CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Extension of Elliptic Curves over Krasner Hyperfields (A Review)

by

Rahila Riaz

A thesis submitted in partial fulfillment for the
degree of Master of Philosophy

in the

Faculty of Computing
Department of Mathematics

2022

Dedicated To

My parents, teachers and my brother for their support and love.

CERTIFICATE OF APPROVAL

Extension of Elliptic Curves over Krasner Hyperfields (A Review)

by

Rahila Riaz

(MMT191017)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Waqas Mahmood	QAU, Islamabad
(b)	Internal Examiner	Dr. Muhammad Afzal	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
April, 2022

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
April, 2022

Dr. M. Abdul Qadir
Dean
Faculty of Computing
April, 2022

Author's Declaration

I, **Rahila Riaz** hereby state that my MPhil thesis entitled "**Extension of Elliptic Curves over Krasner Hyperfields (A Review)**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MPhil degree.

(Rahila Riaz)
Registration No: MMT191017

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis entitled "**Extension of Elliptic Curves over Krasner Hyperfields (A Review)**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MPhil Degree, the University reserves the right to withdraw/revoke my MPhil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Rahila Riaz)
Registration No: MMT191017

Acknowledgement

All praise be to **Almighty ALLAH** who has been bestowed me with his great bounties, gifted me a loving family and excellent teachers and enabled me to complete my dissertation. I would like to express my special gratitude to my kind supervisor **Dr. Rashid Ali** for his constant motivation. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor. Also, many thanks are due to all teachers of CUST Islamabad, **Dr. Muhammad Sagheer**, **Dr. Abdul Rehman Kashif**, **Dr. Shafqat Hussain**, **Dr. Muhammad Afzal**, **Dr. Dur-e-Shehwar** and **Dr. Samina Batul** for conveying the excellent lectures.

I am grateful to the management staff of **Capital University of Science and Technology, Islamabad** for providing a friendly environment for studies. I am thankful to all of my family members for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my **Parents** for their earnest prayers, unconditional love and unflinching support in completing my degree program. They supported and encourage me throughout my life.

I would like to show my gratitude to my seniors specially, **Sir Zia Malik** for guidance, continuous support and patience during my research work. Also, I would like to thanks all of my friends **Khuzaima Nasir** and **Shazia Ramzan** for helping and motivating me during my research work.

Finally, I am obliged to all people who pray for me, share their knowledge during my degree program and support me.

(Rahila Riaz)

Abstract

The purpose of this thesis is to study a recent research in the context of algebraic hyperfields, with implications for cryptography. First, the ideas of extended Weierstrass equation and elliptic hypercurve on Krasner hyperfields are defined and points on elliptic hypercurves are computed in by using different hyperoperations. Elliptic hypercurves are generalization of elliptic curves. The hyperoperations (which are generalization of group operations) on elliptic hypercurves are defined and the way of computing points on elliptic hypercurves is also presented. This thesis shows the relation between elliptic curves and elliptic hypercurves by using hyperoperations. The characteristics of the hypergroups produced from elliptic hypercurves, as well as the corresponding H_v-groups are then investigated. Finally, a class of canonical hypergroups that can be used as an alphabet in a specific cryptographic system are investigated and defined.

Contents

List of Figures

List of Tables

Symbols

$\mathcal{A}$	Alphabet set
$\mathbb{C}$	Set of Complex numbers
$E_{u,v}$	Elliptic curve
$E_{\overline{U},\overline{V}}$	Elliptic hypercurve
$\mathbb{F}$	Field
$\mathbb{F}^*$	$\{\mathbb{F} \setminus 0\}$
$\overline{\mathbb{F}}$	Hyperfield
$\bullet_{uv}$	Elliptic curve group operation
G	Group
$\mathbb{G}$	Single group
$\mathcal{G}$	Subgroup of $\mathbb{F}^*$
$\circ_{\mathbb{G}}$	Hyperoperation defined on subhypergroups of elliptic hypercurve
$\overline{\circ}_{\mathbb{G}}$	Hyperoperation defined on Elliptic hypercurve
$\diamond$	Hyperoperation defined on *alphabet set*
$\oplus$	Hyperaddition
$\odot$	Hypermultiplication
$\circ$	Hyperproduct
$\mathcal{O}$	Identity element of elliptic and hyperelliptic curves
$\mathbb{R}$	Set of Real numbers
$\mathbb{Z}$	Set of Integers

Chapter 1

Introduction

1.1 Historical background

From the beginning of the mankind, the problem which is faced by the states as well as individual is that how to secure the secrete informations. People have always been fascinated by the idea of keeping information hidden from others. The think tanks of such states sit together to resolve this issue. They develop a mechanism to secure the relevant secrete message from authorized people. History of mankind is filled with examples where people of different civilization tried to keep informations secrete from adversaries. As society has evolved, the need for more secure and advanced methods of protecting data has increased. As the world becomes more global village, the demand of information security through electronic devices is increased. In modern age, the exchange of sensitive information, such as credit card numbers, passwords etc., over the internet is common practise. Protecting data in electronic systems is basic need of new era. In cryptography, the original message (plaintext), is converted into coded message (ciphertext) using an encryption method. The ciphertext is then decrypted and converted back to plaintext by the receiver or an authorised person using the decryption method by using a key. Cryptographic techniques are classified into two types: symmetric

key and asymmetric key cryptography [11]. Symmetric key [20](Private key) cryptography is a technique that employs the same key for encryption and decryption. Asymmetric key cryptography is a technique that uses two separate keys that has some mathematical relationship between these keys. In asymmetric key [21] cryptography (Public key cryptography), one key is identified as the public key, while the other is known as the private key. There are many other cryptographic technique such as Hill cipher [56], Elliptic curve cryptography (ECC) [28], Diffie-Hellman key exchange protocol [42], Advanced Encryption Standards (AES) [44], Rivest-Shamir-Adleman encryption (RSA) [67] etc.

