, we presented a study on the application of functional analysis to cryptography. First, we created a new public key system, that is, a key exchange algorithm, using the inner product and orthogonality. Then, we propose a new cryptography by using the inner product, self adjoint operators, and generalized $m$-step Fibonacci numbers and combining them with the key exchange algorithm we have introduced.

## 12.1 A NEW KEY EXCHANGE ALGORITHM CREATED BETWEEN INNER PRODUCT AND ORTHOGONALITY

1. The sender considers an inner product $f(u) = (a, u) = a_1u_1 + a_2u_2 + \ldots + a_nu_n$, where $a, u \in \mathbb{R}^n$

   The sender generates the operator on the inner product equation given as for $T_i = T_{(c_i,d_i)} = c_if + d_i$, where $c_i, d_i$ parameters and $c_i > 0$, $d_i \in \mathbb{R}$, $\forall i = 1, 2, \ldots, j$.

   The sender generates the public key such that

   $T(f) = T_j \circ T_{j-1} \circ \cdots \circ T_1(f) = g.$

   The sender makes the $f$ and $g$ public.

2. The recipient generates a public key and a secret key. Firstly, the recipient creates $b$ vector.

   The recipient selects an arbitrary vector $v$ such that $(b, v) = 0$, i.e. $b$ and $v$ orthogonal.

   The recipient keeps $f(v) = m$ as the secret key and makes $g(v) = n$ the public key.

3. The sender recovers the secret key $m$ from public key $n$ by applying the inverse of operators $T_i$, where for $T_i$, we have $T_i^{-1} = T_{(c_i,d_i)}^{-1} = \frac{(g)-d_i}{c_i}$.

   The sender from $T_i^{-1}$, the inverse of $T_i$, recovers $m$ from $n$ by

   $(T_j \circ T_{j-1} \circ \cdots \circ T_1)^{-1} = T_1^{-1} \circ T_2^{-1} \circ \cdots \circ T_j^{-1}.$

4. The secret key $m$ evaluated by both sender and receiver is used as the key for key exchange.

## 12.2 ALGORITHMS

Encryption Algorithm:

1. X considers inner product $f$ and generates $g$.

2. X recovers the secret key $m$.

3. X creates $\boldsymbol{F}_m^n \longrightarrow K$ matrix, where $\boldsymbol{F}_m^n$ is the multinacci matrix of order $m \times m$.

4. X calculates $(\boldsymbol{F}_m^n)^* \longrightarrow K^*$, where $(\boldsymbol{F}_m^n)^*$ is an adjoint matrix of $\boldsymbol{F}_m^n$.

5. If $m$ is odd, the key matrix is $KK^* = \mathbb{K}_1$, if $m$ is even, the key matrix is $K^*K = \mathbb{K}_2$.

6. Encryption: $Enc(M) : C_i \leftrightarrow (\mathbb{K}_{1,2}M_i, E_n)(\mathrm{mod}\, 41)$; where $C_i$ is ciphertext, $C_i \in \mathbb{R}$, $M_i$ is plaintext and it is $m \times 1$ column vector and $E_n = (F_n, F_{n+1}, \ldots, F_{n+m-1})$.

$$M_i = \begin{cases} \text{first row} & , \quad i \equiv 1(\mathrm{mod}\, m) \\ \text{second row} & , \quad i \equiv 2(\mathrm{mod}\, m) \\ \vdots & \vdots \\ m\text{-}th & , \quad i \equiv 0(\mathrm{mod}\, m) \end{cases}$$

7. Transmit $(C; E_n)$ to Y.

Decryption Algorithm:

Y, after receiving $(C; E_n)$.

1. If $m$ is odd, the key matrix is $KK^* = \mathbb{K}_1$, if $m$ is even, the key matrix is $K^*K = \mathbb{K}_2$.

2. Decryption: $Dec(C) : M_i \leftrightarrow (M_i, \mathbb{K}_{1,2}^* E_n)(\mathrm{mod}\, 41) = (M_i, \mathbb{K}_{1,2} E_n)(\mathrm{mod}\, 41)$, where $\mathbb{K}_{1,2}$ is self-adjoint. Y recovers $m_i$ from $c_i$, where $m_i$ is the component of $M_i$

Suppose $X$ wants to send message to $Y$. After calculating key matrix $\mathbb{K}$ he will encrypt plaintext $M$ with $\mathbb{K}$ using proposed algorithm above.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 | 1 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ! | ? | | |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

**Example 12.1** *(Public key calculation) X chooses* $a = (2, 1, -5, 3)$ *and* $u = (u_1, u_2, u_3, u_4)$. *So* $f(u) = (a, u) = 2u_1 + u_2 - 5u_3 + 3u_4$. *Let* $T_1 = T_{(2,3)}$, $T_2 = T_{(3,5)}$, $T_3 = T_{(1,-3)}$

$$\begin{aligned} g(u) &= T_3 \circ T_2 \circ T_1(f(u)) \\ &= T_3 \circ T_2 \circ T_1(2u_1 + u_2 - 5u_3 + 3u_4) \\ &= T_3 \circ T_2(4u_1 + 2u_2 - 10u_3 + 6u_4 + 3) \\ &= T_3(12u_1 + 6u_2 - 30u_3 + 18u_4 + 14) \\ &= 12u_1 + 6u_2 - 30u_3 + 18u_4 + 11. \end{aligned}$$

*X makes*

$$\begin{cases} f(u) = 2u_1 + u_2 - 5u_3 + 3u_4 \\ g(u) = 12u_1 + 6u_2 - 30u_3 + 18u_4 + 11 \end{cases}$$

*public.*

*Y considers* $b = (1, 3, -6, 1)$ *and selects an arbitrary vector* $v$ *such that* $(b, v) = 0$.

$((1, 3, -6, 1), (v_1, v_2, v_3, v_4)) = 0.$

*Let* $v = (2, 1, 1, 1)$.

*Y evaluates*

$$\begin{aligned} g(v) &= 29 \\ f(v) &= 3. \end{aligned}$$

*Y keeps* $m = f(v) = 3$ *as secret key, makes* $n = g(v) = 29$ *as public key.*

*X recovers secrete key $m$ from the private key $g(v)$ by applying*

$$\begin{aligned}(T_3 \circ T_2 \circ T_1)^{-1}(n) &= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(29) \\ &= T_1^{-1} \circ T_2^{-1}(29+3) \\ &= T_1^{-1} \circ T_2^{-1}(32) \\ &= T_1^{-1}(\frac{32-5}{3}) \\ &= T_1^{-1}(9) \\ &= \frac{9-3}{2} \\ &= 3 \\ &= m.\end{aligned}$$

**Example 12.2** *(Encryption-Decryption) Suppose plaintext $M$ is $CODE$.*
*For encryption, public key $n = 29$ and secret key $m = 3$. $m$ is odd.*

$$K = \mathcal{F}_3^{29} = \begin{pmatrix} F_{31} & F_{30}+F_{29} & F_{30} \\ F_{30} & F_{29}+F_{28} & F_{29} \\ F_{29} & F_{28}+F_{27} & F_{28} \end{pmatrix} = \begin{pmatrix} 15902591 & 13346834 & 8646064 \\ 8646064 & 7256527 & 4700770 \\ 4700770 & 3945294 & 2555757 \end{pmatrix}.$$

*Key matrix*

$$\begin{aligned}\mathbb{K}_1 &= KK^* = \begin{pmatrix} 15902591 & 13346834 & 8646064 \\ 8646064 & 7256527 & 4700770 \\ 4700770 & 3945294 & 2555757 \end{pmatrix} \begin{pmatrix} 15\,902\,591 & 8646\,064 & 4700\,770 \\ 13\,346\,834 & 7256\,527 & 3945\,294 \\ 8646\,064 & 4700\,770 & 2555\,757 \end{pmatrix} \\ &= \begin{pmatrix} 505\,784\,801\,028\,933 & 274\,989\,639\,106\,622 & 149\,508\,845\,384\,714 \\ 274\,989\,639\,106\,622 & 149\,508\,845\,386\,725 & 81\,286\,316\,536\,108 \\ 149\,508\,845\,384\,714 & 81\,286\,316\,536\,108 & 44\,194\,477\,182\,385 \end{pmatrix} (\mathrm{mod}\,41) \\ &= \begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix}.\end{aligned}$$

*The plaintext $M = CODE$ is divided by each character to form a separate block and obtain numerical values*

$M_1 = (C\ ) = (2\ 0\ 0)$, $M_2 = (O) = (0\ 14\ 0)$, $M_3 = (D) = (0\ 0\ 3)$, $M_4 = (E) = (4\ 0\ 0)$

$E_{29} = (F_{29}, F_{30}, F_{31})$.

*Now let's find the $C$ codes corresponding to the plaintext $M$.*

$$\begin{aligned}
C_1 &= (\begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 22 & 16 & 18 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 22 & 16 & 18 \end{pmatrix}, \begin{pmatrix} 38 & 25 & 3 \end{pmatrix})(\text{mod } 41) \\
&= (836 + 400 + 54)(\text{mod } 41) \\
&= 19 \sim (T).
\end{aligned}$$

*According to the $M_1$ plaintext, $C_1$ is encoded as $(T)$.*

$$\begin{aligned}
C_2 &= (\begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 0 \\ 14 \\ 0 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 112 & 154 & 308 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 30 & 31 & 21 \end{pmatrix}, \begin{pmatrix} 38 & 25 & 3 \end{pmatrix})(\text{mod } 41) \\
&= (1140 + 775 + 63)(\text{mod } 41) \\
&= 10 \sim (K).
\end{aligned}$$

*According to the $M_2$ plaintext, $C_2$ is encoded as $(K)$.*

$$\begin{aligned}
C_3 &= (\begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 27 & 66 & 18 \end{pmatrix}, \begin{pmatrix} 38 & 25 & 3 \end{pmatrix})(\text{mod } 41) \\
&= (\begin{pmatrix} 27 & 25 & 18 \end{pmatrix}, \begin{pmatrix} 38 & 25 & 3 \end{pmatrix})(\text{mod } 41) \\
&= (1026 + 625 + 54)(\text{mod } 41) \\
&= 24 \sim (Y).
\end{aligned}$$

*According to the $M_3$ plaintext, $C_3$ is encoded as $(Y)$.*

$$\begin{aligned} C_4 &= (\begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 4700770 & 8646064 & 15902591 \end{pmatrix})(\mathrm{mod}\, 41) \\ &= (\begin{pmatrix} 3 & 32 & 36 \end{pmatrix}, \begin{pmatrix} 38 & 25 & 3 \end{pmatrix})(\mathrm{mod}\, 41) \\ &= (114 + 800 + 108) \bmod 41 \\ &= 38 \sim (!). \end{aligned}$$

*According to the $M_4$ plaintext, $C_4$ is encoded as $(D)$. Then we get $C = (C_1C_2C_3C_4) = (T\ K\ Y\ !)$.*

*Transmit $(T\ K\ Y\ !; E_{29})$.*

*Decryption: Y, after receiving $(T\ K\ Y\ !; E_{29})$. Now let's solve the codes using the self adjoint and inner product properties.*

$(M_i, \mathbb{K}^*_{1,2}E_n)(\mathrm{mod}\, 41) = (M_i, \mathbb{K}_{1,2}E_n)(\mathrm{mod}\, 41)$

$$\begin{aligned} (\begin{pmatrix} m_1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 38 \\ 25 \\ 3 \end{pmatrix})(\mathrm{mod}\, 41) &= 19 \\ (\begin{pmatrix} m_1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 645 & 645 & 910 \end{pmatrix})(\mathrm{mod}\, 41) &= 19 \\ m_1 &= \frac{19}{645}(\mathrm{mod}\, 41) \\ m_1 &= 2 \sim (C). \end{aligned}$$

*The plaintext of $M_1$ corresponding to the $C_1$ code is $(C)$.*

$$\begin{aligned} (\begin{pmatrix} 0 & m_2 & 0 \end{pmatrix}, \begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 38 \\ 25 \\ 3 \end{pmatrix})(\mathrm{mod}\, 41) &= 10 \\ (\begin{pmatrix} 0 & m_2 & 0 \end{pmatrix}, \begin{pmatrix} 645 & 645 & 910 \end{pmatrix})(\mathrm{mod}\, 41) &= 10 \\ m_2 &= \frac{10}{645}(\mathrm{mod}\, 41) \\ m_2 &= 14 \sim (O). \end{aligned}$$

*The plaintext of $M_2$ corresponding to the $C_2$ code is $(O)$.*

$$
\begin{aligned}
(\begin{pmatrix} 0 & 0 & m_3 \end{pmatrix}, \begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 38 \\ 25 \\ 3 \end{pmatrix})(\mathrm{mod}\, 41) &= 24 \\
(\begin{pmatrix} 0 & 0 & m_3 \end{pmatrix}, \begin{pmatrix} 645 & 645 & 910 \end{pmatrix})(\mathrm{mod}\, 41) &= 24 \\
m_3 &= \frac{24}{910}(\mathrm{mod}\, 41) \\
m_3 &= 3 \sim (D).
\end{aligned}
$$

*The plaintext of $M_3$ corresponding to the $C_3$ code is $(D)$.*

$$
\begin{aligned}
(\begin{pmatrix} m_4 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 11 & 8 & 9 \\ 8 & 11 & 22 \\ 9 & 22 & 6 \end{pmatrix} \begin{pmatrix} 38 \\ 25 \\ 3 \end{pmatrix})(\mathrm{mod}\, 41) &= 38 \\
(\begin{pmatrix} m_4 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 645 & 645 & 910 \end{pmatrix})(\mathrm{mod}\, 41) &= 38 \\
m_4 &= \frac{38}{645}(\mathrm{mod}\, 41) \\
m_4 &= 4 \sim (E).
\end{aligned}
$$

*The plaintext of $M_4$ corresponding to the $C_4$ code is $(E)$. Thus Y recovered the plaintext CODE sent by X succesfully.*

## 12.3 COMPLEXITY ANALYSIS

To compute the common secret key either $n$ or the $2j$ parameters $c_i, d_i$ for all $i = 1, 2, \ldots, j$ in key exchange algorithm and to obtain key matrices $\mathbb{K}_1 = KK^*$, $\mathbb{K}_2 = K^*K$ and calculations of their adjoints are very difficult. Because they involve matrix multiplications of a $(m \times m)$ matrix $\boldsymbol{F}_m$ in to $n$ times. However for X and Y it is quite easy to construct key matrices from the terms of $m$-th order generalized Fibonacci sequence, which reduces the calculations of matrix multiplication as well as that of obtaining its adjoint.

## 12.4 SECURITY STRENGTH AND ANALYSIS

In the context of security strength analysis one of the most popular attack is Brute force attack [18, 84].

To create all conceivable matrices is one method for an adversary (let's say Z) to defeat our suggested method using a brute force attack. Since, we are studying on $F_p$ ($p > 26$ be a prime), Z need to check $p^{m^2}$ matrices.

In example 12.2 , $p = 41$ and $m = 3$, then Z need to check $41^9$ matrices, which is equivalent to $3,27\,381\,934\,393\,961 \times 10^{14}$.

But we are aware that

$$|GL_m(F_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \dots (p^m - p^1)(p^m - 1). \tag{12.1}$$

determines the order of the General Linear group $GL_m$, which consists of all invertible matrices of order $m \times m$ over $F_p$. Our key matrices are invertible and we have

$$\begin{aligned} |GL_3(F_{41})| &= (41^3 - 41^2)(41^3 - 41^1)(41^3 - 1) \\ &= 3.19\,202\,373\,504 \times 10^{14}. \end{aligned}$$

It is clear that making prime $p$ too large is almost unbreakable. Also, if we increase the size of key matrix for fixed $p$, then $|GL_m(F_p)| \longrightarrow \infty$, i.e. it depends on $m$ and $p$. The difficulty in obtaining the key matrices is highlighted by this. Furthermore, the method's difficulty makes cracking the password difficult.