The techniques needed to protect data belong to the field of cryptography [49]. Cryptography is the study of sending a message in secret way so that no other person except the authorized can read or control it. It is a technique for protecting data or information from attackers. Within its history, such strategies have evolved from simple forms to the complicated ones we have today. Simple conversion entails rearranging letters, as well as replacing or relocating letters. Some prominent historical figures who employed various techniques of data security **Ceasar** [4], who used the concealment of three letters to communicate with his generals, and **Jefferson**, who invented a wheel cipher that was used in the United States Navy during the World War II [12]. Complex methods, on the other hand, are the consequence of current technology such as data encryption, digital signature, sender/receiver authentication, public key cryptography, and secure computing, among others.

With the passage of time, there is a need of new techniques, which are efficient and helpful. Since the beginnings, hyperstructure theory, particularly hypergroup theory, has found applications in a variety of fields. Over the last several decades, hyperstructures (also known as hyperalgebras or non-deterministic algebras) have been investigated from several perspectives. However, there is no clear relationship or connection between the vast quantity of research on the issue reported in the literature. This is due to the various techniques adopted by the many writers

in attempting to expand the notions and structures from ordinary algebra theory. Furthermore, there appears to be a lack of communication across the three primary fields of knowledge in which this issue has been studied: mathematics, computer science, and logic.

Study of hyperstructure theory starts with the hypergroup introduced by **Marty** [45] in 1934. He applied hypergroups to groups, algebraic functions and rational functions. The idea of operation is essential in ordinary algebras. It may be generalised to multioperation, resulting in the formation of multialgebras. This generalization was already achieved by **Marty** in his paper " Sur une generalization de la notion de groupe "[45]. A multioperation (also known as a hyperoperation) is a generalisation of an operation that returns a set of values rather than a single value. We refer to algebraic hyperstructures as the class of structures made of a set and at least one multioperation. Multialgebras (or hyperalgebras) are a type of hyperstructure, as are hypergroups, hyperrings, and hyperlattices.
In this thesis, some of the hyperoperations [66], as a generalization of group operation are presented with appropriate examples. These hyperoperations also shows the relation with elliptic curve group.

1.2 Literature Review

In this section, the literature related to elliptic curves 1.2.1 and elliptic hypercurve 1.2.2 will be discussed.

1.2.1 Elliptic Curves

Elliptic curves appear first time in the work of Diophantus in second century A.D. Since then the theory of elliptic curves were studied in number theory. Till 1920, elliptic curves were studied mainly by **Cauchy** et. al [48]. In 1984, Lenstra [41] used elliptic curves for factoring integers. Integer factorization algorithm [54] is one of the initial application in cryptography. Fermat's last theorem

and general reciprocity law was proved using elliptic curves and that is how elliptic curves became the centre of attraction for many mathematicians.

Elliptic curves and its properties have been studied in mathematics as pure mathematical concepts for long since second or third century A.C. but its use in cryptography is very recent. The name "elliptic" itself was given in nineteenth century, though it has been studied widely by many mathematicians. Use of elliptic curve in cryptography was not known till 1984. Mathematicians have studied elliptic curves and their properties since 1984, and they have mostly been applied in cryptography. Elliptic curves theory has been used to deal with lengthy pure mathematics problems for the last 35 years and to derive efficient algorithms for practical usage, particularly in cryptography and computational number theory. A curve which satisfies the equation $k^2 = p(h)$, where $p(h)$ is a polynomial having degree 3 with no repeating roots is called an elliptic curve. **Miller** [51] and **Koblitz** [38] [37] independently proposed different cryptographic use of elliptic curves in 1985. In the discrete log cryptosystem, they suggested using a group of points on an elliptic curve defined over a finite field [50]. It is a whole new approach to solving cryptography problems. One can utilise a smaller elliptic curve group while preserving the same level of security. In many cases, the conclusion is a lower key size, reduced bandwidth, and faster implementation, particularly in smart cards and cell phones.

Elliptic curve cryptography (ECC) is a public key cryptography. ECC is based on the characteristics of a certain form of equation derived from a mathematical group. Equations based on elliptic curves provide a highly important property for cryptography purposes. The major reason for ECC's attraction is that no sub- exponential algorithm [22] exists to solve the discrete logarithm problem on a correctly selected elliptic curve. This means that with ECC, much smaller parameters may be used with the same level of security. In 2005, the United States National Security Agency published a study recommending that they take use of the previous 30 years of public key research and analysis and migrate from first generation public key algorithms to elliptic curves [8].

1.2.2 Elliptic Hypercurves

Marty presented the concept of hypergroup which is a generalization of group at the 8th Congress of Scandinavian Mathematicians in 1934 [45]. The main purpose is to solve several problems in group, algebraic functions, and rational fractions theories [45]. The article paper of **Litvino** [43] contains brief description of ideas, construction, results and prospects of hypergroup theory. Reasearch on this theory can be found in the books of **Corsini** [16], **Davvaz** and **Leoreanu-Fotea** [19] **Corsini** and **Leoreanu** [17], and **Vougiouklis** [65]. **Krasner** [39] proposed Krasner hyperrings/hyperfields in 1956 as a new tool for studying approximations on valued fields. He described algebraic hyperstructures [17] with ring-like properties, with addition, multiplication, or both as multi-valued operations. The paper that was reviewed by **Nakassis** [55] has some great theoretical insights. This article informs the reader about historical features of hyperring and hyperfield theory.

After a lengthy period of research, new applications in a general algebraic geometrical framework have been recognized, especially from an algebraic and hyperstructural perspective. **Connes** and **Consani** [14] were the first who demonstrated the use of hyperrings in the study of algebraic geometry. They also used hyperrings in number theory [15], highlighting the significance of Krasner hyperfields in affine algebraic group schemes. Furthermore, hyperring theory has proven to be a helful algebraic framework for studying tropical geometry [63], supertropical algebras [33], and other areas of algebraic geometry over hyperrings [34]. **Tahan** and **Davvaz** [1] [2] demonstrated linkages between hyperrings and arithmetic functions. **Jun** [35] in his article paper expalined the geormtery of hyperfields. He explained all the basic definitions and algebraic geometry over hyperings. **Hamidi** and **Leoreanu-Fotea** [27]constructed regular hypergroups on all non-empty sets and they also investigated closed hypergroups. The largest class of hyperstructres is the one which satisfies the weak associativity. These are called H_v- structures. **Arabpour**and **Jafarpour** defined H_v-groups and introduced a special product of elements in H_v-groups.

Recently, **Massouros** and **Massouros** overviewed the foundations of hypergroup

theory and focuses on the essential principles of hypergroup [46]. **Cristea** and **Kankaras** defined the concept of reducibility and focussed on some classes on hyperrings [18]. **Ameri** et. al [6] presented a computational method for construction and classification of finite hyperfield.

Previously, the study of elliptic curves was limited to fields; however now, elliptic curves are extended to the hyperfields. The purpose of this thesis is to start a new research in the context of algebraic hyperfields, with potential applications in cryptography. The work done in this research thesis includes:

1. Behavior of the generalised Weierstrass equation is investigated when reduced on quotient Krasner hyperfields which results in the proposal of an elliptic hypercurves.

2. Several hyperoperations which are extensions of group operations on fields are constructed by using elliptic hypercurves. These hyperoperations gives the possibility of simaltaneously studying elliptic curves at the same time.

3. The properties of related hypergroups with elliptic hypercurves are studied.

4. A class of canonical hypergroups that can be utilised as an alphabet in Berardi's cryptographic system is constructed [10].

1.3 Thesis Contributions

In the thesis, article entitled " Extension of Elliptic curves over Krasner hyperfields" by **Vahedi** et. al [61], is thoroughly reviewed. The main purpose of this work is to present and illustrate the definitions of various hyperoperations with the help of examples. These hyperoperations are the extension of group operations and are multivalued operations. This work clearly shows the realtion between hyperations and elliptic curve group operations. More precisely, the three hyperopeartions $\circ_{\mathbb{G}}$, $\overline{\circ}_{\mathbb{G}}$ and $\diamond$ are defined and explained in detail with the help of examples. All these three hyperoperations and the group operation $\bullet_{uv}$ are related. The thoery is ellaborated with the help of appropriate examples to help the reader

to understand hyperoperations.

Elliptic curves are also extended to elliptic hypercures. Elliptic hypercurves are the extension of elliptic curves which satisfy the generalized weierstrass equation. In this thesis the method of computing base points of elliptic hypercurves is also discussed in detail. In particular, the thesis will help to differentiate between elliptic curves and elliptic hypercurves.

1.4 Thesis Layout

Rest of the thesis is originated as follow:

In **Chapter** 2, mathematical background will be described which includes all the relevant definitions. These definition will help the reader to understand this thesis well. The method of finding multiplicative inverse of elliptic curves is also explained. At the end of this chapter cryptographic background is explained which includes the types of cryptography.

In **Chapter** 3, Elliptic curves over real numbers will be discussed in detail. This chapter will helps the reader to understand elliptic curves operation.

In **Chapter** 4, hyperoperations which are extension of group operation are defined. The way of computing points on elliptic hypercurves is presented. Three hyperoperations are also solved with the help of examples which shows relation between hyperoperations and elliptic curve group operations. Elliptic hypercurves are also defined and base points are computed.

In **Chapter** 5, all the above work will be concluded and some future work will be discussed.

Chapter 2

Background

This chapter will describe the basic concepts and background related to cryptography and mathematics behind it. It will help the reader for the better understanding of the thesis. Next section is reserved for mathematical background that includes basic definitions of hyperoperation, hypergroup, Krasner hyperfield and Regular hypergroup.

2.1 Mathematical Background of Elliptic Curves

Some basic mathematical concepts that will help to understand Chapter 3 of this thesis, are described below:

Definition 2.1.1.
A nonempty set G together with a binary operation '$*$' is a **Group** [24], if the following properties are satisfied:

1. **Associativity Property**: A binary operation '$*$' is associative i.e.,

$$(g * h) * i = g * (h * i), \text{ for all } g, h, i \in G$$

2. **Identity element**: There is an identity element $e \in G$, such that

$$g * e = e * g, \text{ for all } g \in G.$$

3. **Inverse element**: For each $g \in G$, there exists an element $g^{'} \in G$ such that

$$g * g^{'} = g^{'} * g = e.$$

the element $g^{'}$ is called inverse of g.
Moreover, if G satisfies

$$g_1 * g_2 = g_2 * g_1$$

for all $g_1, g_2 \in G$ then G is called an **abelian** or **commutative** group.

Example 2.1.2.

1. The set $GL_2(\mathbb{R})$ of 2×2 invertible matrices over the real numbers with multiplication as the binary operation is a group.