# CHAPTER 13

# A NEW APPLICATION TO CRYPTOLOGY USING GENERALIZED JACOBSTHAL MATRICES, INNER PRODUCT AND SELF-ADJOINT OPERATOR

This chapter has been accepted by the journal and is now in the printing stage. We discussed a study on the use of functional analysis in cryptography in this chapter. First, utilizing the inner product and orthogonality, we developed a new public key system, or key exchange method. Then, using our newly developed key exchange method in conjunction with the inner product, self adjoint operators, and generalized $m$-step Jacobsthal numbers, we suggest a new cryptography.

## 13.1 KEY EXCHANGE ALGORITHM CREATED BETWEEN INNER PRODUCT AND ORTHOGONALITY

1. The sender considers an inner product $f(u) = (a, u) = a_1u_1 + a_2u_2 + \ldots + a_nu_n$, where $a, u \in \mathbb{R}^n$

   The sender generates the operator on the inner product equation given as for $T_i = T_{(c_i,d_i)} = c_if + d_i$, where $c_i, d_i$ parameters and $c_i > 0$, $d_i \in \mathbb{R}$, $\forall i = 1, 2, \ldots, j$.

   The sender generates the public key such that

   $$T(f) = T_j \circ T_{j-1} \circ \cdots \circ T_1(f) = g.$$

   The sender makes the $f$ and $g$ public.

2. The recipient generates a public key and a secret key. Firstly, The recipient creates $b$ vector.

   The recipient selects an arbitrary vector $v$ such that $(b, v) = 0$, i.e. $b$ and $v$ orthogonal.

The recipient keeps $f(v) = m$ as the secret key and makes $g(v) = n$ the public key.

3. The sender recovers the secret key $m$ from public key $n$ by applying the inverse of operators $T_i$, where for $T_i$, we have $T_i^{-1} = T_{(c_i,d_i)}^{-1} = \frac{(g)-d_i}{c_i}$.

   The sender from $T_i^{-1}$, the inverse of $T_i$, recovers $m$ from $n$ by

   $(T_j \circ T_{j-1} \circ \cdots \circ T_1)^{-1} = T_1^{-1} \circ T_2^{-1} \circ \cdots \circ T_j^{-1}$.

4. The secret key $m$ evaluated by both sender and receiver is used for key exchange.

## 13.2 ALGORITHMS

Encryption Algorithm:

1. X considers inner product $f$ and generates $g$.

2. X recovers the secret key $m$.

3. X creates $\boldsymbol{J}_m^n \longrightarrow K$ matrix, where $\boldsymbol{J}_m^n$ is the multinacci matrix of order $m \times m$.

4. X calculates $(\boldsymbol{J}_m^n)^* \longrightarrow K^*$, where $(\boldsymbol{J}_m^n)^*$ is an adjoint matrix of $\boldsymbol{J}_m^n$.

5. If $m$ is odd, the key matrix is $KK^* = \mathbb{K}_1$, if $m$ is even, the key matrix is $K^*K = \mathbb{K}_2$.

6. Encryption: $Enc(M) : C_i \leftrightarrow (\mathbb{K}_{1,2}M_i, E_n)(\mathrm{mod}\, 41)$; where $C_i$ is ciphertext, $C_i \in \mathbb{R}$, $M_i$ is plaintext and it is $m \times 1$ column vector and $E_n = (J_n, J_{n+1}, \ldots, J_{n+m-1})$, where

$$M_i = \begin{cases} \text{first row} & , \quad i \equiv 1(\mathrm{mod}\, m) \\ \text{second row} & , \quad i \equiv 2(\mathrm{mod}\, m) \\ \vdots & \vdots \\ m\text{-}th & , \quad i \equiv 0(\mathrm{mod}\, m) \end{cases}$$

7. Transmit $(C; E_n)$ to Y.

Decryption Algorithm:

Y, after receiving $(C; E_n)$.

1. If $m$ is odd, the key matrix is $KK^* = \mathbb{K}_1$, if $m$ is even, the key matrix is $K^*K = \mathbb{K}_2$.

2. Decryption: $Dec(C) : M_i \leftrightarrow (M_i, \mathbb{K}^*_{1,2}E_n)(\mathrm{mod}\, 41) = (M_i, \mathbb{K}_{1,2}E_n)(\mathrm{mod}\, 41)$, where $\mathbb{K}_{1,2}$ is self-adjoint. Y recovers $m_i$ from $c_i$, where $m_i$ is the component of $M_i$

Suppose $X$ wants to send a message to $Y$. After calculating key matrix $\mathbb{K}$ he will encrypt plaintext $M$ with $\mathbb{K}$ using the proposed algorithm above.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | 0 | 1 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ! | ? | | |
| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

**Example 13.1** *(Public key calculation) X chooses* $a = (2, -3, 1, -4, 3)$ *and* $u = (u_1, u_2, u_3, u_4, u_5)$. *So* $f(u) = (a, u) = 2u_1 - 3u_2 + u_3 - 4u_4 + 3u_5$. *Let* $T_1 = T_{(1,1)}$, $T_2 = T_{(2,-4)}$, $T_3 = T_{(4,-7)}$

$$\begin{aligned} g(u) &= T_3 \circ T_2 \circ T_1(f(u)) \\ &= T_3 \circ T_2 \circ T_1(2u_1 - 3u_2 + u_3 - 4u_4 + 3u_5) \\ &= T_3 \circ T_2(2u_1 - 3u_2 + u_3 - 4u_4 + 3u_5 + 1) \\ &= T_3(4u_1 - 6u_2 + 2u_3 - 8u_4 + 6u_5 - 2) \\ &= 16u_1 - 24u_2 + 8u_3 - 32u_4 + 24u_5 - 15. \end{aligned}$$

*X makes*

$$\begin{cases} f(u) = 2u_1 - 3u_2 + u_3 - 4u_4 + 3u_5 \\ g(u) = 16u_1 - 24u_2 + 8u_3 - 32u_4 + 24u_5 - 15 \end{cases}$$

*public.*

*Y considers* $b = (2, 3, -7, 2, -1)$ *and selects an arbitrary vector* $v$ *such that* $(b, v) = 0$.

$((2, 3, -7, 2, 0), (v_1, v_2, v_3, v_4, v_5)) = 0.$

*Let* $v = (2, 1, 1, 0, 1)$.

*Y evaluates*

$$\begin{aligned} g(v) &= 25 \\ f(v) &= 5. \end{aligned}$$

*Y keeps* $m = f(v) = 5$ *as a secret key, makes* $n = g(v) = 25$ *as a public key.*

*X recovers secrete key* $m$ *from the private key* $g(v)$ *by applying*

$$\begin{aligned}
(T_3 \circ T_2 \circ T_1)^{-1}(n) &= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(25) \\
&= T_1^{-1} \circ T_2^{-1}(\frac{25+7}{4}) \\
&= T_1^{-1} \circ T_2^{-1}(8) \\
&= T_1^{-1}(\frac{8+4}{2}) \\
&= T_1^{-1}(4) \\
&= \frac{6-1}{1} \\
&= 5 \\
&= m
\end{aligned}$$

**Example 13.2** *(Encryption-Decryption) Suppose plaintext* $M$ *is* $KEY$*.*

*For encryption, public key* $n = 25$ *and secret key* $m = 5$*.* $m$ *is odd. We get*

$$\begin{aligned}
K &= \mathcal{J}_5^{25} \\
&= \begin{pmatrix}
J_{28} & J_{27}+J_{26}+J_{25}+2J_{24} & J_{27}+J_{26}+2J_{25} & J_{27}+2J_{26} & 2J_{27} \\
J_{27} & J_{26}+J_{25}+J_{24}+2J_{23} & J_{26}+J_{25}+2J_{24} & J_{26}+2J_{25} & 2J_{26} \\
J_{26} & J_{25}+J_{24}+J_{23}+2J_{22} & J_{25}+J_{24}+2J_{23} & J_{25}+2J_{24} & 2J_{25} \\
J_{25} & J_{24}+J_{23}+J_{22}+2J_{21} & J_{24}+J_{23}+2J_{22} & J_{24}+2J_{23} & 2J_{24} \\
J_{24} & J_{23}+J_{22}+J_{21}+2J_{20} & J_{23}+J_{22}+2J_{21} & J_{23}+2J_{22} & 2J_{23}
\end{pmatrix} \\
&= \begin{pmatrix}
17318417 & 17318416 & 17318415 & 17318417 & 17318418 \\
8659209 & 8659208 & 8659207 & 8659206 & 8659208 \\
4329604 & 4329605 & 4329604 & 4329603 & 4329602 \\
2164801 & 2164803 & 2164804 & 2164803 & 2164802 \\
1082401 & 1082400 & 1082402 & 1082403 & 1082402
\end{pmatrix}.
\end{aligned}$$

*Key matrix*

$$\begin{aligned}
\mathbb{K}_1 &= KK^* = \begin{pmatrix} 17318417 & 17318416 & 17318415 & 17318417 & 17318418 \\ 8659209 & 8659208 & 8659207 & 8659206 & 8659208 \\ 4329604 & 4329605 & 4329604 & 4329603 & 4329602 \\ 2164801 & 2164803 & 2164804 & 2164803 & 2164802 \\ 1082401 & 1082400 & 1082402 & 1082403 & 1082402 \end{pmatrix} \\
&\times \begin{pmatrix} 17\,318\,417 & 8659\,209 & 4329\,604 & 2164\,801 & 1082\,401 \\ 17\,318\,416 & 8659\,208 & 4329\,605 & 2164\,803 & 1082\,400 \\ 17\,318\,415 & 8659\,207 & 4329\,604 & 2164\,804 & 1082\,402 \\ 17\,318\,417 & 8659\,206 & 4329\,603 & 2164\,803 & 1082\,403 \\ 17\,318\,418 & 8659\,208 & 4329\,602 & 2164\,802 & 1082\,402 \end{pmatrix} \pmod{41} \\
&= \begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix}.
\end{aligned}$$

*The plaintext $M = KEY$ is divided by each character to form a separate block and obtain numerical values*

$M_1 = (K\ ) = (10\ 0\ 0\ 0\ 0)$, $M_2 = (E) = (0\ 4\ 0\ 0\ 0)$, $M_3 = (Y) = (0\ 0\ 24\ 0\ 0)$

*and*

$$\begin{aligned}
E_{25} &= (J_{25}, J_{26}, J_{27}, J_{28}, J_{29}) \\
&= \begin{pmatrix} 2164801 & 4329604 & 8659209 & 17318417 & 34636833 \end{pmatrix} \pmod{41} \\
&= \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}.
\end{aligned}$$

*Now let's find the $C$ codes corresponding to the plaintext $M$.*

$$
\begin{aligned}
C_1 &= \left(\begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 10 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= \left(\begin{pmatrix} 13 & 6 & 39 & 29 & 28 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= (13 + 24 + 351 + 493 + 924) (\mathrm{mod}\, 41) \\
&= 1 \sim (B).
\end{aligned}
$$

*According to the $M_1$ plaintext, $C_1$ is encoded as $(B)$.*

$$
\begin{aligned}
C_2 &= \left(\begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= \left(\begin{pmatrix} 27 & 28 & 19 & 11 & 23 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= (27 + 112 + 171 + 187 + 759) (\mathrm{mod}\, 41) \\
&= 26 \sim (0).
\end{aligned}
$$

*According to the $M_2$ plaintext, $C_2$ is encoded as $(0)$.*

$$
\begin{aligned}
C_3 &= \left(\begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 24 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= \left(\begin{pmatrix} 28 & 32 & 40 & 4 & 26 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 9 & 17 & 33 \end{pmatrix}\right) (\mathrm{mod}\, 41) \\
&= (28 + 128 + 360 + 68 + 858) (\mathrm{mod}\, 41) \\
&= 7 \sim (H).
\end{aligned}
$$

*According to the $M_3$ plaintext, $C_3$ is encoded as $(H)$. $C = (C_1C_2C_3) = (B\ 0\ H\ )$. Transmit $(B\ 0\ H\ ; E_{25})$.*

*Decryption: Y, after receiving* $(B\ 0\ H\ ; E_{25})$.

$(M_i, \mathbb{K}^*_{1,2} E_n)(\mathrm{mod}\, 41) = (M_i, \mathbb{K}_{1,2} E_n)(\mathrm{mod}\, 41)$

$$\left(\begin{pmatrix} m_1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 9 \\ 17 \\ 33 \end{pmatrix}\right)(\mathrm{mod}\, 41) = 1$$

$$\Longrightarrow$$

$$\begin{aligned} \left(\begin{pmatrix} m_1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 37 & 27 & 2 & 35 & 38 \end{pmatrix}\right)(\mathrm{mod}\, 41) &= 1 \\ m_1 &= \frac{1}{37}(\mathrm{mod}\, 41) \\ m_1 &= 10 \sim (K). \end{aligned}$$

*The plaintext of* $M_1$ *corresponding to the* $C_1$ *code is* $(K)$.

$$\begin{aligned} \left(\begin{pmatrix} 0 & m_2 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 9 \\ 17 \\ 33 \end{pmatrix}\right)(\mathrm{mod}\, 41) &= 26 \\ \left(\begin{pmatrix} 0 & m_2 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 37 & 27 & 2 & 35 & 38 \end{pmatrix}\right)(\mathrm{mod}\, 41) &= 26 \\ m_2 &= \frac{26}{27}(\mathrm{mod}\, 41) \\ m_2 &= 4 \sim (E). \end{aligned}$$

*The plaintext of* $M_2$ *corresponding to the* $C_2$ *code is* $(E)$.

$$\begin{aligned} \left(\begin{pmatrix} 0 & 0 & m_3 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 30 & 17 & 8 & 7 & 11 \\ 17 & 7 & 15 & 13 & 16 \\ 8 & 15 & 29 & 7 & 25 \\ 7 & 13 & 7 & 39 & 22 \\ 11 & 16 & 25 & 22 & 18 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 9 \\ 17 \\ 33 \end{pmatrix}\right)(\mathrm{mod}\, 41) &= 7 \\ \left(\begin{pmatrix} 0 & 0 & m_3 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 37 & 27 & 2 & 35 & 38 \end{pmatrix}\right)(\mathrm{mod}\, 41) &= 7 \\ m_3 &= \frac{7}{2}(\mathrm{mod}\, 41) \\ m_3 &= 24 \sim (Y). \end{aligned}$$

*The plaintext of $M_3$ corresponding to the $C_3$ code is $(Y)$. Thus Y recovered the plaintext KEY sent by X successfully.*

## 13.3 COMPLEXITY ANALYSIS

To compute the common secret key either $n$ or the $2j$ parameters $c_i, d_i$ for all $i = 1, 2, \ldots, j$ in key exchange algorithm and to abtain key matrices $\mathbb{K}_1 = KK^*$, $\mathbb{K}_2 = K^*K$ and calculations of their adjoints are very difficult. Because they involve matrix multiplications of a $(m \times m)$ matrix $\boldsymbol{J}_m$ in to $n$ times. However for X and Y it is quite easy to construct key matrices from the terms of $m$-th order generalized Jacobsthal sequence, which reduces the calculations of matrix multiplication as well as that of obtaining its adjoint.

## 13.4 SECURITY STRENGTH AND ANALYSIS

In the context of security strength analysis, one of the most popular attacks is the Brute force attack [18, 84].

To create all conceivable matrices is one method for an adversary (let's say Z) to defeat our suggested method using a brute force attack. Since we are studying on $F_p$ ($p > 26$ be a prime), Z needs to check $p^{m^2}$ matrices.

In Example (13.2) , $p = 41$ and $m = 5$, then Z needs to check $41^{25}$ matrices, equivalent to $2,0\,873\,554\,875\,923\,477\,449\,109\,855\,954\,682\,643\,681\,001 \times 10^{40}$.

But we are aware that

$$|GL_m(F_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \ldots (p^m - p^1)(p^m - 1). \tag{13.1}$$

determines the order of the General Linear group $GL_m$, which consists of all invertible matrices of order $m \times m$ over $J_p$. Our key matrices are invertible, and we have

$$\begin{aligned} |GL_5(J_{41})| &= (41^5 - 41^4)(41^5 - 41^3)(41^5 - 41^2)(41^5 - 41)(41^5 - 1) \\ &= 2,0\,352\,026\,622\,286\,237\,622\,737\,800\,936\,665\,088 \times 10^{40}. \end{aligned}$$

It is clear that making prime $p$ too large is almost unbreakable. Also, we observed that it does not depend on $n$, and if we increase the size of the key matrix for fixed $p$, then $|GL_m(J_p)| \longrightarrow \infty$, i.e. it depends on $m$ and $p$. This presents the difficulty of obtaining the key matrices. In addition, the difficulty of the method also makes it difficult to crack the password.

# CHAPTER 14

# A NEW CODING THEORY USING WOODALL NUMBERS, INNER PRODUCT, ADJOINT OPERATOR AND ELLIPTIC CURVES

Elliptic curves have also been extensively used in cryptology in recent years. The reason for the increasing interest in elliptic curves is that they use a smaller key size compared to other key exchange algorithms such as RSA and ElGamal. In other words, elliptic curve cryptography reduces the processing steps. Significant work has been done in elliptic curve cryptography, see [1,5,78,92,94,95].

In this chapter, we found polynomials with rational coefficients that convert Woodall numbers to Woodall numbers. We then construct a key exchange algorithm between linear Diophantine equations and polynomials that converts first-order Woodall numbers to Woodall numbers. Finally, we created a new cryptosystem with Woodall matrices and elliptic curves using the inner product and adjoint operators.

## 14.1 POLYNOMIALS WITH RATIONAL COEFFICIENTS MAPPING FROM WOODALL NUMBERS TO WOODALL NUMBERS

In this section, we will find polynomials with rational coefficients that convert Woodall numbers to Woodall numbers. First, let's give all first-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers.

**Theorem 14.1** *All first-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers are of the form*

$$P_1(x) = \frac{n}{m}2^{r_1}.x + \frac{n}{m}2^{r_1} - 1,$$

*where* $n, m \in \mathbb{Z}^+$ *and* $n - m = r_1 \in \mathbb{Z}$.

Proof. We want to find a polynomial $P_1(x) = a_1x + a_0$ such that $P_1(m.2^m - 1) = n.2^n - 1$ and $n, m \in \mathbb{Z}^+$, $a_1, a_0 \in \mathbb{Q}$.

Note that

$P_1(m.2^m - 1) = n.2^n - 1 \Rightarrow P_1(m.2^m - 1) + 1 = n.2^n$.

Let $Q(x) = P_1(x - 1) + 1$. Here, we get $Q(m.2^m) = n.2^n$. Then, we have

$$\begin{aligned} Q(x) &= P_1(x-1)+1 \\ &= a_1(x-1)+a_0+1 \\ &= a_1x - a_1 + a_0 + 1, \end{aligned}$$

and for $x = m.2^m$,

$$Q(m.2^m) = n.2^n = a_1m - a_1 + a_0 + 1 \Rightarrow m^{-1}2^{-m}Q(m.2^m) = \frac{n}{m}2^{n-m} = a_1 + \frac{a_0 - a_1 + 1}{m.2^m}.$$

If we take $m$ large enough, so for $m \to \infty$ we get $m^{-1}2^{-m}Q(m.2^m) \to a_1$.

$m^{-1}2^{-m}Q(m.2^m) = \frac{n}{m}2^{n-m} = \frac{n}{m}2^{r_1}$, where $n - m = r_1$.

So $a_1 = \frac{n}{m}2^{r_1}$. Also

$$\begin{aligned} (a_0 - a_1 + 1)m^{-1}2^{-m} &= 0 \Rightarrow a_0 - a_1 + 1 = 0 \\ &\Rightarrow a_0 = a_1 - 1 = \frac{n}{m}2^{r_1} - 1. \end{aligned}$$

If $a_1$ and $a_0$ are substituted in the $P_1$ polynomial, we get the expression

$P_1(x) = \frac{n}{m}2^{r_1}.x + \frac{n}{m}2^{r_1} - 1$. □

Now we will give form of all second-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers.

**Theorem 14.2** *All second-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers are of the form*

$$P_2(x) = \frac{n}{m^2}2^{r_2}.x^2 + \frac{n}{m^2}2^{r_2+1}.x + \frac{n}{m^2}2^{r_2} - 1,$$

*where* $n, m \in \mathbb{Z}^+$ *and* $n - 2m = r_2 \in \mathbb{Z}$.

Proof. We want to find a polynomial $P_2(x) = a_2x^2 + a_1x + a_0$ such that $P_2(m.2^m - 1) = n.2^n - 1$ and $n, m \in \mathbb{Z}^+$, $a_2, a_1, a_0 \in \mathbb{Q}$.

Note that

$P_2(m.2^m - 1) = n.2^n - 1 \Rightarrow P_2(m.2^m - 1) + 1 = n.2^n.$

Let $Q(x) = P_2(x - 1) + 1$. Here, we get $Q(m.2^m) = n.2^n$. Then, we obtain

$$\begin{aligned} Q(x) &= a_2(x-1)^2 + a_1(x-1) + a_0 + 1 \\ &= a_2x^2 + (a_1 - 2a_2)x + a_2 - a_1 + a_0 + 1, \end{aligned}$$

and for $x = m.2^m$,

$Q(m.2^m) = n.2^n = a_2(m.2^m)^2 + (a_1 - 2a_2)m.2^m + a_2 - a_1 + a_0 + 1$

$\Rightarrow m^{-2}2^{-2m}Q(m.2^m) = \frac{n}{m^2}2^{n-2m} = a_2 + (a_1 - 2a_2)m^{-1}.2^{-m} + (a_2 - a_1 + a_0 + 1)m^{-2}2^{-2m}.$

If we take $m$ large enough, so for $m \to \infty$ we get $m^{-2}2^{-2m}Q(m.2^m) \to a_2$. So

$a_2 = \frac{n}{m^2}2^{n-2m} = \frac{n}{m^2}2^{r_2}$, where $n - 2m = r_2$.

Also

$(a_1 - 2a_2)m^{-1}.2^{-m} + (a_2 - a_1 + a_0 + 1)m^{-2}2^{-2m} = 0$

$$\begin{aligned} a_1 - 2a_2 &= 0 \text{ and } a_2 - a_1 + a_0 + 1 = 0 \\ &\Rightarrow a_1 = 2a_2 = 2\frac{n}{m^2}2^{r_2} = \frac{n}{m^2}2^{r_2+1} \\ &\Rightarrow a_0 = \frac{n}{m^2}2^{r_2} - 1. \end{aligned}$$

If $a_2, a_1$ and $a_0$ are substituted in the $P_2$ polynomial, we get the expression

$P_2(x) = \frac{n}{m^2}2^{r_2}.x^2 + \frac{n}{m^2}2^{r_2+1}.x + \frac{n}{m^2}2^{r_2} - 1.$ □

We will generalize the above polynomials in the following theorem.

**Theorem 14.3** *All kth-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers are of the form*

$$\begin{aligned} P_k(x) &= \binom{k}{0}\frac{n}{m^k}2^{r_k}.x^k + \binom{k}{1}\frac{n}{m^k}2^{r_k}.x^{k-1} + \binom{k}{2}\frac{n}{m^k}2^{r_k}.x^{k-2} + \cdots \\ &\quad + \binom{k}{k-1}\frac{n}{m^k}2^{r_k}.x + \frac{n}{m^k}2^{r_k} - 1 \end{aligned}$$

*,where* $n, m, k \in \mathbb{Z}^+$ *and* $n - km = r_k \in \mathbb{Z}$.

Proof. We want to find a polynomial $P_k(x) = a_k x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_2x^2 + a_1x + a_0$ such that $P_k(m.2^m - 1) = n.2^n - 1$ and $n, m \in \mathbb{Z}^+$, $a_k, a_{k-1}, a_{k-2}, \ldots, a_0 \in \mathbb{Q}$. Note that

$$P_k(m.2^m - 1) = n.2^n - 1 \Rightarrow P_k(m.2^m - 1) + 1 = n.2^n.$$

Let $Q(x) = P_k(x-1) + 1$. Here, we get $Q(m.2^m) = n.2^n$. Then, we have

$$\begin{aligned}
Q(x) &= a_k(x-1)^k + a_{k-1}(x-1)^{k-1} + \cdots + a_2(x-1)^2 + a_1(x-1) + a_0 + 1 \\
&= a_k[\binom{k}{0}x^k - \binom{k}{1}x^{k-1} + \binom{k}{2}x^{k-2} - \binom{k}{3}x^{k-3} + \cdots + \binom{k}{k}(-1)^k] \\
&\quad + a_{k-1}[\binom{k-1}{0}x^{k-1} - \binom{k-1}{1}x^{k-2} + \binom{k-1}{2}x^{k-3} - \cdots + \binom{k-1}{k-1}(-1)^{k-1}] \\
&\quad + a_{k-2}[\binom{k-2}{0}x^{k-2} - \binom{k-2}{1}x^{k-3} + \cdots + \binom{k-2}{k-2}(-1)^{k-2}] + \cdots \\
&\quad + a_2[\binom{2}{0}x^2 - \binom{2}{1}x + 1] + a_1(x-1) + a_0 + 1.
\end{aligned}$$

If the $Q$ polynomial is rearranged, the following expression is reached.

$$\begin{aligned}
Q(x) &= \binom{k}{0}a_k x^k + [-\binom{k}{1}a_k + \binom{k-1}{0}a_{k-1}]x^{k-1} \\
&\quad + [\binom{k}{2}a_k - \binom{k-1}{1}a_{k-1} + \binom{k-2}{0}a_{k-2}]x^{k-2} \\
&\quad + [-\binom{k}{3}a_k + \binom{k-1}{2}a_{k-1} - \binom{k-2}{1}a_{k-2} + \binom{k-3}{0}a_{k-3}]x^{k-3} + \cdots \\
&\quad + [a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k + 1].
\end{aligned}$$

For $x = m.2^m$,

$$\begin{aligned}
m^{-k}.2^{-km}Q(m.2^m) &= \frac{n}{m^k}.2^{n-km} \\
&= a_k + [-\binom{k}{1}a_k + \binom{k-1}{0}a_{k-1}]m^{-1}.2^{-m} \\
&\quad + [\binom{k}{2}a_k - \binom{k-1}{1}a_{k-1} + \binom{k-2}{0}a_{k-2}]m^{-2}.2^{-2m} \\
&\quad + [-\binom{k}{3}a_k + \binom{k-1}{2}a_{k-1} - \binom{k-2}{1}a_{k-2} + \binom{k-3}{0}a_{k-3}]m^{-3}.2^{-3m} + \cdots \\
&\quad + [a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k + 1]m^{-k}.2^{-km}.
\end{aligned}$$

If we take $m$ large enough, so for $m \to \infty$ we get $m^{-k}.2^{-km}Q(m.2^m) \to a_k$. So

$$a_k = \frac{n}{m^k}2^{n-km} = \frac{n}{m^k}2^{r_k}, \text{ where } n - km = r_k.$$

Also

$$\begin{aligned}
-\binom{k}{1}a_k+\binom{k-1}{0}a_{k-1} &= 0 \Rightarrow a_{k-1}=\binom{k}{1}\frac{n}{m^k}2^{r_k}\\
\binom{k}{2}a_k-\binom{k-1}{1}a_{k-1}+\binom{k-2}{0}a_{k-2} &= 0 \Rightarrow a_{k-2}=\binom{k}{2}\frac{n}{m^k}2^{r_k}\\
-\binom{k}{3}a_k+\binom{k-1}{2}a_{k-1}-\binom{k-2}{1}a_{k-2}+\binom{k-3}{0}a_{k-3} &= 0 \Rightarrow a_{k-3}=\binom{k}{3}\frac{n}{m^k}2^{r_k}\\
&\vdots\\
a_0-a_1+a_2-a_3+\cdots+(-1)^k a_k+1 &= 0 \Rightarrow a_0=\frac{n}{m^k}2^{r_k}-1.
\end{aligned}$$

If $a_k, a_{k-1}, a_{k-2}, \ldots, a_0$ are substituted in the $P_k$ polynomial, we get the expression

$$\begin{aligned}
P_k(x) &= \binom{k}{0}\frac{n}{m^k}2^{r_k}.x^k+\binom{k}{1}\frac{n}{m^k}2^{r_k}.x^{k-1}+\binom{k}{2}\frac{n}{m^k}2^{r_k}.x^{k-2}+\cdots\\
&\quad+\binom{k}{k-1}\frac{n}{m^k}2^{r_k}.x+\frac{n}{m^k}2^{r_k}-1. \ \square
\end{aligned}$$

## 14.2 KEY EXCHANGE ALGORITHM BASED ON THE RELATIONSHIP BETWEEN $j$-VARIABLE LINEAR DIOPHANTINE EQUATIONS AND POLYNOMIALS WITH RATIONAL COEFFICIENTS MAPPING FROM WOODALL NUMBERS TO WOODALL NUMBERS

In this section we will construct a key exchange algorithm based on the relationship between linear diophantine equations with $j$-variables and all first-order polynomials with rational coefficients mapping from Woodall numbers to Woodall numbers.
Key exchange algorithm will be given with the following steps.

1. Public key generation by the sender.

   - The sender considers the linear diophantine equation $g(x_1, x_2, \ldots, x_j)$ and the operator $T$ given as $T(g)=\frac{n}{m}2^r.g+\frac{n}{m}2^r-1$, where $n, m \in \mathbb{Z}^+$ and $n-m=r \in \mathbb{Z}$.
   - Generates public key $h(x_1, x_2, \ldots, x_j)$ as

     $$\underbrace{T\circ T\circ \ldots \circ T}_{s-times}(g) = h(x_1, x_2, \ldots, x_j).$$

   - The sender generates the open diophantine equations of $h$ and $g$.

2. Public key and private key generation by the recipient.

   - The receiver creates a linear Diophantine equation $f(x_1, x_2, \ldots, x_j) = a_1x_1 + a_2x_2 + \ldots + a_jx_j = b$ in $j$-variables for $j > 2$ such that $\gcd(a_1, a_2, \ldots, a_j)$ divides $b$ and selects a random solution $(\alpha_1, \alpha_2, \ldots, \alpha_j)$ of the linear Diophantine equation $f(x_1, x_2, \ldots, x_j) = a_1x_1 + a_2x_2 + \ldots + a_jx_j = b$.
   - The receiver calculates the expressions $h(\alpha_1, \alpha_2, \ldots, \alpha_j) = u$ and $g(\alpha_1, \alpha_2, \ldots, \alpha_j) = v$ according to the $h(x_1, x_2, \ldots, x_j)$ and $g(x_1, x_2, \ldots, x_j)$ public key Diophantine equations.
   - The receiver makes $v$ the private key and $u$ the public key.

3. Resolution of the private key by the sender.

   - The sender decrypts the private key $v$ from the public key $u$ by applying the inverse of the $T$ operator, where $T^{-1} = \frac{m}{n}2^{-r}(h - \frac{n}{m}2^r + 1)$.
   - Solve $v$ from $u$ with the expression $(T \circ T \circ \ldots \circ T)^{-1}(u) = T^{-1} \circ T^{-1} \circ \ldots \circ T^{-1}(u)$.

4. Key exchange

   - $v$ secret key calculated by both sender and receiver can be used as key for key exchange.

## 14.3 ENCRYPTION AND DECRYPTION

### Encryption

1. X considers $g$ and generates $h$.

2. X recovers the secret key $v$.

3. X creates $\boldsymbol{W}_3^v \longrightarrow K$ matrix, where $\boldsymbol{W}_3^v$ is Woodall matrix of order $3 \times 3$.