2. The set of complex numbers $G = \{1, i, -1, -i\}$ under multiplication of complex numbers is a group[32]. The multiplication table for G is given below:

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

3. The set of matrices

$$G = \left\{ e = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \alpha = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \beta = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \gamma = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

under multiplication is a group. The multiplication table is given as:

Definition 2.1.3.

A group G that can be constructed by some single element is called a **Cyclic group**. That is for some $\alpha \in G$,

TABLE 2.1: Multiplication operation $*$ on G

$*$	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

$$\langle G, * \rangle = \{\alpha^m | m \in \mathbb{Z}\}.$$
$$\alpha^m = \alpha * \alpha * \alpha * \cdots * \alpha, \text{ for some } \alpha \in G.$$

or in addition notation it can be given as:

$$\langle G, + \rangle = \{m\alpha | m \in \mathbb{Z}\}.$$
$$m\alpha = \alpha + \alpha + \alpha + \cdots + \alpha, \text{ for some } \alpha \in G.$$

Here α is called a **generator** of G such that every element of G is constructed by α, which can be written as $G = \langle \alpha \rangle$.

Example 2.1.4.

1. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is a cyclic group under binary operation usual addition '+'. $1 \in \mathbb{Z}_4$, such that

   $1 = 1$, $1+1 = 2$, $1+1+1 = 3$, $1+1+1+1 = 4 \mod 4 = 0$ (under mod 4).

   so 1 is a generator of $\mathbb{Z}_4$.

2. $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is a cyclic group under binary operation multiplication '$\cdot$'.
   Let $c = 2 \in \mathbb{Z}_{11}$, such that

   $$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,$$
   $$2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1.$$

   So 2 is a generator of $\mathbb{Z}_{11}$.

Definition 2.1.5.

A nonempty set $(R, +, \cdot)$ is called a **Ring** [13] if for all $p, q, r \in R$ the following axioms are satisfied:

1. **Closure**: R is closed under binary operation multiplication '$\cdot$'.
2. **Abelian**: $(R, +)$ is abelian.
3. **Associativity**: R is associative under binary operation multiplication'$\cdot$', then

$$(p \cdot q) \cdot r = p \cdot (q \cdot r).$$

4. **Distributivity**: R satisfies both left and right distributive laws.

$$(q + r) \cdot p = q \cdot p + r \cdot p.$$
$$p \cdot (q + r) = p \cdot q + p \cdot r.$$

Further, a ring R is said to be a **commutative ring** if it holds the following axiom:

$$q \cdot r = r \cdot q, \text{ for all } q, r \in R.$$

Example 2.1.6.

1. The set of integers $\mathbb{Z}$ under two binary operations usual addition'$+$' and multiplication '$\cdot$' is a ring.
2. The set of polynomials under binary operations usual addition '$+$' and multiplication '$\cdot$' of polynomials is a ring.

Definition 2.1.7.

If a set $(\mathbb{F}, +, *)$ satisfies all the following properties then it is called a **Field** [9].

1. $\mathbb{F}$ is **closed** under usual addition'$+$' and multiplication '$\cdot$'.
2. $\mathbb{F}$ is **abelian** under addition '$+$' and multiplication'$\cdot$'.

3. $\mathbb{F}$ is **associative** under addition '+' and multiplication '$\cdot$'.

4. $\mathbb{F}$ is **distributive** i.e, $r_1(r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3)$.

5. There exists **identity** elements such that $r_1 + 0 = r_1$ and $r_1 \cdot 1 = r_1$.

6. For every elements r_1 and $r_2^{'}$ there exists **inverse** element $r_1^{'}$ such that $r_1 + r_1^{'} = 0$ and $r_1 \cdot r_2^{'} = 1$.

Example 2.1.8.
The set of real numbers $\mathbb{R}$ and set of complex numbers $\mathbb{C}$ are fields under usual operations '+' and '$\cdot$'.

Definition 2.1.9.
Modular Arithmetic [59], is an arithmetics system for integers. **Friedrich** was first who proposed the notion of modular arithmetic in his book named Disquisitiones Arithmeticae, published in 1801. It is defined as:
For any given integer n and any positive integer x, we get an integer known as quotient q and a remainder r, when x is divided by p, such that:

$$x = qp + r, \text{ where } 0 \leq r < p$$

Modular arithmetics have the following **Properties**:

1. $[(g \bmod p) + (h \bmod p)] \bmod p = (g + h) \bmod p$.

2. $[(g \bmod p) \times (h \bmod p)] \bmod p = (g \times h) \bmod p$.

3. $[(g \bmod p) - (h \bmod p)] \bmod p = (g - h) \bmod p$.

Definition 2.1.10.
The **order of a finite field** must be a power of a prime p^n, where n is a positive integer and p is a prime number.
Generally the finite field of order p^n is represented as $G\mathbb{F}(p^n)$ known as **Galois field**. It is named in the honor of the mathematician who first studied the finite fields.

For any given prime number p, the **finite field of order** p is a set of integers $\{0, 1, 2, \cdots p-1\}$ together with arithmetic operations modulo p. Finite field of order p is represented as $G\mathbb{F}(p)$.

Example 2.1.11.

1. $G\mathbb{F}(3) = \{0, 1, 2\}$ under binary operations $(+, \cdot)$ modulo 3.
2. The simplest finite field is $G\mathbb{F}(2)$ [59]. Its arithmetic operations are given by:

   Addition

+	0	1
0	0	1
1	1	0

   Multiplication

×	0	1
0	0	0
1	0	1

   where Addition is Exclusive-OR (XOR) operation and multiplication is AND operation.

Definition 2.1.12.
The positive integer d will be the **greatest common divisor** of p and q if

1. p and q are divisible by d.
2. d is divisible by the divisors of p and q.

$$\gcd\,(p,\, q) = \max\,\{h \text{ , such that } h|p \text{ and } h|q\}.$$

The **Eucledian algorithm** [59] is based on the following theorem. For any positive integer p and q,

$$\gcd(p,\, q) = \gcd\,(q,\, p \bmod q)$$

The Eucledian algorithm uses the above equation to find greatest common divisor as follows:

Algorithm 2.1.13.

1. $L \leftarrow p; M \leftarrow q$
2. if $M = 0$ return $L = \texttt{gcd}(p, q)$
3. $K = L \bmod M$
4. $L \leftarrow M$
5. $M \leftarrow K$
6. goto 2

Example 2.1.14.

The gcd$(252, 105)$ is calculated as:

$$252 = 105 \times 2 + 42$$
$$105 = 42 \times 2 + 21$$
$$42 = 21 \times 2 + 0$$

so gcd $(252, 105) = 21$.

It is easy to find the **Multiplicative inverse [59] in** $G\mathbb{F}(p)$. The multiplicative inverse of m under modulo n exists, if gcd $(n, m) = 1$, We have the following algorithm for finding the multiplicative inverse:

Algorithm 2.1.15.

1. $(L_1, L_2, L_3) \leftarrow (1, 0, n); (M_1, M_2, M_3) \leftarrow (0, 1, m)$.
2. If $M_3 = 0$ returns $L_3 =$ gcd (n, m); no inverse.
3. If $L_3 = 1$ returns $M_3 =$ gcd $(n, m); M_2 = m^{-1} \bmod n$.
4. $Q = \dfrac{L_3}{M_3}$.
5. $(U_1, U_2, U_3) \leftarrow (L_1 - QM_1, L_2 - QM_2, L_3 - QM_3)$.

6. $(L_1, L_2, L_3) \leftarrow (M_1, M_2, M_3)$.

7. $(M_1, M_2, M_3) \leftarrow (U_1, U_2, U_3)$.

8. goto 2.

Example 2.1.16.

The multiplicative inverse of 4 modulo 7 is computed as follow:

TABLE 2.2: Multiplicative Inverse

Q	L_1	L_2	L_3	M_1	M_2	M_3
–	1	0	7	0	1	4
1	0	1	4	1	−1	3
1	1	−1	3	−1	2	1

In the above Table, L_3 is taken as 7 and M_3 is 4. The values of L_1 and L_2 are 1 and 0 respectively. The values of M_1 and M_2 are 0 and 1 respectively by using point 1. By dividing 7 by 4 and get $Q = 1$ by using 4.

Now in the next step L_3 will replaced by M_3 of first step and taken as 4. L_1 and L_2 values are also replaced by M_1 and M_2 of first step. The value of M_3 will be now taken as 3 which is the remainder of first step.

In the second step the values of M_1 and M_2 are calculated by using 5:

$M_1 = L_1 - M_1 \times Q$ and

$M_2 = L_2 - M_2 \times Q$.

For 2nd row: $M_1 = 1 - 1(0) = 1$ and $M_2 = 0 - 1(1) = -1$. The values of L_1 and L_2 are taken from 1st row and Q is taken from 2nd row.

Similarly the values of L_1, L_2 and L_3 are replaced by M_1, M_2 and M_3 of previous step respectively.

For 3rd row: $M_1 = 0 - 1(1) = -1$ and $M_2 = 1 - 1(-1) = 2$. The values of L_1 and L_2 are taken from 2nd row and Q is taken from 3rd row.

so $4^{-1} \bmod 7 = 2$.

To check that $4^{-1} \bmod 7 = 2$ multiply 4 by 2,

$4 \times 2 = 8 \bmod 7 = 1$.

2.2 Elliptic Hypercurves

This section will help the reader to understand all the basic and related concepts of Chapter 4 of this thesis.

Definition 2.2.1.

Let K be a nonempty set and $P^*(K)$ be set of all nonempty subsets of K. **Hyperoperation** '$\circ$' on K is defined by a mapping as:

$$\circ : K \times K \to P^*(K) \mid (k_1, k_2) \to (k_1 \circ k_2).$$

The pair $(K, \circ)$ is called the **Hypergroupoid**.

The set $k_1 \circ k_2$ is called the **Hyperproduct** of k_1 and k_2, for all $k_1, k_2 \in K$. [27].

Definition 2.2.2.

The operation $*$ on $P^*(K)$ is determined by the operation $\circ$ in the following sense:

$$* : P^*(K) \times P^*(K) \to P^*(K)$$

such that,

$$U * V = \bigcup_{(k_1,k_2)\in U\times V} (k_1 \circ k_2) \tag{2.1}$$

Where, $U, V \in P^*(K)$.

Definition 2.2.3.

A **Semi-hypergroup** K [25] is a nonempty set endowed with an associative hyperproduct '$\circ$' *i.e.*,

$$(k_1 \circ k_2) \circ k_3 = k_1 \circ (k_2 \circ k_3)$$

for all $k_1, k_2, k_3 \in K$.

Example 2.2.4.

Let $(K, \circ)$ be a semi-hypergroup on $K = \{0, \ell, m, n, p, 1\}$ with the hyperoperation $\circ$ given by the following table [31]:

TABLE 2.3: Semi-Hypergroup under Hyperoperation '$\circ$'

$\circ$	0	ℓ	m	n	p	1
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
ℓ	$\{0\}$	$\{1,\ell\}$	$\{\ell,m,1\}$	$\{0,\ell,m,n\}$	K	$\{\ell\}$
m	$\{0\}$	$\{0,m\}$	$\{m\}$	$\{m,p,1\}$	$\{0,1,m,p\}$	$\{m\}$
n	$\{0\}$	$\{n\}$	$\{n,p\}$	$\{n\}$	$\{n,p\}$	n
p	$\{0\}$	$\{0,p\}$	$\{0,p\}$	$\{0,p\}$	$\{0,p\}$	$\{p\}$
1	$\{0\}$	$\{\ell\}$	$\{m\}$	$\{n\}$	$\{p\}$	$\{1\}$

First we will show that $\ell \circ (m \circ n) = (\ell \circ m) \circ n$.