4. Encryption: $Enc(M) : C_i \leftrightarrow (KM_i, E) (\mathrm{mod}\, 43)$; where $C_i$ is ciphertext, $C_i \in \mathbb{R}$, $M_i$ is plaintext and it is $3 \times 1$ column vector and $E = (R_{3+v}, R_{3+v+1}, R_{3+v+2})$.

5. $M_i = \begin{cases} \text{first row} & , \ i \equiv 1(\text{mod}\,3) \\ \text{second row} & , \ i \equiv 2(\text{mod}\,3) \\ \text{third row} & , \ i \equiv 0(\text{mod}\,3) \end{cases}$

6. Transmit $(C; E)$ to Y.

**Decryption**

Y, after receiving $(C; E)$.

1. Y calculates $(\boldsymbol{W}_3^v)^* \longrightarrow K^*$, where $(\boldsymbol{W}_3^v)^*$ is adjoint matrix of $\boldsymbol{W}_3^v$.

2. Decryption: $Dec(C) : M_i \leftrightarrow (M_i, K^*E)(\text{mod}\,43)$. Y recovers $m_i$ from $c_i$, where $m_i$ is the component of $M_i$

Suppose $X$ wants to send message to $Y$. After calculating key matrix $K$ he will encrypt plaintext $M$ with $K$ using proposed algorithm above.

Let's consider the elliptic curve

$y^2 = x^3 + 5x + 29(\text{mod}\,43)$.

$|E(F_{43})(5, 29)| = 43$, where $|.|$ denotes order of $E(F_{43})(5, 29)$.

The points of this elliptic curve are as follows:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(1, 11)$ | $(1, 32)$ | $(2, 2)$ | $(2, 41)$ | $(6, 19)$ | $(6, 24)$ | $(10, 2)$ | $(10, 41)$ | $(12, 21)$ |
| $(12, 22)$ | $(18, 19)$ | $(18, 24)$ | $(19, 19)$ | $(19, 24)$ | $(21, 8)$ | $(21, 35)$ | $(23, 20)$ | $(23, 23)$ |
| $(24, 16)$ | $(24, 27)$ | $(25, 16)$ | $(25, 27)$ | $(27, 14)$ | $(27, 29)$ | $(29, 15)$ | $(29, 28)$ | $(31, 2)$ |
| $(31, 41)$ | $(33, 21)$ | $(33, 22)$ | $(35, 6)$ | $(35, 37)$ | $(36, 9)$ | $(36, 34)$ | $(37, 16)$ | $(37, 27)$ |
| $(39, 17)$ | $(39, 26)$ | $(41, 21)$ | $(41, 22)$ | $(42, 18)$ | $(42, 25)$ | $\infty$ | | |

Let's create the characters table as follows.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $(1, 11)$ | $(25, 16)$ | $(21, 8)$ | $(29, 28)$ | $(35, 6)$ | $(12, 22)$ | $(10, 41)$ | $(37, 27)$ | $(12, 21)$ |
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ |
| $(39, 17)$ | $(42, 18)$ | $(18, 19)$ | $(31, 41)$ | $(19, 19)$ | $(41, 21)$ | $(6, 19)$ | $(2, 41)$ | $(23, 23)$ |
| $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ |
| $(18, 24)$ | $(36, 9)$ | $(10, 2)$ | $(31, 2)$ | $(27, 29)$ | $(6, 24)$ | $(29, 15)$ | $(2, 2)$ | $(33, 21)$ |
| $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | $0$ |
| $(19, 24)$ | $(25, 27)$ | $(21, 35)$ | $(1, 32)$ | $(39, 26)$ | $(23, 20)$ | $(37, 16)$ | $(24, 16)$ | $(42, 25)$ |
| $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ | $8$ | $9$ |
| $(24, 27)$ | $(36, 34)$ | $(27, 14)$ | $(41, 22)$ | $(33, 22)$ | $(35, 37)$ | $\infty$ | | |
| $.$ | $,$ | $?$ | $-$ | $+$ | $;$ | $*$ | | |

The characters table can be decreased or increased by changing the numbers $a$, $b$ and $p$.

**Example 14.1** *The sender* $g(x_1, x_2, x_3) = 3x_1 - 5x_2 + x_3 - 4$ *take the linear Diophantine equation and let* $m = 1$, $n = 3$, $s = 2$. *So* $n - m = r = 2$ *and* $T = 3.2^2 g + 3.2^2 - 1 = 12g + 11$.

$$\begin{aligned} h(x_1, x_2, x_3) &= T \circ T(g(x_1, x_2, x_3)) \\ &= T \circ T(3x_1 - 5x_2 + x_3 - 4) \\ &= T(36x_1 - 60x_2 + 12x_3 - 37) \\ &= 432x_1 - 720x_2 + 144x_3 - 433. \end{aligned}$$

$$\begin{cases} g(x_1, x_2, x_3) = 3x_1 - 5x_2 + x_3 - 4 \\ h(x_1, x_2, x_3) = 432x_1 - 720x_2 + 144x_3 - 433 \end{cases}$$

*system is created.*

*The receiver considers the linear Diophantine equation* $f(x_1, x_2, x_3) = 4x_1 - 3x_2 + 2x_3 - 17$ *and its solution* $(\alpha_1, \alpha_2, \alpha_3) = (5, 1, 0)$.

$$\begin{aligned} h(\alpha_1, \alpha_2, \alpha_3) &= 1007 = u \\ g(\alpha_1, \alpha_2, \alpha_3) &= 6 = v. \end{aligned}$$

*The receiver makes* $v$ *the private key and* $u$ *the public key.*

*The sender solves* $v$ *from* $u$.

$$\begin{aligned} (T \circ T)^{-1}(h(\alpha_1, \alpha_2, \alpha_3)) &= T^{-1} \circ T^{-1}(h(\alpha_1, \alpha_2, \alpha_3)) \\ &= T^{-1} \circ T^{-1}(1007) \\ &= T^{-1}(\frac{1}{3}.2^{-2}(1007 - 3.2^2 + 1)) \\ &= T^{-1}(83) \\ &= \frac{1}{3}.2^{-2}(83 - 3.2^2 + 1) \\ &= 6 \\ &= v \end{aligned}$$

*So* $v$ *public secret key can be used as key for key exchange.*

**Example 14.2** *(Encryption-Decryption) Suppose plaintext* $M$ *is* $MATH$.

*For encryption, public key* $u = 1007$ *and secret key* $v = 6$.

$$
\begin{aligned}
K &= \boldsymbol{W}_3^6 = \frac{1}{2}\begin{pmatrix} -5R_9+19R_8-16R_7 & 24R_8-92R_7+76R_6 & 4(-5R_8+19R_7-16R_6) \\ -5R_8+19R_7-16R_6 & 24R_7-92R_6+76R_5 & 4(-5R_7+19R_6-16R_5) \\ -5R_7+19R_6-16R_5 & 24R_6-92R_5+76R_4 & 4(-5R_6+19R_5-16R_4) \end{pmatrix} (\text{mod}43) \\
&= \begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix}
\end{aligned}
$$

*The plaintext $M = MATH$ is divided each character to form a separate block and obtain numerical values*

$$
\begin{aligned}
M_1 &= (M) = ((31,41)\ 0\ 0),\ M_2 = (A) = (0\ (1,11)\ 0), \\
M_3 &= (T) = (0\ 0\ (36,9)),\ M_4 = (H) = ((37,27)\ 0\ 0).
\end{aligned}
$$

*According to step 5 in Encryption, $E$ becomes as follows.*

$$
\begin{aligned}
E &= (R_{3+v}, R_{3+v+1}, R_{3+v+2}) = (R_9, R_{10}, R_{11}) \\
&= (4607, 10239, 22527) \bmod 43 \\
&= \begin{pmatrix} 6, & 5, & 38 \end{pmatrix}.
\end{aligned}
$$

*Now let's find the $C$ codes corresponding to the plaintext $M$.*

$$
\begin{aligned}
C_1 &= (\begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix} \begin{pmatrix} (31,41) \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}) \\
&= (\begin{pmatrix} 38.(31,41) & 20.(31,41) & 0.(31,41) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}) \\
&= (\begin{pmatrix} (6,24) & (25,16) & \infty \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}) \\
&= 6.(6,24) + 5.(25,16) + 38.\infty \\
&= (37,27) + (33,21) + \infty \\
&= (29,28) + \infty \\
&= (29,28) \sim (D)
\end{aligned}
$$

*According to the $M_1$ plaintext, $C_1$ is encoded as $(D)$.*

$$
\begin{aligned}
C_2 &= \left(\begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix}\begin{pmatrix} 0 \\ (1,11) \\ 0 \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 12.(1,11) & 24.(1,11) & 20.(1,11) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} (18,19) & (42,18) & (6,24) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= 6.(18,19) + 5.(42,18) + 38.(6,24) \\
&= (10,2) + (37,27) + (10,2) \\
&= (6,24) + (10,2) \\
&= (25,16) \sim (B)
\end{aligned}
$$

*According to the $M_2$ plaintext, $C_2$ is encoded as $(B)$.*

$$
\begin{aligned}
C_3 &= \left(\begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ (36,9) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 37.(36,9) & 0.(36,9) & 24.(36,9) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} (41,21) & \infty & (29,15) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= 6.(41,21) + \infty + 38.(29,15) \\
&= (2,2) + \infty + (42,25) \\
&= (2,2) + (42,25) \\
&= (10,2) \sim (U)
\end{aligned}
$$

*According to the $M_3$ plaintext, $C_3$ is encoded as $(U)$.*

$$\begin{aligned}
C_4 &= \left(\begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix}\begin{pmatrix} (37,27) \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 38.(37,27) & 20.(37,27) & 0.(37,27) \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} (39,26) & (19,24) & \infty \end{pmatrix}, \begin{pmatrix} 6 & 5 & 38 \end{pmatrix}\right) \\
&= 6.(39,26) + 5.(19,24) + 38.\infty \\
&= (18,19) + (12,22) + \infty \\
&= (24,27) + \infty \\
&= (24,27) \sim (.)
\end{aligned}$$

*According to the $M_4$ plaintext, $C_4$ is encoded as $(.)$. As a result, our message is encoded as $C = (C_1C_2C_3C_4) = (D\ B\ U\ .)$. Transmit $(D\ B\ U\ .; E)$.*

*Decryption: Y, after receiving $(D\ B\ U\ .; E)$.*

$$K = \begin{pmatrix} 38 & 12 & 37 \\ 20 & 24 & 0 \\ 0 & 20 & 24 \end{pmatrix} \Longrightarrow K^* = \begin{pmatrix} 38 & 20 & 0 \\ 12 & 24 & 20 \\ 37 & 0 & 24 \end{pmatrix}, \textit{where } m_1, m_2, m_3, m_4 \in E(F_{43})(5,29).$$

*Now let's solve the codes using the adjoint and inner product properties.*

$$\begin{aligned}
\left(\begin{pmatrix} m_1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 38 & 20 & 0 \\ 12 & 24 & 20 \\ 37 & 0 & 24 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \\ 38 \end{pmatrix}\right) \bmod 43 &= (29,28) \\
\left(\begin{pmatrix} m_1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 27 & 6 & 16 \end{pmatrix}\right) &= (29,28) \\
27.m_1 &= (29,28) \\
m_1 &= (31,41) \sim (M)
\end{aligned}$$

$\frac{1}{27} \bmod 43 = 8$, $m_1 = 8.(29,28) = (31,41)$.

*The plaintext of $M_1$ corresponding to the $C_1$ code is $(M)$.*

$$
\begin{aligned}
(\begin{pmatrix} 0 & m_2 & 0 \end{pmatrix}, \begin{pmatrix} 38 & 20 & 0 \\ 12 & 24 & 20 \\ 37 & 0 & 24 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \\ 38 \end{pmatrix}) \bmod 43 &= (25, 16) \\
(\begin{pmatrix} 0 & m_2 & 0 \end{pmatrix}, \begin{pmatrix} 27 & 6 & 16 \end{pmatrix}) &= (25, 16) \\
6.m_2 &= (25, 16) \\
m_2 &= (1, 11) \sim (A)
\end{aligned}
$$

$\frac{1}{6} \bmod 43 = 36$, $m_2 = 36.(25, 16) = (1, 11)$.

*The plaintext of $M_2$ corresponding to the $C_2$ code is $(A)$.*

$$
\begin{aligned}
(\begin{pmatrix} 0 & 0 & m_3 \end{pmatrix}, \begin{pmatrix} 38 & 20 & 0 \\ 12 & 24 & 20 \\ 37 & 0 & 24 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \\ 38 \end{pmatrix}) \bmod 43 &= (10, 2) \\
(\begin{pmatrix} 0 & 0 & m_3 \end{pmatrix}, \begin{pmatrix} 27 & 6 & 16 \end{pmatrix}) &= (10, 2) \\
16.m_3 &= (10, 2) \\
m_3 &= (36, 9) \sim (T)
\end{aligned}
$$

$\frac{1}{16} \bmod 43 = 35$, $m_3 = 35.(10, 2) = (36, 9)$.

*The plaintext of $M_3$ corresponding to the $C_3$ code is $(T)$.*

$$
\begin{aligned}
(\begin{pmatrix} m_4 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 38 & 20 & 0 \\ 12 & 24 & 20 \\ 37 & 0 & 24 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \\ 38 \end{pmatrix}) \bmod 43 &= (24, 27) \\
(\begin{pmatrix} m_4 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 27 & 6 & 16 \end{pmatrix}) &= (24, 27) \\
27.m_4 &= (24, 27) \\
m_4 &= (37, 27) \sim (H)
\end{aligned}
$$

$m_4 = 8.(24, 27) = (37, 27)$.

*The plaintext of $M_4$ corresponding to the $C_4$ code is $(H)$.*

*Thus $Y$ recovered the plaintext $MATH$ sent by $X$ succesfully.*

## 14.4 COMPLEXITY ANALYSIS

It is very difficult to compute the common secret key, either $v$ or the parameters $m$, $n$ in the key exchange algorithm, and to obtain key matrices $K$ and its adjoint, because they require $v$ matrix multiplications of a $(3 \times 3)$ matrix $\boldsymbol{W}_3$. However, for X and Y, it is quite easy to construct 3-$rd$ order key matrices from the terms of the Woodall sequence, and this reduces the calculations of matrix multiplication as well as those of obtaining its adjoint. Also, using elliptic curves when creating the character table makes the work more complicated. Because different character tables can be created using different elliptic curves.

## 14.5 SECURITY STRENGTH AND ANALYSIS

One of the most common attacks in the area of security strength testing is the Brute force attack [18, 84].

To create all conceivable matrices is one method for an adversary (let's say Z) to defeat our suggested method using a brute force attack. Since, we are studying on $F_p$ ($p > 26$ be a prime), Z need to check $p^{m^2}$ matrices.

In Example (14.2), $p = 43$ and $m = 3$, then Z need to check $43^9$ matrices, which is equivalent to $5,02\,592\,611\,936\,843 \times 10^{14}$.

But we are aware that

$$|GL_m(F_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \dots (p^m - p^1)(p^m - 1) \tag{14.1}$$

determines the order of the General Linear group $GL_m$, which consists of all invertible matrices of order $m \times m$ over $F_p$. Our key matrices are invertible and we obtain

$$\begin{aligned} |GL_3(\boldsymbol{W}_{43})| &= (43^3 - 43^2)(43^3 - 43^1)(43^3 - 1) \\ &= 4,90\,632\,743\,395\,872 \times 10^{14}. \end{aligned}$$

Probability of finding the key matrix for $p = 43$ is $2.038\,2 \times 10^{-15}$. It is obvious that if prime $p$ is made too big, it is practically indestructible. Additionally, we noticed that it is independent of $v$ and that if we increase the key matrix's size for a fixed $p$, then $|GL_3(\boldsymbol{W}_p)| \longrightarrow \infty$, i.e. it depends on $p$. This presents the difficulty of obtaining the key matrices. In addition, the difficulty of the method also makes it difficult to crack the password.

# CHAPTER 15

# A NEW CODING ALGORITHM WITH EIGENVALUES AND EIGENVECTORS OF BALANCING MATRICES

In this chapter, we created a new coding and decoding algorithm using the eigenvalues and eigenvectors of the balancing matrices, as well as the Jordan canonical form. For detailed information the Jordan canonical form and on matrix eigenvalues and eigenvectors, see [10, 12, 96].

## 15.1 CODING WITH EIGENVALUES AND EIGENVECTORS OF BALANCING $Q$-MATRICES

Since the matrices we will use are $2 \times 2$, we will divide our $M$ message into blocks of 4 characters. If there are less than 4 characters in the blocks created, we will put point at the end of the block until we complete it with 4 characters.

**Algorithms**

Encryption Algorithm:

1. Create message blocks.

2. Determine the number $n$.

3. Construct a matrix of $M_i$ message blocks.

4. Create the $K = Q_B^n$ key matrix, where $Q_B$ Balancing matrix.

5. Calculate $KM_i = A_i$ matrices.

6. Find the eigenvalues of the $A_i$ matrices and determine an eigenvector corresponding to these eigenvalues.

**a)** Create encrypted message

$$C_i = \begin{bmatrix} \lambda_1 & v_1 \\ \lambda_2 & v_2 \end{bmatrix}_{2\times 3}$$

if matrix $A_i$ can be diagonalized, where $\lambda_1$ and $\lambda_2$ are the eigenvalues, $v_1$ and $v_2$ are the eigenvectors corresponding to these eigenvalues, respectively.

**b)** If matrix $A_i$ is not diagonalizable, find the matrices $P_i$ and $J_i$ using the Jordan canonical form, where $P_i^{-1}A_iP_i = J_i$. Create encrypted message

$$C_i = [J_i, P_i]_{2\times 4}\,.$$

7. Transmit $(n, C)$, where $C$ is obtained by combining $C_i$'s.

Decryption Algorithm:
$(n, C)$, after reaching the person who will decrypt it.

1. **a)** If $C_i$ is of the $2 \times 3$ matrix type, then construct matrices $P_i$ and $D_i$ (diagonal matrix) and determine matrix $A_i$.

   **b)** If $C_i$ is of the $2\times 4$ matrix type, then construct matrices $P_i$ and $J_i$ and determine matrix $A_i$.

2. Calculate matrix $M_i = K^{-1}A_i$.

3. Create the $M$ message, where $M$ is obtained by combining $M_i$'s.

Suppose that $X$ wants to send a message to $Y$. After calculating key matrix $K$, he will encrypt plaintext $M$ with $K$ using the proposed algorithm above. Let's create the characters table as follows, where $n$ is the number of blocks of the encrypted message to be sent.

| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ |
|---|---|---|---|---|---|---|---|---|---|
| $n+4$ | $n+11$ | $n+19$ | $n$ | $n+46$ | $n+26$ | $n+42$ | $n+31$ | $n+15$ | $n+1$ |
| $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ |
| $n+5$ | $n+28$ | $n+12$ | $n+37$ | $n+20$ | $n+35$ | $n+3$ | $n+16$ | $n+29$ | $n+8$ |
| $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |  | 0 | 1 | 2 |
| $n+13$ | $n+24$ | $n+2$ | $n+17$ | $n+44$ | $n+41$ | $n+21$ | $n+38$ | $n+32$ | $n+14$ |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ? |
| $n+9$ | $n+22$ | $n+43$ | $n+40$ | $n+36$ | $n+45$ | $n+25$ | $n+33$ | $n+18$ | $n+7$ |
| ! | ; | + | − | × | ÷ | = |  |  |  |
| $n+30$ | $n+39$ | $n+10$ | $n+23$ | $n+34$ | $n+27$ | $n+6$ |  |  |  |

**Example 15.1** *Let the plaintext be* $M = (MATHEMATICS.)$.

***Encryption***

*First, let's create the message blocks.* $M_1 = (MATH)$, $M_2 = (EMAT)$, $M_3 = (ICS.)$. *Since the number of blocks is* 3, $n = 3$. *Message block matrices are*

$$M_1 = \begin{pmatrix} M & A \\ T & H \end{pmatrix} = \begin{pmatrix} 15 & 7 \\ 11 & 34 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} E & M \\ A & T \end{pmatrix} = \begin{pmatrix} 49 & 15 \\ 7 & 11 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} I & C \\ S & . \end{pmatrix} = \begin{pmatrix} 18 & 22 \\ 32 & 36 \end{pmatrix}.$$

*Now let's create the* $K$ *key matrix.*

$$K = Q_B^3 = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}.$$

*Let's find the* $C$ *code corresponding the plaintext* $M$. *We get*

$$KM_1 = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix} \begin{pmatrix} 15 & 7 \\ 11 & 34 \end{pmatrix} = \begin{pmatrix} 2675 & 238 \\ 459 & 41 \end{pmatrix} = A_1.$$

*The eigenvalues of the matrix* $A_1$ *are* $\lambda_1 = 1358 - 3\sqrt{204\,859}$, $\lambda_2 = 3\sqrt{204\,859} + 1358$. *If the eigenvector* $\begin{pmatrix} \frac{439}{153} - \frac{1}{153}\sqrt{204\,859} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_1$ *is taken, and the eigenvector*

$\begin{pmatrix} \frac{1}{153}\sqrt{204\,859}+\frac{439}{153} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_2$ *is taken, the plaintext* $M_1$ *is encrypted as*

$$C_1 = \begin{pmatrix} 1358-3\sqrt{204\,859} & \frac{439}{153}-\frac{1}{153}\sqrt{204\,859} & 1 \\ 3\sqrt{204\,859}+1358 & \frac{1}{153}\sqrt{204\,859}+\frac{439}{153} & 1 \end{pmatrix}.$$

*For* $M_2$*, we have*

$$KM_2 = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}\begin{pmatrix} 49 & 15 \\ 7 & 11 \end{pmatrix} = \begin{pmatrix} 9751 & 2675 \\ 1673 & 459 \end{pmatrix} = A_2.$$

*The eigenvalues of the matrix* $A_2$ *are* $\lambda_1 = \sqrt{26\,060\,591}+5105$, $\lambda_2 = 5105-\sqrt{26\,060\,591}$. *If the eigenvector* $\begin{pmatrix} \frac{1}{1673}\sqrt{26\,060\,591}+\frac{4646}{1673} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_1$ *is taken, and the eigenvector* $\begin{pmatrix} \frac{4646}{1673}-\frac{1}{1673}\sqrt{26\,060\,591} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_2$ *is taken, the plaintext* $M_2$ *is encrypted as*

$$C_2 = \begin{pmatrix} \sqrt{26\,060\,591}+5105 & \frac{1}{1673}\sqrt{26\,060\,591}+\frac{4646}{1673} & 1 \\ 5105-\sqrt{26\,060\,591} & \frac{4646}{1673}-\frac{1}{1673}\sqrt{26\,060\,591} & 1 \end{pmatrix}.$$

*For* $M_3$*, we obtain*

$$KM_3 = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}\begin{pmatrix} 18 & 22 \\ 32 & 36 \end{pmatrix} = \begin{pmatrix} 2552 & 3228 \\ 438 & 554 \end{pmatrix} = A_3.$$

*The eigenvalues of the matrix* $A_3$ *are* $\lambda_1 = 1553-3\sqrt{267\,985}$, $\lambda_2 = 3\sqrt{267\,985}+1553$. *If the eigenvector* $\begin{pmatrix} \frac{333}{146}-\frac{1}{146}\sqrt{267\,985} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_1$ *is taken, and the eigenvector* $\begin{pmatrix} \frac{1}{146}\sqrt{267\,985}+\frac{333}{146} \\ 1 \end{pmatrix}$ *corresponding to* $\lambda_2$ *is taken, the plaintext* $M_3$ *is encrypted as*

$$C_3 = \begin{pmatrix} 1553-3\sqrt{267\,985} & \frac{333}{146}-\frac{1}{146}\sqrt{267\,985} & 1 \\ 3\sqrt{267\,985}+1553 & \frac{1}{146}\sqrt{267\,985}+\frac{333}{146} & 1 \end{pmatrix}.$$

*As a result, message* $M$ *is sent as* $(3, C)$*, where* $C = (C_1C_2C_3)$.

***Decryption***

*After obtaining the $(3, C)$ cipher, $Y$ simply creates the*

$$P_1 = \begin{pmatrix} \frac{439}{153} - \frac{1}{153}\sqrt{204\,859} & \frac{1}{153}\sqrt{204\,859} + \frac{439}{153} \\ 1 & 1 \end{pmatrix},$$

$$P_1^{-1} = \begin{pmatrix} -\frac{153}{409\,718}\sqrt{204\,859} & \frac{439}{409\,718}\sqrt{204\,859} + \frac{1}{2} \\ \frac{153}{409\,718}\sqrt{204\,859} & \frac{153}{409\,718}\sqrt{204\,859}\left(\frac{1}{153}\sqrt{204\,859} - \frac{439}{153}\right) \end{pmatrix},$$

*and*

$$D_1 = \begin{pmatrix} 1358 - 3\sqrt{204\,859} & 0 \\ 0 & 3\sqrt{204\,859} + 1358 \end{pmatrix}$$

*matrices. Using the $P_1$, $P_1^{-1}$, and $D_1$ matrices, we obtain*

$$\begin{aligned} & P_1 D_1 P_1^{-1} \\ = & \begin{pmatrix} \frac{439}{153} - \frac{1}{153}\sqrt{204\,859} & \frac{1}{153}\sqrt{204\,859} + \frac{439}{153} \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1358 - 3\sqrt{204\,859} & 0 \\ 0 & 3\sqrt{204\,859} + 1358 \end{pmatrix} \\ & \times \begin{pmatrix} -\frac{153}{409\,718}\sqrt{204\,859} & \frac{439}{409\,718}\sqrt{204\,859} + \frac{1}{2} \\ \frac{153}{409\,718}\sqrt{204\,859} & \frac{153}{409\,718}\sqrt{204\,859}\left(\frac{1}{153}\sqrt{204\,859} - \frac{439}{153}\right) \end{pmatrix} \\ = & \begin{pmatrix} 2675 & 238 \\ 459 & 41 \end{pmatrix} \\ = & A_1. \end{aligned}$$

*The inverse of the $K$ key matrix is* $K^{-1} = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}^{-1} = \begin{pmatrix} -6 & 35 \\ -35 & 204 \end{pmatrix}$. *We get*

$$K^{-1}A_1 = \begin{pmatrix} -6 & 35 \\ -35 & 204 \end{pmatrix} \begin{pmatrix} 2675 & 238 \\ 459 & 41 \end{pmatrix} = \begin{pmatrix} 15 & 7 \\ 11 & 34 \end{pmatrix} = M_1.$$

$$M_1 = \begin{pmatrix} 15 & 7 \\ 11 & 34 \end{pmatrix} \Rightarrow M_1 = (MATH).$$

*As a result, we get the plaintext $M_1 = (MATH)$, corresponding to the $C_1$ cipher.*

*Let's find the plaintext $M_2$ corresponding to $C_2$.*

$$P_2 = \begin{pmatrix} \frac{1}{1673}\sqrt{26\,060\,591} + \frac{4646}{1673} & \frac{4646}{1673} - \frac{1}{1673}\sqrt{26\,060\,591} \\ 1 & 1 \end{pmatrix},$$

$$P_2^{-1} = \begin{pmatrix} \frac{1673}{52\,121\,182}\sqrt{26\,060\,591} & \frac{1}{2} - \frac{2323}{26\,060\,591}\sqrt{26\,060\,591} \\ -\frac{1673}{52\,121\,182}\sqrt{26\,060\,591} & \frac{1673}{52\,121\,182}\sqrt{26\,060\,591}\left(\frac{1}{1673}\sqrt{26\,060\,591} + \frac{4646}{1673}\right) \end{pmatrix},$$

*and*

$$D_2 = \begin{pmatrix} \sqrt{26\,060\,591} + 5105 & 0 \\ 0 & 5105 - \sqrt{26\,060\,591} \end{pmatrix}$$

*matrices are created. Using the* $P_2$, $P_2^{-1}$, *and* $D_2$ *matrices, we obtain*

$$\begin{aligned} & P_2 D_2 P_2^{-1} \\ = & \begin{pmatrix} \frac{1}{1673}\sqrt{26\,060\,591} + \frac{4646}{1673} & \frac{4646}{1673} - \frac{1}{1673}\sqrt{26\,060\,591} \\ 1 & 1 \end{pmatrix} \\ & \times \begin{pmatrix} \sqrt{26\,060\,591} + 5105 & 0 \\ 0 & 5105 - \sqrt{26\,060\,591} \end{pmatrix} \\ & \times \begin{pmatrix} \frac{1673}{52\,121\,182}\sqrt{26\,060\,591} & \frac{1}{2} - \frac{2323}{26\,060\,591}\sqrt{26\,060\,591} \\ -\frac{1673}{52\,121\,182}\sqrt{26\,060\,591} & \frac{1673}{52\,121\,182}\sqrt{26\,060\,591}\left(\frac{1}{1673}\sqrt{26\,060\,591} + \frac{4646}{1673}\right) \end{pmatrix} \\ = & \begin{pmatrix} 9751 & 2675 \\ 1673 & 459 \end{pmatrix} \\ = & A_2. \end{aligned}$$

$$K^{-1}A_2 = \begin{pmatrix} -6 & 35 \\ -35 & 204 \end{pmatrix}\begin{pmatrix} 9751 & 2675 \\ 1673 & 459 \end{pmatrix} = \begin{pmatrix} 49 & 15 \\ 7 & 11 \end{pmatrix} = M_2$$

*is obtained by using the* $K^{-1} = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}^{-1} = \begin{pmatrix} -6 & 35 \\ -35 & 204 \end{pmatrix}$ *matrix, which is the inverse of the* $K$ *matrix. Consequently,*

$$M_2 = \begin{pmatrix} 49 & 15 \\ 7 & 11 \end{pmatrix} \Rightarrow M_2 = (EMAT).$$

*Let's find the plaintext* $M_3$ *corresponding to* $C_3$.

$$\begin{aligned} P_3 &= \begin{pmatrix} \frac{333}{146} - \frac{1}{146}\sqrt{267\,985} & \frac{1}{146}\sqrt{267\,985} + \frac{333}{146} \\ 1 & 1 \end{pmatrix}, \\ P_3^{-1} &= \begin{pmatrix} -\frac{73}{267\,985}\sqrt{267\,985} & \frac{333}{535\,970}\sqrt{267\,985} + \frac{1}{2} \\ \frac{73}{267\,985}\sqrt{267\,985} & \frac{73}{267\,985}\sqrt{267\,985}\left(\frac{1}{146}\sqrt{267\,985} - \frac{333}{146}\right) \end{pmatrix}, \end{aligned}$$

*and*

$$D_3 = \begin{pmatrix} 1553 - 3\sqrt{267\,985} & 0 \\ 0 & 3\sqrt{267\,985} + 1553 \end{pmatrix}$$