Consider $\ell \circ (m \circ n)$.

From Table 2.3, $m \circ n = \{m, p, 1\}$ then,

$$\begin{aligned}
\ell \circ (m \circ n) &= \ell \circ \{m, p, 1\} \\
&= \bigcup_{v \in (m \circ n)} \ell \circ v \\
&= (\ell \circ m) \cup (\ell \circ p) \cup (\ell \circ 1) \\
&= \{\ell, m, 1\} \cup K \cup \{\ell\} \\
\ell \circ (m \circ n) &= \{0, \ell, m, n, p, 1\}.
\end{aligned}$$

where $(\ell \circ m) = \{\ell, m, 1\}$, $(\ell \circ p) = K$ and $(\ell \circ 1) = \{\ell\}$.

Now consider $(l \circ m) \circ n$.

From Table 2.3, $(\ell \circ m) = \{\ell, m, 1\}$. Then,

$$\begin{aligned}
(\ell \circ m) \circ n &= \{\ell, m, 1\} \circ n \\
&= \bigcup_{u \in (m \circ n)} \ell \circ n \\
&= (\ell \circ n) \cup (m \circ n) \cup (1 \circ n) \\
&= \{0, \ell, l, n\} \cup \{m, p, 1\} \cup \{n\} \\
&= \{0, \ell, m, n, p, 1\}
\end{aligned}$$

where $(\ell \circ n) = \{0, 1, \ell, n\}$, $(m \circ n) = \{m, p, 1\}$ and $(1 \circ n) = \{n\}$.

Similarly, one can show that

$$k_1 \circ (k_2 \circ k_3) = (k_1 \circ k_2) \circ k_3$$

for all $k_1, k_2, k_3 \in K$.

Hence $\{0, \ell, m, n, p, 1\}$ is a semi-hypergroup.

Definition 2.2.5.

A semi-hypergroup K endowed with the hyperoperation '$\circ$' is a **hypergroup**, if it satisfies the following axiom:

$$k \circ K = K \circ k = K.$$

for all $k \in K$, where

$$k \circ K = \bigcup_{k' \in K} k \circ k',$$

and

$$K \circ k = \bigcup_{k' \in K} k' \circ k.$$

This property is called reproducibility [25].

Example 2.2.6.

Let $K = \{0, 1, 2\}$ is a hypergroup with the hyperoperations '$\circ$':

TABLE 2.4: Hypergroup under Hyperoperation '$\circ$'

$\circ$	0	1	2
0	$\{0\}$	$\{0\}$	$\{0, 1, 2\}$
1	$\{1\}$	$\{1\}$	$\{0, 1, 2\}$
2	$\{2\}$	$\{2\}$	$\{0, 1, 2\}$

As it is a hypergroup so it must be a semi-hypergroup [27] such that

$$k_1 \circ (k_2 \circ k_3) = (k_1 \circ k_2) \circ k_3$$

for all $k_1, k_2, k_3 \in K$.

Let $k = 1$, so

$$\begin{aligned} k \circ K &= 1 \circ \{0,1,2\} \\ &= (1 \circ 0) \cup (1 \circ 1) \cup (1 \circ 2) \\ &= \{1\} \cup \{1\} \cup \{0,1,2\} \\ &= \{0,1,2\} \\ K \circ k &= \{0,1,2\} \circ 1 \\ &= (0 \circ 1) \cup (1 \circ 1) \cup (2 \circ 1) \\ &= \{0\} \cup \{1\} \cup \{2\} \\ &= \{0,1,2\} \\ &= K \end{aligned}$$

where from Table 2.8, $(1 \circ 0) = \{1\}$, $(1 \circ 1) = \{1\}$, $(1 \circ 2) = \{0,1,2\}$, $(0 \circ 1) = 0$, $(1 \circ 1) = \{1\}$ and $(2 \circ 1) = \{2\}$.
Similarly, one can satisfy

$$k \circ K = K \circ k$$

for all $k \in K$.

Definition 2.2.7.
A set $\mathbb{R}$ equipped with two hyperoperations, the hyperaddition '$\oplus$' and the hypermultiplication '$\odot$' is called a **Hyperring** [27] if:

1. $(\mathbb{R}, \oplus)$ is a hypergroup *i.e.*,

$$k_1 \oplus K = K$$

2. $(\mathbb{R}, \odot)$ is a semi-hypergroup *i.e.*,

$$(k_1 \odot k_2) \odot k_3 = k_1 \odot (k_2 \odot k_3)$$

3. $\mathbb{R}$ distributive with respect to hyperaddition '$\oplus$' *i.e.*,

$$k_1 \odot (k_2 \oplus k_3) = (k_1 \odot k_2) \oplus (k_1 \odot k_3)$$

Example 2.2.8.

The set $\mathbb{R} = \{0, 1\}$ with the hyperoperation $\oplus$ and $\odot$ as defined below is a hyper-ring.

Hyperaddition $\oplus$

$\oplus$	0	1
0	$\{0\}$	$\{0,1\}$
1	$\{0,1\}$	$\{1\}$

Hypermultiplication $\odot$

$\odot$	0	1
0	$\{0\}$	$\{0\}$
1	$\{0,1\}$	$\{0,1\}$

Definition 2.2.9.