*matrices are created. Using the $P_3$, $P_3^{-1}$, and $D_3$ matrices, we have*

$$\begin{aligned}
& P_3 D_3 P_3^{-1} \\
= & \begin{pmatrix} \frac{333}{146} - \frac{1}{146}\sqrt{267\,985} & \frac{1}{146}\sqrt{267\,985} + \frac{333}{146} \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1553 - 3\sqrt{267\,985} & 0 \\ 0 & 3\sqrt{267\,985} + 1553 \end{pmatrix} \\
& \times \begin{pmatrix} -\frac{73}{267\,985}\sqrt{267\,985} & \frac{333}{535\,970}\sqrt{267\,985} + \frac{1}{2} \\ \frac{73}{267\,985}\sqrt{267\,985} & \frac{73}{267\,985}\sqrt{267\,985}\left(\frac{1}{146}\sqrt{267\,985} - \frac{333}{146}\right) \end{pmatrix} \\
= & \begin{pmatrix} 2552 & 3228 \\ 438 & 554 \end{pmatrix} \\
= & A_3.
\end{aligned}$$

$$K^{-1}A_3 = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}\begin{pmatrix} 118 & 138 \\ 68 & 80 \end{pmatrix} = \begin{pmatrix} 18 & 22 \\ 32 & 36 \end{pmatrix} = M_3$$

*is obtained by using the* $K^{-1} = \begin{pmatrix} 204 & -35 \\ 35 & -6 \end{pmatrix}^{-1} = \begin{pmatrix} -6 & 35 \\ -35 & 204 \end{pmatrix}$ *matrix, which is the inverse of the $K$ matrix. Consequently,*

$$M_3 = \begin{pmatrix} 18 & 22 \\ 32 & 36 \end{pmatrix} \Rightarrow M_3 = (ICS.).$$

*If $M_1$, $M_2$, $M_3$ are combined, the encrypted message is successfully decrypted. So, $Y$ gets message $M = (MATHEMATICS.)$.*

**Example 15.2** *Let the plaintext be $M = (JKI; QA \div .)$.*

***Encryption***

*First, let's create the message blocks. $M_1 = (JKI;)$ and $M_2 = (QA \div .)$. Since the number of blocks is 2, $n = 2$. Message block matrices are*

$$\begin{aligned}
M_1 &= \begin{pmatrix} J & K \\ I & ; \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 17 & 41 \end{pmatrix}, \\
M_2 &= \begin{pmatrix} Q & A \\ \div & . \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 29 & 35 \end{pmatrix}.
\end{aligned}$$

*Now let's create the $K$ key matrix.*

$$K = Q_B^2 = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 35 & -6 \\ 6 & -1 \end{pmatrix}.$$

*Let's find the $C$ code corresponding the plaintext $M$. We have*

$$KM_1 = \begin{pmatrix} 35 & -6 \\ 6 & -1 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 17 & 41 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} = A_1.$$

*Let* $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ *be the eigenvector corresponding to the eigenvalue $\lambda_1 = 2$. $A_1$ matrix cannot be diagonalized. So let's use the Jordan canonical form. We get*

$$\left( \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} - 2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 - \alpha_2 \\ \alpha_1 - \alpha_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
$$\Rightarrow \quad \alpha_1 - \alpha_2 = 1.$$

*If we take $\alpha_2 = 0$, then $\alpha_1 = 1$, and we have*

$$P_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \; P_1^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}.$$

*Using the $P_1$, $P_1^{-1}$, and $A_1$ matrices, we obtain*

$$P_1^{-1} A_1 P_1 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = J_1.$$

*The plaintext $M_1$ is encrypted as*

$$C_1 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix}.$$

*For $M_2$, we have*

$$KM_2 = \begin{pmatrix} 35 & -6 \\ 6 & -1 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 29 & 35 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = A_2.$$

*Let* $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ *be the eigenvector corresponding to the eigenvalue $\lambda_1 = 1$. $A_2$ matrix cannot be diagonalized. So let's use the Jordan canonical form. We get*

$$\left( \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - 1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\Rightarrow \quad \alpha_1 = 1.$$

*Let $\alpha_2 = 2$, then we have*

$$P_2 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \; P_2^{-1} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}.$$

*Using the $P_2$, $P_2^{-1}$, and $A_2$ matrices, we get*

$$P_2^{-1}A_2P_2 = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = J_2.$$

*The plaintext $M_2$ is encrypted as*

$$C_2 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}.$$

*Transmit* $(2,\ C_1C_2)$.

***Decryption***

*After obtaining the $(2, C_1C_2)$ cipher, we simply calculates*

$$P_1J_1P_1^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} = A_1.$$

*Then using the $K^{-1}$ matrice, we obtain*

$$M_1 = \begin{pmatrix} 35 & -6 \\ 6 & -1 \end{pmatrix}^{-1}\begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 17 & 41 \end{pmatrix}.$$

*Consequently,* $M_1 = \begin{pmatrix} 3 & 7 \\ 17 & 41 \end{pmatrix} \Rightarrow M_1 = (JKI;)$.

*Let's find the plaintext $M_2$ corresponding to $C_2$. We get*

$$P_2J_2P_2^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = A_2.$$

*Then using the $K^{-1}$ matrice, we have*

$$M_2 = \begin{pmatrix} 35 & -6 \\ 6 & -1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 29 & 35 \end{pmatrix}.$$

*Consequently,* $M_2 = \begin{pmatrix} 5 & 6 \\ 29 & 35 \end{pmatrix} \Rightarrow M_2 = (QA \div .)$. *If $M_1$ and $M_2$ are combined, the encrypted message is successfully decrypted and we get message* $M = M_1M_2 = (JKI; QA \div .)$.

## 15.2 SECURITY STRENGTH AND ANALYSIS

One of the most common attacks in the area of security strength testing is the Brute force attack [18, 84].

To create all conceivable matrices is one method for an adversary (let's say Z) to defeat our suggested method using a brute force attack. Since, we are studying on $F_p$ ($p > 26$ be a prime), Z need to check $p^{m^2}$ matrices.

In Example (15.1), $p = 47$ and $m = 2$, then Z need to check $47^4 = 4879\,681$ matrices, which is equivalent to $4,879\,681 \times 10^6$.

But we are aware that

$$|GL_m(F_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \dots (p^m - p^1)(p^m - 1). \tag{15.1}$$

determines the order of the General Linear group $GL_m$, which consists of all invertible matrices of order $m \times m$ over $F_p$. Our key matrices are invertible and we obtain

$$\begin{aligned} |GL_2(K_{47})| &= (47^2 - 47^1)(47^2 - 1) \\ &= 4,773\,696 \times 10^6. \end{aligned}$$

Probability of finding the key matrix for $p = 47$ is $2.094\,8 \times 10^{-7}$. It is obvious that if prime $p$ is made too big, it is practically indestructible. Additionally, we noticed that it is independent of $n$ and that if we increase the key matrix's size for a fixed $p$, then $|GL_2(K_p)| \longrightarrow \infty$, i.e. it depends on $p$.

In addition, it is difficult to find the eigenvalues of the A matrices formed by transforming the message blocks with the key matrix K and then find the eigenvectors corresponding to these eigenvalues. Moreover, the fact that each eigenvalue corresponds to more than one eigenvector means endless trials. That is, the probability of finding the right vectors approaches zero. On the other hand, if A matrices are not diagonalizable, the Jordan Canonical form will be used. This provides a separate difficulty in calculations, see Example (15.2). This makes it difficult or even nearly impossible to crack the password.

# CHAPTER 16

# A NEW CODING ALGORITHM USING FIBONACCI NUMBERS, LINEAR MAPPINGS, AND CHANGE OF BASIS

In this chapter, we will first create a symmetric encryption algorithm by making linear transformations from $\mathbb{R}^2$ to $\mathbb{R}^2$, Fibonacci numbers, and transitioning from the standard base of $\mathbb{R}^2$ to a base we have determined. Later, we will complicate this algorithm a little more and add a key exchange algorithm to create an asymmetric encryption algorithm.

## 16.1 CODING ALGORITHM USING FIBONACCI NUMBERS, LINEAR MAPPINGS, AND CHANGE OF BASIS

Since we will use linear mappings $\mathbb{R}^2 \to \mathbb{R}^2$, we will divide our $M$ message into 4-character blocks. If there is a block with less than 4 characters, we will leave a space at the end of the block until we complete it to 4 characters.

**Algorithms**

Encryption Algorithm

1. Create message blocks.

2. Determine the number $n$.

3. Determine the values corresponding to the characters in the $M_i$ message blocks.

4. Place the values in the message blocks such that they are the coefficients of the linear mapping $M_i : \mathbb{R}^2 \to \mathbb{R}^2$.

5. Construct the $E = \{(1,0),(0,1)\}$ standard base and the $S = \{(F_{n+1}, F_n),(F_n, F_{n-1})\}$ base.

6. Find the base change matrix $P$ from $E$ to $S$ and $P^{-1}$ matrix.

7. Calculate matrix $[M_i]_E$ based on base $E$.

8. Calculate matrix $[M_i]_S = P^{-1}[M_i]_E P$, where $[M_i]_S$ is the matrix with respect to the base $S$.

9. Construct the encrypted message $C_i(x, y)$ so that the inputs of the $[M_i]_S$ matrix are the coefficients of the $C_i : \mathbb{R}^2 \to \mathbb{R}^2$ linear mapping.

10. Transmit $[n, C]$, where $C$ is obtained by combining $C_i$'s.

Decryption Algorithm
$[n, C]$, after reaching the person who will decrypt it.

1. Build $[M_i]_S$ using $C_i(x, y)$.

2. Construct the base change matrix $P$ and its inverse $P^{-1}$.

3. Calculate matrix $[M_i]_E = P[M_i]_S P^{-1}$.

4. Create the $M_i : \mathbb{R}^2 \to \mathbb{R}^2$ linear mapping and the $M_i$ block.

5. Create the $M$ message, where $M$ is obtained by combining $M_i$'s.

Suppose that $X$ wants to send a message to $Y$. Let's create the characters table as follows, where $n$ is the number of blocks of the encrypted message to be sent.

| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ |
|---|---|---|---|---|---|---|---|---|---|
| $n^2+4$ | $n^2+11$ | $n^2+19$ | $n^2$ | $n^2+46$ | $n^2+26$ | $n^2+42$ | $n^2+31$ | $n^2+15$ | $n^2+1$ |
| $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ |
| $n^2+5$ | $n^2+28$ | $n^2+12$ | $n^2+37$ | $n^2+20$ | $n^2+35$ | $n^2+3$ | $n^2+16$ | $n^2+29$ | $n^2+8$ |
| $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | | 0 | 1 | 2 |
| $n^2+13$ | $n^2+24$ | $n^2+2$ | $n^2+17$ | $n^2+44$ | $n^2+41$ | $n^2+21$ | $n^2+38$ | $n^2+32$ | $n^2+14$ |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | . | , | ? |
| $n^2+9$ | $n^2+22$ | $n^2+43$ | $n^2+40$ | $n^2+36$ | $n^2+45$ | $n^2+25$ | $n^2+33$ | $n^2+18$ | $n^2+7$ |
| ! | ; | + | − | × | ÷ | = | | | |
| $n^2+30$ | $n^2+39$ | $n^2+10$ | $n^2+23$ | $n^2+34$ | $n^2+27$ | $n^2+6$ | | | |

**Example 16.1** *Let the plaintext be* $M = (EXAMPLE.)$.

***Encryption***

*First, let's create the message blocks.* $M_1 = (EXAM)$, $M_2 = (PLE.)$. *Since the number of blocks is* 2, $n = 2$. *The values corresponding to the message blocks are* $M_1 = (50, 21, 8, 16)$, $M_2 = (39, 32, 50, 37)$. *Now let's determine the* $C$ *ciphertext corresponding to* $M$.

*Let's find* $C_1$ *first. The linear mapping* $M_1(x, y)$ *representing the* $M_1$ *block is* $M_1(x, y) = (50x + 21y, 8x + 16y)$. *Since* $n = 2$, *we have bases*

$$E = \{(1, 0), (0, 1)\} \text{ and } S = \{(F_3, F_2), (F_2, F_1)\} = \{(2, 1), (1, 1)\}.$$

*We get*

$$P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

*as the base change matrix from* $E$ *to* $S$. *We obtain the following calculations*

$$P^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \ [M_1]_E = \begin{pmatrix} 50 & 21 \\ 8 & 16 \end{pmatrix}$$

*and*

$$[M_1]_S = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 50 & 21 \\ 8 & 16 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 89 & 47 \\ -57 & -23 \end{pmatrix}.$$

*As a result,* $M_1$ *is encoded as* $C_1(x, y) = (89x + 47y, -57x - 23y)$.

*Let's find the* $C_2$ *encrypted message corresponding to* $M_2$. *The linear mapping* $M_2(x, y)$ *representing the* $M_2$ *block is* $M_2(x, y) = (39x + 32y, 50x + 37y)$. *We have*

$$P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \ P^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \ [M_2]_E = \begin{pmatrix} 39 & 32 \\ 50 & 37 \end{pmatrix},$$

*and*

$$[M_2]_S = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 39 & 32 \\ 50 & 37 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -27 & -16 \\ 164 & 103 \end{pmatrix}.$$

$M_2$ *is encoded as* $C_2(x, y) = (-27x - 16y, 164x + 103y)$.

*Transmit* $[2, \begin{pmatrix} 89x + 47y, -57x - 23y \\ 39x + 32y, 50x + 37y \end{pmatrix}]$.

***Decryption***

*Let's find $M_1$ by decoding the $C_1$ code. We obtain the following calculations*

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 89 & 47 \\ -57 & -23 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 50 & 21 \\ 8 & 16 \end{pmatrix} = [M_1]_E$$

*and*

$M_1(x, y) = (50x + 21y, 8x + 16y)$.

*So our plaintext is resolved as $M_1 = (50, 21, 8, 16) = (EXAM)$.*
*Let's find $M_2$ by decoding the $C_2$ code. We get*

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -27 & -16 \\ 164 & 103 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 39 & 32 \\ 50 & 37 \end{pmatrix} = [M_2]_E$$

*and*

$M_2(x, y) = (39x + 32y, 50x + 37y)$.

*So our plaintext is resolved as $M_2 = (39, 32, 50, 37) = (PLE.)$. Consequently, our message is $M = M_1M_2 = (EXAMPLE.)$.*

## 16.2 KEY EXCHANGE ALGORITHM CREATED BETWEEN INNER PRODUCT AND ORTHOGONALITY

1. The sender considers an inner product $f(u) = (a, u) = a_1u_1 + a_2u_2 + \ldots + a_nu_n$, where $a, u \in \mathbb{R}^n$

   The sender generates the operator on the inner product equation given as for $T_i = T_{(c_i,d_i)} = c_if + d_i$, where $c_i, d_i$ parameters and $c_i > 0$, $d_i \in \mathbb{R}$, $\forall i = 1, 2, \ldots, j$.

   The sender generates the public key such that

   $T(f) = T_j \circ T_{j-1} \circ \cdots \circ T_1(f) = g$.

   The sender makes the $f$ and $g$ public.

2. The recipient generates public key and secret key. Firstly, the recipient creates $b$ vector.

The recipient selects an arbitrary vector $v$ such that $(b, v) = 0$, i.e. $b$ and $v$ orthogonal.

The recipient keeps $f(v) = m$ as secret key and makes $g(v) = k$ public key.

3. The sender recovers the secret key $m$ from public key $k$ by applying the inverse of operators $T_i$, where for $T_i$ we have $T_i^{-1} = T_{(c_i,d_i)}^{-1} = \frac{(g)-d_i}{c_i}$.

   The sender from $T_i^{-1}$ the inverse of $T_i$ recovers $m$ from $k$ by

   $(T_j \circ T_{j-1} \circ \cdots \circ T_1)^{-1} = T_1^{-1} \circ T_2^{-1} \circ \cdots \circ T_j^{-1}$.

4. The secret key $m$ evaluated by both sender and receiver is used as the key for key exchange.

## 16.3 A NEW ALGORITHM USING KEY EXCHANGE

**Algorithms**

Encryption Algorithm

1. Create message blocks.
2. Determine the number $n$.
3. Determine the values corresponding to the characters in the $M_i$ message blocks.
4. Place the values in the message blocks such that they are the coefficients of the linear mapping $M_i : \mathbb{R}^2 \to \mathbb{R}^2$.
5. Consider inner product $f$ and generate $g$.
6. Recover the secret key $m$.
7. Create $E = \{(F_{n+1}, F_n), (F_n, F_{n-1})\}$ and $S = \{(F_{m+1}, F_m), (F_m, F_{m-1})\}$ bases.
8. Find the base change matrix $P$ from $E$ to $S$ and $P^{-1}$ matrix.
9. Calculate matrix $[M_i]_E$ based on base $E$.

10. Calculate matrix $[M_i]_S = P^{-1}[M_i]_E P$, where $[M_i]_S$ is the matrix with respect to the base $S$.

11. Construct the encrypted message $C_i(x, y)$ so that the inputs of the $[M_i]_S$ matrix are the coefficients of the $C_i : \mathbb{R}^2 \to \mathbb{R}^2$ linear mapping.

12. Transmit $[n, C]$, where $C$ is obtained by combining $C_i$'s.

Decryption Algorithm
$[n, C]$, after reaching the person who will decrypt it.

1. Build $[M_i]_S$ using $C_i(x, y)$.

2. Construct the base change matrix $P$ and its inverse $P^{-1}$.

3. Calculate matrix $[M_i]_E = P[M_i]_S P^{-1}$.

4. Create the $M_i : \mathbb{R}^2 \to \mathbb{R}^2$ linear mapping and the $M_i$ block.

5. Create the $M$ message, where $M$ is obtained by combining $M_i$'s.

**Example 16.2** *(Public key calculation) X chooses* $a = (1, 2, 3, -5)$ *and* $u = (u_1, u_2, u_3, u_4)$. *So* $f(u) = (a, u) = u_1 + 2u_2 + 3u_3 - 5u_4$. *Let* $T_1 = T_{(1,3)}$, $T_2 = T_{(2,-4)}$, $T_3 = T_{(1,-2)}$

$$\begin{aligned} g(u) &= T_3 \circ T_2 \circ T_1(f(u)) \\ &= T_3 \circ T_2 \circ T_1(u_1 + 2u_2 + 3u_3 - 5u_4) \\ &= T_3 \circ T_2(u_1 + 2u_2 + 3u_3 - 5u_4 + 3) \\ &= T_3(2u_1 + 4u_2 + 6u_3 - 10u_4 + 2) \\ &= 2u_1 + 4u_2 + 6u_3 - 10u_4. \end{aligned}$$

*X makes*

$$\begin{cases} f(u) = u_1 + 2u_2 + 3u_3 - 5u_4 \\ g(u) = 2u_1 + 4u_2 + 6u_3 - 10u_4 \end{cases}$$

*public.*

*Y considers* $b = (2, 4, -5, 1)$ *and selects an arbitrary vector* $v$ *such that* $(b, v) = 0$.

$((2, 4, -5, 1), (v_1, v_2, v_3, v_4)) = 0.$

*Let* $v = (1, 2, 2, 0)$.

*Y evaluates*

$$\begin{aligned} g(v) &= 22 \\ f(v) &= 11. \end{aligned}$$

*Y keeps* $m = f(v) = 11$ *as secret key, makes* $k = g(v) = 22$ *as public key.*

*X recovers secret key* $m$ *from the private key* $g(v)$ *by applying*

$$\begin{aligned} (T_3 \circ T_2 \circ T_1)^{-1}(k) &= T_1^{-1} \circ T_2^{-1} \circ T_3^{-1}(22) \\ &= T_1^{-1} \circ T_2^{-1}(22 + 2) \\ &= T_1^{-1} \circ T_2^{-1}(24) \\ &= T_1^{-1}(\frac{24 + 4}{2}) \\ &= T_1^{-1}(14) \\ &= \frac{14 - 3}{1} \\ &= 11 \\ &= m. \end{aligned}$$

**Example 16.3** *Let the plaintext be* $M = (KEY\ EXCHANGE)$.

***Encryption***

*Let's create the message blocks.* $M_1 = (KEY\ )$, $M_2 = (EXCH)$, $M_3 = (ANGE)$. *Since the number of blocks is* 3, $n = 3$. *The values corresponding to the message blocks are* $M_1 = (14, 45, 53, 30)$, $M_2 = (55, 26, 28, 40)$, $M_3 = (13, 46, 51, 55)$. *Now let's determine the* $C$ *ciphertext corresponding to* $M$.

*Let's find* $C_1$ *first. The linear mapping* $M_1(x, y)$ *representing the* $M_1$ *block is* $M_1(x, y) = (14x + 45y, 53x + 30y)$. *Since* $m = 11$ *and* $n = 3$, *we have bases*

$$\begin{aligned} E &= \{(F_4, F_3), (F_3, F_2)\}\,,\ S = \{(F_{12}, F_{11}), (F_{11}, F_{10})\}\,, \\ E &= \{(3, 2), (2, 1)\}\,,\ S = \{(144, 89), (89, 55)\}\,. \end{aligned}$$

*We find*

$$P = \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix}$$

*the base change matrix from $E$ to $S$, by writing*

$$\begin{aligned}(144,89) &= 34(3,2)+21(2,1)\\ (89,55) &= 21(3,2)+13(2,1),\end{aligned}$$

*which is a linear combination of the vectors in $E$ for each vector in $S$. We have*

$$P^{-1}=\begin{pmatrix}13 & -21\\ -21 & 34\end{pmatrix}.$$

*The matrix with respect to the base $E$ of the linear mapping $M_1(x,y)$ is*

$$[M_1]_E=\begin{pmatrix}306 & 199\\ -393 & -262\end{pmatrix}.$$

*We obtained the matrix $[M_1]_E$ by calculations of*

$$\begin{aligned}M_1(3,2) &= (132,219)=306(3,2)-393(2,1),\\ M_1(2,1) &= (73,136)=199(3,2)-262(2,1).\end{aligned}$$

*Using the $P$, $P^{-1}$ and $[M_1]_E$ matrices, we get*

$$\begin{aligned}[M_1]_S &= \begin{pmatrix}13 & -21\\ -21 & 34\end{pmatrix}\begin{pmatrix}306 & 199\\ -393 & -262\end{pmatrix}\begin{pmatrix}34 & 21\\ 21 & 13\end{pmatrix}\\ &= \begin{pmatrix}585\,723 & 362\,008\\ -947\,619 & -585\,679\end{pmatrix}.\end{aligned}$$

*$M_1$ is encoded as $C_1(x,y)=(585\,723x+362\,008y,-947\,619x-585\,679y)$.*
*Let's find the $C_2$ encrypted message corresponding to $M_2$. The linear mapping $M_2(x,y)$ representing the $M_2$ block is $M_2(x,y)=(55x+26y,28x+40y)$. The matrix with respect to the base $E$ of the linear mapping $M_2(x,y)$ is*

$$[M_2]_E=\begin{pmatrix}111 & 56\\ -58 & -16\end{pmatrix}.$$

*We obtained the matrix $[M_2]_E$ by calculations of*

$$\begin{aligned}M_2(3,2) &= (217,164)=111(3,2)-58(2,1),\\ M_2(2,1) &= (136,96)=56(3,2)-16(2,1).\end{aligned}$$

*Using the $P$, $P^{-1}$ and $[M_2]_E$ matrices, we obtain*

$$[M_2]_S = \begin{pmatrix} 13 & -21 \\ -21 & 34 \end{pmatrix} \begin{pmatrix} 111 & 56 \\ -58 & -16 \end{pmatrix} \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix}$$
$$= \begin{pmatrix} 112\,818 & 69\,713 \\ -182\,422 & -112\,723 \end{pmatrix}.$$

*$M_2$ is encoded as $C_2(x, y) = (112\,818x + 69\,713y, -182\,422x - 112\,723y)$.*

*Now let's find the $C_3$ encrypted message corresponding to $M_3$. The linear mapping $M_3(x, y)$ representing the $M_3$ block is $M_3(x, y) = (13x + 46y, 51x + 55y)$. The matrix with respect to the base $E$ of the linear mapping $M_3(x, y)$ is*

$$[M_3]_E = \begin{pmatrix} 395 & 242 \\ -527 & -327 \end{pmatrix}.$$

*We obtained the matrix $[M_3]_E$ by calculations of*

$$M_3(3, 2) = (131, 263) = 395(3, 2) - 527(2, 1),$$
$$M_3(2, 1) = (72, 157) = 242(3, 2) - 327(2, 1).$$

*Using the $P$, $P^{-1}$ and $[M_3]_E$ matrices, we calculate the following*

$$[M_3]_S = \begin{pmatrix} 13 & -21 \\ -21 & 34 \end{pmatrix} \begin{pmatrix} 395 & 242 \\ -527 & -327 \end{pmatrix} \begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix}$$
$$= \begin{pmatrix} 761\,141 & 470\,411 \\ -1231\,442 & -761\,073 \end{pmatrix}.$$

*$M_3$ is encoded as $C_3(x, y) = (761\,141x + 470\,411y, -1231\,442x - 761\,073y)$. As a result, message $M$ is sent as*

$$[3, \begin{pmatrix} 585\,723x + 362\,008y, -947\,619x - 585\,679y \\ 112\,818x + 69\,713y, -182\,422x - 112\,723y \\ 761\,141x + 470\,411y, -1231\,442x - 761\,073y \end{pmatrix}].$$

***Decryption***

*Let's find $M_1$ by decoding the $C_1$ code. Using the $P$, $P^{-1}$ and $[M_1]_S$ matrices, we get*

$$\begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} \begin{pmatrix} 585\,723 & 362\,008 \\ -947\,619 & -585\,679 \end{pmatrix} \begin{pmatrix} 13 & -21 \\ -21 & 34 \end{pmatrix} = \begin{pmatrix} 306 & 199 \\ -393 & -262 \end{pmatrix}$$
$$= [M_1]_E.$$

*Since the matrix* $[M_1]_E$ *is the matrix with respect to base* $E$ *of the linear mapping* $M_1(x, y)$*, we have the following:*

$$\begin{aligned} M_1(3,2) &= 306(3,2) - 393(2,1) = (132, 219), \\ M_1(2,1) &= 199(3,2) - 262(2,1) = (73, 136). \end{aligned}$$

*Using these equalities, we get*

$$\begin{aligned} 3M_1(1,0) + 2M_1(0,1) &= (132, 219), \\ 2M_1(1,0) + M_1(0,1) &= (73, 136), \end{aligned}$$

*and*

$$M_1(1,0) = (14, 53),\ M_1(0,1) = (45, 30).$$

*If the linear mapping* $M_1(x, y)$ *is written as*

$$M_1(x, y) = xM_1(1,0) + yM_1(0,1),$$

*we get*

$$M_1(x, y) = x(14, 53) + y(45, 30) = (14x + 45y, 53x + 30y).$$

*The plaintext corresponding to the* $C_1$ *encrypted message would be* $M_1 = (14, 45, 53, 30) = (KEY\ )$*.*

*Let's find* $M_2$ *by decoding the* $C_2$ *code. Using the* $P$*,* $P^{-1}$ *and* $[M_2]_S$ *matrices, we obtain*

$$\begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} \begin{pmatrix} 112\,818 & 69\,713 \\ -182\,422 & -112\,723 \end{pmatrix} \begin{pmatrix} 13 & -21 \\ -21 & 34 \end{pmatrix} = \begin{pmatrix} 111 & 56 \\ -58 & -16 \end{pmatrix} = [M_2]_E .$$

*Since the matrix* $[M_2]_E$ *is the matrix with respect to base* $E$ *of the linear mapping* $M_2(x, y)$*, we have the following:*

$$\begin{aligned} M_2(3,2) &= 111(3,2) - 58(2,1) = (217, 164), \\ M_2(2,1) &= 56(3,2) - 16(2,1) = (136, 96). \end{aligned}$$

*Using these equalities, we get*

$$\begin{aligned} 3M_2(1,0) + 2M_2(0,1) &= (217, 164), \\ 2M_2(1,0) + M_2(0,1) &= (136, 96), \end{aligned}$$

*and*

$M_2(1,0) = (55,28),\ M_2(0,1) = (26,40).$

*If the linear mapping* $M_2(x,y)$ *is written as*

$M_2(x,y) = xM_2(1,0) + yM_2(0,1),$

*we obtain*

$M_2(x,y) = x(55,28) + y(26,40) = (55x + 26y, 28x + 40y).$

*The plaintext corresponding to the* $C_2$ *encrypted message would be* $M_2 = (55,26,28,40) = (EXCH)$.

*Let's find* $M_3$ *by decoding the* $C_3$ *code. Using the* $P$, $P^{-1}$ *and* $[M_3]_S$ *matrices, we get*

$$\begin{pmatrix} 34 & 21 \\ 21 & 13 \end{pmatrix} \begin{pmatrix} 761\,141 & 470\,411 \\ -1231\,442 & -761\,073 \end{pmatrix} \begin{pmatrix} 13 & -21 \\ -21 & 34 \end{pmatrix} = \begin{pmatrix} 395 & 242 \\ -527 & -327 \end{pmatrix} = [M_3]_E .$$

*Since the matrix* $[M_3]_E$ *is the matrix with respect to base* $E$ *of the linear mapping* $M_3(x,y)$, *we have the following:*

$$\begin{aligned} M_3(3,2) &= 395(3,2) - 527(2,1) = (131,263), \\ M_3(2,1) &= 242(3,2) - 327(2,1) = (72,157). \end{aligned}$$

*Using these equalities, we obtain*

$$\begin{aligned} 3M_3(1,0) + 2M_3(0,1) &= (131,263), \\ 2M_3(1,0) + M_3(0,1) &= (72,157), \end{aligned}$$

*and*

$M_3(1,0) = (13,51),\ M_3(0,1) = (46,55).$

*If the linear mapping* $M_2(x,y)$ *is written as*

$M_3(x,y) = xM_3(1,0) + yM_3(0,1),$

*we have*

$M_3(x,y) = x(13,51) + y(46,55) = (13x + 46y, 51x + 55y).$

*The plaintext corresponding to the $C_3$ encrypted message would be $M_3 = (13, 46, 51, 55) = (ANGE)$.*
*As a result, if $M_1$, $M_2$, and $M_3$ are combined, the $C$ encrypted message is decoded as $M_1M_2M_3 = (KEY\ EXCHANGE)$.*

## 16.4 COMPLEXITY ANALYSIS

In the first algorithm we created, $n$ shows the number of blocks. The $S$ base and $P$ matrix are obtained according to the $n$ number. That is, as the number $n$ changes, the base $S$ and matrix $P$, as well as the table of characters, change. As a result of this, the encrypted linear transformation differs according to every $n$ number.
In the second algorithm we created, a key exchange algorithm created using inner product and orthogonality was included, making our first algorithm even more complex. The $c_i$ and $d_i$ parameters in the $T$ linear transform in the key exchange algorithm allow us to define as many $T$ linear transforms as we want. In this algorithm, $E$ and $S$ bases differ according to the number of $n$ blocks and the $m$ variable we will obtain according to the key exchange algorithm. Therefore, the transition matrix from $E$ to $S$ also changes in $P$. As a result, the encrypted linear transformation also changes according to every $n$ and $m$ numbers.
In addition to these, the difficulty of the calculations we use in the algorithms makes it difficult or even impossible for the encrypted messages to be solved by the intervening hackers.

## REFERENCES


**[1] Hoffstein J, Pipher J and Silverman J H** (2008) *An Introduction to Mathematical Cryptography.* Vol. 1. Springer.

**[2] Kraft J S and Washington L C** (2014) *An Introduction to Number Theory with Cryptography.* Taylor & Francis Group.

**[3] Yan S Y** (2013) *Computational Number Theory and Modern Cryptography.* John Wiley & Sons Singapore.

**[4] Rosen K H** (2011) *Elementary Number Theory and Its Applications.* 6th Edition, Addison-Wesley.

**[5] Paar C and Pelzl J** (2009) *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer Science & Business Media.

**[6] Andreescu T, Andrica D and Cucurezeanu I** (2010) *An Introduction Diophantine Equations.* A Problem-Based Approach, Springer Science+Business Media.