A **canonical hypergroup** [58] is a set $\mathbb{S}$, with a binary hyperoperation $\oplus$, if it satisfies the following properties:

1. $s_1 \oplus (s_2 \oplus s_3) = (s_1 \oplus s_2) \oplus s_3$, for all $s_1, s_2, s_3 \in \mathbb{S}$.
2. $s_1 \oplus s_2 = s_2 \oplus s_1$, for all $s_1, s_2 \in \mathbb{S}$.
3. For every $s_1 \in \mathbb{S}$, there exists $0 \in \mathbb{S}$, $0 \oplus \{s_1\} = \{s_1\}$.
4. For every $s_1 \in \mathbb{S}$ there exists a unique element $s_1^{'} \in \mathbb{S}$ such that $0 \in s_1 \oplus s_1^{'}$. ($-s_1$ can be written for $s_1^{'}$ and called as the opposite of s_1).
5. If $s_3 \in s_1 \oplus s_2$, then $s_2 \in s_3 \oplus (-s_1)$ and $s_1 \in s_3 \oplus (-s_2)$.

Example 2.2.10.

Let $\mathbb{S} = \{0, t, w\}$ [62]. Then $\mathbb{S}$ with hyperaddition $\oplus$ as defined in the following table:

TABLE 2.5: Canonical Hypergroup under Hyperaddition '$\oplus$'

$\oplus$	0	t	w
0	$\{0\}$	$\{t\}$	$\{w\}$
t	$\{t\}$	$\{0,t\}$	$\{w\}$
w	$\{w\}$	$\{w\}$	$\{0,t,w\}$

is a cannonical hypergroup.

Definition 2.2.11.

A set $\mathbb{S}$ equipped with binary hyperoperations '$\oplus$' and '$\odot$' is a **Krasner hyperring** [52] if it holds the following axioms:

1. $(\mathbb{S}, \oplus)$ is a cannonical hypergroup.
2. $(\mathbb{S}, \odot)$ is a semi-hypergroup with zero which is a bilaterally absorbing element *i.e.*, $s_1 \odot 0 = 0 \odot s_1 = 0$.
3. The multilpication is distributive under the hyperoperation $\oplus$ [27].
   Moreover, A Krasner hyperring $(\mathbb{S}, \oplus, \odot)$ is called commutative, if $(\mathbb{S}, \odot)$ is a commutative semi-hypergroup with a unit element *i.e.*, $s_1 \odot s_2 = s_2 \odot s_1$.

Example 2.2.12.

Let a set $\mathbb{S} = \{0, r, s, t\}$ with hyperaddition '$\oplus$' and hypermultiplication '$\odot$' is a Krasner hyperring [27].

Hyperaddition $\oplus$

$\oplus$	0	r	s	t
0	$\{0\}$	$\{r\}$	$\{s\}$	$\{r\}$
r	$\{r\}$	$\{0, s\}$	$\{r, t\}$	$\{s\}$
s	$\{s\}$	$\{r, t\}$	$\{0, s\}$	$\{r\}$
t	$\{t\}$	$\{s\}$	$\{r\}$	$\{0\}$

Hypermultiplication $\odot$

$\odot$	0	r	s	t
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
r	$\{0\}$	$\{r\}$	$\{s\}$	$\{t\}$
s	$\{0\}$	$\{s\}$	$\{s\}$	$\{t\}$
t	$\{0\}$	$\{t\}$	$\{0\}$	$\{t\}$

Definition 2.2.13.

A Krasner hyperring $(\mathbb{S}, \oplus, \odot)$ is called a **Krasner hyperfield**, if $(\mathbb{S} \setminus \{0\}, \odot)$ is a hypergroup [6].

If each $x \neq 0 \in \mathbb{S}$ has a multiplicative inverse then $(S, \oplus, \odot)$ is a hyperfield.

Example 2.2.14.

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite set with two elements, then $\mathbb{F}_2$ becomes a Krasner hyperfield with the following hyperoperations [35]:

Hyperaddition $\oplus$

$\oplus$	0	1
0	$\{0\}$	$\{1\}$
1	$\{1\}$	$\{0,1\}$

Hypermultiplication $\odot$

$\odot$	0	1
0	$\{0\}$	$\{0\}$
1	$\{0\}$	$\{1\}$

Definition 2.2.15.

Let $(\mathbb{F}, \oplus, \odot)$ be a field and $\mathbb{G}$ be a normal subgroup of $(\mathbb{F}^* = \mathbb{F} \setminus \{0\}, \odot)$. Take $\frac{\mathbb{F}}{\mathbb{G}} = \{p\mathbb{G} | p \in \mathbb{F}\}$ under the hyperaddition '$\oplus$' and multiplication '$\odot$' given by

i) $p\mathbb{G} \oplus q\mathbb{G} = \{r\mathbb{G} | r \in p\mathbb{G} + q\mathbb{G}\}$

ii) $p\mathbb{G} \odot q\mathbb{G} = \{pq\mathbb{G}\}$

for all $p\mathbb{G}, q\mathbb{G} \in \frac{\mathbb{F}}{\mathbb{G}}$, then $\left(\frac{\mathbb{F}}{\mathbb{G}}, \oplus, \odot\right)$ is a hyperfield. Denote $\overline{p} = p\mathbb{G}$ and $\overline{q} = q\mathbb{G}$ then $\frac{\overline{\mathbb{F}}}{\mathbb{G}} = (\mathbb{F}, \oplus, \odot)$ is known as **Constructed hyperfield** or **Quotient Krasner hyperfield** [5].