**[7] Kameswari P A, Sriniasarao S S and Belay A** (2021) An Applications of Linear Diophantine Equations to Cryptography. *Advances in Mathematics: Scientific Journal,* 10(6): 2799-2806.

**[8] Hankerson D, Menezes A and Vanstone S** (2004) *Guide to Elliptic Curve Cryptography.* Springer-Verlag, New York.

**[9] Rynne B P and Youngson M A** (2000) *Linear Functional Analysis.* Springer-Verlag.

**[10] Lipschutz S and Lipson M L** (2018) *Linear Algebra.* Schaum's Outline Series, Sixth Edition.

**[11] Piziak R and Odell P L** (2007) *Matrix Theory From Generalized Inverses to Jordan Form.* Taylor & Francis Group.

**[12] Elaydi S** (1999) *An Introduction to Difference Equations.* Springer-Verlag, 428 New York.

**[13] Soykan Y** (2019) Simson Identity of Generalized m-Step Fibonacci Numbers. *Int. J. Adv. Appl. Math. and Mech.,* 7(2): 45-56.

**[14] Adegoke K** (2018) Linear Properties of Generalized n-Step Fibonacci Numbers. *arXiv:1808.02878v1 [math.NT]*.

## REFERENCES (continued)


**[15] Bacani J B and Rabago J F T** (2015) On Generalized Fibonacci Numbers. *Applied Mathematical Sciences,* 9(25): 3611-3622.

**[16] Cook C K and Bacon M R** (2013) Some Identities for Jacobsthal and Jacobsthal-Lucas Numbers Satisfying Higher Order Recurrence Relations. *Annales Mathematicae et Informaticae,* 41: 27-39.

**[17] Uçar S, Taş N and Özgür N Y** (2019) A New Application to Coding Theory via Fibonacci and Lucas Numbers. *Mathematical Sciences and Applications E-notes,* 7(1): 62-70.

**[18] Prasad K and Mahato H** (2021) Cryptography Using Generalized Fibonacci Matrices with Affine-Hill Cipher. *Journal of Discrete Mathematical Sciences and Cryptography,* DOI: 10.1080/09720529.2020.1838744.

**[19] Soykan Y** (2023) On Generalized Padovan Numbers. *Int. J. Adv. Appl. Math. and Mech.,* 10(4): 72-90.

**[20] Soykan Y** (2019) On Generalized Third-Order Pell Numbers. *Asian Journal of Advanced Research and Reports,* 6(1): 1-18.

**[21] Kiliç E and Taşci D** (2006) The Generalized Binet Formula, Represantation and Sums of The Generalized Order-k Pell Numbers. *Taiwanese Journal of Mathematics,* 10(6): 1661-1670.

**[22] Soykan Y** (2020) A Study on Generalized (r,s,t)-Numbers. *MathLAB J.,* 7: 101-129.

**[23] Soykan Y** (2020) On Generalized Grahaml Numbers. *Journal of Advances in Mathematics and Computer Science,* 35(2): 42-57; Article no.JAMCS.55255.

**[24] Davis P J** (1979) *Circulant Matrices.* JohnWiley&Sons, New York.

**[25] Behera A and Panda G K** (1999) On The Square Roots of Triangular Numbers. *The Fibonacci Quarterly,* 37(2): 98-105.

**[26] King C H** (1960) Some Properties of Fibonacci Numbers. *Master's Thesis,* San Jose State College.

**[27] Ray P K** (2012) Certain Matrices Associated with Balancing and Lucas-Balancing Numbers. *Matematika,* 28(1): 15-22.

**[28] Basu M and Prasad M** (2009) Coding Theory on The m-Extension of The Fibonacci p-Numbers. *Chaos, Solitons and Fractals,* 42: 2522-2530.

**[29] Basu M and Prasad M** (2009) The Generalized Relations Among The Code Elements for Fibonacci Coding Theory. *Chaos, Solitons and Fractals,* 41: 2517-2525.

**[30] Basu M and Prasad M** (2011) Coding Theory on The (m,t)-Extension of The Fibonacci p-Numbers. *Discrete Mathematics, Algorithms and Applications,* 3: 259-267.

**[31] Basu M and Das M** (2014) Tribonacci Matrices and A New Coding Theory. *Discrete Mathematics, Algorithm and Applications,* 6(1): 1450008 (17 pages).

**[32] Basu M and Das M** (2014) Coding Theory on Fibonacci n-Step Numbers. *Discrete Mathematics, Algorithms and Applications*, 6(2): 1450017 (32 pages).

**[33] Basu M and Das M** Coding Theory on Constant Coefficient Fibonacci n-Step Numbers. Communicated.

**[34] Esmaili M and Esmaeili M** (2010) A Fibonacci-Polynomial Based Coding Method with Error Detection and Correction. *Computers and Mathematics with Applications,* 60: 2738-2752.

**[35] Esmaili M, Moosavi M and Gulliver T A** (2017) A New Class of Fibonacci Sequence Based Error Correcting Codes. *Cryptography and Communications,* 9: 379-396.

**[36] Prasad B** (2014) Coding Theory on (h(x), g(y))-Extension of Fibonacci p-Numbers Polynomials. *Universal Journal of Computational Mathematics* 2: 6-10.

**[37] Prasad B** (2014) High Rates of Fibonacci Polynomials Coding Theory. *Discrete Mathematics, Algorithms and Applications* 6.

**[38] Prasad B** (2016) Coding Theory on Lucas p Numbers. *Discrete Mathematics, Algorithms and Applications* 8.

**[39] Stakhov A P** (2006) Fibonacci Matrices, A Generalization of The Cassini Formula, and A New Coding Theory. *Chaos, Solitons and Fractals,* 30: 56-66.

**[40] Stakhov A, Massingue V and Sluchenkov A** (1999) *Introduction into Fibonacci Coding and Cryptography.* Osnova, Kharkov.

**[41] Taş N, Uçar S, Özgür N Y and Kaymak Ö** (2018) A New Coding/Decoding Algorithm Using Finonacci Numbers. *Discrete Math. Algorithms Appl.,* 10(02): 1850028.

**[42] Baumslag G, Fine B, Kreuzer M and Rosenberger G** (2015) *A Course in Mathematical Cryptography.* Walter de Gruyter, Berlin.

**[43] Bertaccini M** (2022) *Cryptography Algorithms.* Packt Birmingham-Mumbai.

**[44] Buell D** (2021) *Fundamentals of Cryptography.* Springer.

**[45] Easttom C** (2016) *Modern Cryptography.* Applied Mathematics for Encryption and Information Security, McGraw-Hill Education.

**REFERENCES (continued)**


**[46] Klima R and Sigmon N** (2019) *Cryptology Classical and Modern.* Second Edition, Taylor & Francis Group.

**[47] Schneier B** (1996) *Applied Cryptography.* Second Edition, John Wiley &. Sons, Inc..

**[48] Stinson D R and Paterson M B** (2019) *Cryptography Theory and Practice.* Fourth Edition, Taylor & Francis Group.

**[49] Stothers A J** (2010) *On The Complexity of Matrix Multiplication.* The University of Edinburgh.

**[50] Soykan Y and İrge V** (2022) Generalized Woodall Numbers: An Investigation of Properties of Woodall and Cullen Numbers via Their Third Order Linear Recurrence Relations. *Universal Journal of Mathematics and Applications,* 5(2): 69-81.

**[51] Sloane N J A** The on-Line Encyclopedia of Integer Sequences. *http://oeis.org/*

**[52] Cunningham A J C and Woodall H J** (1917) Factorisation of $Q=(2^q \mp q)$ and $(q.2^q \mp 1)$. *Messenger of Mathematics,* 47: 1-38.

**[53] Berrizbeitia P, Fernandes J G, González M J, Luca F and Huguet V J M** (2012) On Cullen Numbers which are Both Riesel and Sierpiński Numbers. *Journal of Number Theory,* 132: 2836-2841.

**[54] Bilu Y, Marques D and Togbe A** (2019) Generalized Cullen Numbers in Linear Recurrence Sequences. *Journal of Number Theory*, 202: 412-425.

**[55] Grantham J and Graves H** (2021) The abc Conjecture Implies That Only Finitely Many s-Cullen Numbers Are Repunits. *http://arxiv.org/abs/2009.04052v3, MathNT.*

**[56] Guy R** (1994) *Unsolved Problems in Number Theory (2nd ed.).* Springer-Verlag, New York.

**[57] Hooley C** (1976) *Applications of The Sieve Methods to The Theory of Numbers.* Cambridge University Press, Cambridge.

**[58] Keller W** (1995) New Cullen Primes. *Math. Comput.*, 64: 1733-1741.

**[59] Luca F and Stanica P** (2004) Cullen Numbers in Binary Recurrent Sequences. *FT. Howard (ed.), Applications of Fibonacci Numbers, Proceedings of the Tenth International Research Conference on Fibonacci Numbers and their Applications, Kluwer Academic Publishers,* 9: 167-175.

## REFERENCES (continued)


**[60] Marques D** (2014) On Generalized Cullen and Woodall Numbers That are Also Fibonacci Numbers. *Journal of Integer Sequences,* 17, Article 14.9.4.

**[61] Marques D** (2015) Fibonacci s-Cullen and s-Woodall Numbers. *Journal of Integer Sequences,* 18, Article 15.1.4.

**[62] Meher N K and Rout S S** (2020) Cullen Numbers in Sums of Terms of Recurrence Sequence. *http://arxiv.org/abs/2010.10014v1, MathNT.*

**[63] Bruce I** (1984) A Modified Tribonacci Sequence. *Fibonacci Quarterly,* 22(3): 244-246.

**[64] Catalani M** (2012) Identities for Tribonacci-related sequences. *arXiv:math/0209179.*

**[65] Choi E** (2013) Modular Tribonacci Numbers by Matrix Method. *Journal of the Korean Society of Mathematical Education Series B: Pure and Applied. Mathematics,* 20(3): 207-221.

**[66] Elia M** (2001) Derived Sequences, The Tribonacci Recurrence and Cubic Forms. *Fibonacci Quarterly,* 39(2): 107-115.

**[67] Er M C** (1984) Sums of Fibonacci Numbers by Matrix Methods. *Fibonacci Quarterly,* 22(3): 204-207.

**[68] Lin P Y** (1988) De Moivre-Type Identities For The Tribonacci Numbers. *Fibonacci Quarterly,* 26: 131-134.

**[69] Pethe S** (1988) Some Identities for Tribonacci sequences. *Fibonacci Quarterly,* 26(2): 144-151.

**[70] Scott A, Delaney T and Hoggatt J V** (1977) The Tribonacci sequence. *Fibonacci Quarterly,* 15(3): 193-200.

**[71] Shannon A** (1977) Tribonacci Numbers and Pascal's Pyramid. *Fibonacci Quarterly,* 15(3): 268-275.

**[72] Soykan Y** (2019) Tribonacci and Tribonacci-Lucas Sedenions. *Mathematics,* 7(1): 74.

**[73] Spickerman W** (1982) Binet's Formula for The Tribonacci Sequence. *Fibonacci Quarterly,* 20: 118-120.

**[74] Yalavigi C C** (1972) Properties of Tribonacci Numbers. *Fibonacci Quarterly,* 10(3): 231-246.

**[75] Yilmaz N and Taskara N** (2014) Tribonacci and Tribonacci-Lucas Numbers via The Determinants of Special Matrices. *Applied Mathematical Sciences,* 8(39): 1947-1955.

## REFERENCES (continued)


**[76] Kalman D** (1982) Generalized Fibonacci Numbers By Matrix Methods. *Fibonacci Quarterly,* 20(1): 73-76.

**[77] Soykan Y** (2021) On the Recurrence Properties of Generalized Tribonacci Sequence. *Earthline Journal of Mathematical Sciences,* 6(2): 253-269.

**[78] Stinson D R** (2006) *Cryptography: Theory and Practice.* 3rd Ed. Chapman and Hall/CRC, Taylor & Francis Group.

**[79] Elgamal T A** (1985) Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Thory,* 31(4): 469-472.

**[80] Yosh H** (2011) The Key Exchange Cryptosystem Used with Higher Order Diophantine Equations. *International Journal of Network Security & Its Applications* 3(2): 43-50.

**[81] Hirata-Kohno N and Petho A** (2014) A Key Exchange Protocol Based on Diophantine Equation and S-Integers. *JSIAM Letters,* 6(0): 85-88.

**[82] Kameswari P A and Kumar L P** (1998) *LU-A Method for Recovering A Key in The Key Exchange Cryptosystem by Diophantine Equations.* Third Edition, Addison-Wesley.

**[83] Mao W** (2003) *Modern Cryptography: Theory and Practice.* Pearson Education India.

**[84] Stallings W** (2017) *Cryptography and Network Security: Principles and Practice.* 7th Ed. Pearson Education Limited.

**[85] Gupta I, Singh J and Chaudhary R** (2007) Cryptanalysis of An Extension of The Hill Cipher. *Cryptologia,* 31(3): 246-253.

**[86] Sundarayya P and Prasad G V** (2019) A Public Key Cryptosystem Using Affine Hill Cipher Under Modulation of Prime Number. *Journal of Information and Optimization Sciences,* 40(4): 919-930.

**[87] Thilaka B and Rajalakshmi K** (2005) An Extension of Hill Cipher Using Generalized Inverses and mth Residue Modulo n. *Cryptologia,* 29(4): 367-376.

**[88] Viswanath M and Kumar M R** (2015) A Public Key Cryptosystem Using Hill's Cipher. *Journal of Discrete Mathematical Sciences and Cryptography,* 18(1-2): 129-138.

**[89] Myasnikov A G, Shpilrain V and Ushakov A** (2008) *Group-Based Cryptography.* Adv. Courses in Math. -CRM Barcelona, Birkhäuser, Basel.

**[90] Buchmann J** (2004) *Introduction to Cryptography.* Springer.

## REFERENCES (continued)


**[91] Koblitz N** (1984) *A Course in Number Theory and Cryptography.* Springer Verlag, Berlin.

**[92] Koblitz N** (1987) Elliptic Curve Cryptosystems. *Math. Comp.*, 48(177): 203-209.

**[93] Ling S, Wang H and Xing C** (2013) *Algebraic Curves in Cryptography.* Taylor & Francis.

**[94] Geetha G and Jain P** (2014) Implementation of Matrix Based Mapping Method Using Elliptic Curve Cryptography. *International Journal of Computer Applications Technology and Research,* 3(5): 312-317.

**[95] Priyatharsan U, Rupasinghe P L and Murray I** (2017) A New Elliptic Curve Cryptographic System over The Finite Fields. *In 2017 6th National Conference on Technology and Management (NCTM),* IEEE, pp. 164-169.

**[96] Chahal J S** (2019) *Fundamentals of Linear Algebra.* Taylor & Francis Group, Boca Raton.

**[97] Diffie W and Hellman M** (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory,* 22(6): 644-654.

**[98] Koblitz N** (1994) *A Course in Number Theory and Cryptography.* Springer Science & Business Media, 114.

**[99] Soykan Y** (2020) On Generalized (r,s)-Numbers. *International Journal of Advances in Applied Mathematics and Mechanics,* 8(1): 1-14.

**[100] Srinivasarao B S S** (2020) *A Key Exchange with Linear Diophantine equations.* M. Phil., Dissertation.

## CURRICULUM VITAE

Vedat İRGE He completed his primary, secondary and high school education in Bolu. In 2010, he graduated from Zonguldak Karaelmas University, Faculty of Science and Art, Department of Mathematics. In 2013, he graduated from Zonguldak Bülent Ecevit University, Institute of Science, Graduated School of Mathematics. Since 2015, he has been working as a mathematic teacher at National Ministry of Education.