For all $X \subseteq \mathbb{F}$,

$$\overline{L} = \{\overline{\ell} \,| \ell \in L\}$$

and for all $M \subseteq \mathbb{F}^2$,

$$\overline{M} = \{\overline{(\ell, m)} \mid (\ell, m) \in M\}$$

where $\overline{(\ell, m)} = (\overline{\ell}, \overline{m})$.

Definition 2.2.16.

If for every $a \in \mathbb{G}$, there exists $b \in \mathbb{G}$ such that $b^2 = a$, then the group $\mathbb{G}$ is called single [61].

Example 2.2.17.

Conisder $F = \mathbb{Z}_7$. By using Definition 2.2.16, $\mathbb{G}$ can be computed as:

$1^2 \mod 7 = 1$, $2^2 \mod 7 = 4$, $3^2 \mod 7 = 2$,
$4^2 \mod 7 = 2$, $5^2 \mod 7 = 4$ and $6^2 \mod 7 = 1$

then we have $\mathbb{G} = \{1, 2, 4\}$.

By using $\overline{F} = \{p\,\mathbb{G}, p \in F\}$, we can compute the set $\overline{F}$ as:

$$\begin{aligned}
&p = 0, \text{ then } p\mathbb{G} = 0\{1,2,4\} = 0,\\
&p = 1, \text{then } 1\{1,2,4\} = \{1,2,4\},\\
&p = 2, \text{ then } 2\{1,2,4\} \mod 7 = \{2,4,1\},\\
&p = 3, \text{ then } 3\{1,2,4\} \mod 7 = \{3,6,5\},\\
&p = 4, \text{ then } 4\{1,2,4\} \mod 7 = \{4,1,2\},\\
&p = 5, \text{ then } 5\{1,2,4\} \mod 7 = \{5,3,6\},\\
&p = 6, \text{ then } 6\{1,2,4\} \mod 7 = \{6,5,3\}.
\end{aligned}$$

Hence we are getting same sets on $1, 2, 4$ and $3, 6, 5$. We can say that $1 = 2 = 4$ and $3 = 5 = 6$.
Also we know that $\overline{p} = p\mathbb{G}$, so these values can be written as

$$\overline{1} = \overline{2} = \overline{4},$$

and

$$\overline{3} = \overline{5} = \overline{6}.$$

So we have,

$$\overline{F} = \{\bar{0}, \bar{1}, \bar{3}\}.$$

Hyperaddition $\oplus$ and hypermultiplication $\odot$ on $\overline{\mathbb{F}}$ is given by the following table [61]:

TABLE 2.6: Hyperaddition

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{3}$
$\bar{0}$	$\{\bar{0}\}$	$\{\bar{1}\}$	$\{\bar{3}\}$
$\bar{1}$	$\{\bar{1}\}$	$\{\bar{1},\bar{3}\}$	$\{\bar{0},\bar{1},\bar{3}\}$
$\bar{3}$	$\{\bar{3}\}$	$\{\bar{0},\bar{1},\bar{3}\}$	$\{\bar{1},\bar{3}\}$

TABLE 2.7: Hypermultiplication

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{3}$
$\bar{0}$	$\{\bar{0}\}$	$\{\bar{0}\}$	$\{\bar{0}\}$
$\bar{1}$	$\{\bar{0}\}$	$\{\bar{1}\}$	$\{\bar{3}\}$
$\bar{3}$	$\{\bar{0}\}$	$\{\bar{3}\}$	$\{\bar{1}\}$

The values in Table 2.6 are computed as follows:

By Definition 2.2.15, $\bar{1} \oplus \bar{3}$ is computed as:

$$\begin{aligned}
\bar{1} &= 1G = 1 \times \{1,2,4\} = \{1,2,4\}.\\
\bar{3} &= 3G = 3 \times \{1,2,4\} \mod 7 = \{3,6,5\}.\\
\bar{1} \oplus \bar{3} &= \{1,2,4\} + \{3,6,5\}\\
&= \{1+3, 1+6, 1+5, 2+3, 2+5, 2+6, 4+3, 4+5, 4+6\} \mod 7\\
&= \{4,7,6,6,8,7,7,10,9\} \mod 7\\
&= \{4,0,6,6,1,0,0,3,2\} \mod 7\\
&= \{\bar{4},\bar{0},\bar{6},\bar{3},\bar{2}\}\\
\bar{1} \oplus \bar{3} &= \{\bar{0},\bar{1},\bar{3}\}.
\end{aligned}$$

Here $\bar{4} = \bar{2} = \bar{1}$ and $\bar{3} = \bar{6}$.

Similarly other values of Table 2.6 can be computed.

By using Definition 2.2.15, the values in Table 2.7 are computed as follows:

$$\begin{aligned}
\bar{3} &= \{3,6,5\}\\
\bar{3} \odot \bar{3} &= 3 \times 3 \times \{1,2,4\}\\
&= 9 \times \{1,2,4\}\\
&= \{9,18,36\} \mod 7\\
&= \{2,4,1\}.\\
\bar{3} \odot \bar{3} &= \bar{1}.
\end{aligned}$$

Here $\bar{1} = \bar{2} = \bar{4}$

Similarly other values in Table 2.7 can be calculated.

Definition 2.2.18.

Let $(\mathbb{R}_1, +, \cdot)$ and $(\mathbb{S}_1, \oplus, \odot)$ be two hyperrings. A map

$$f : \mathbb{R}_1 \to \mathbb{S}_1$$

is called **homomorphism of hyperring** if the following conditions are satisfied.

1. $f(r_1 + r_2) \subseteq f(r_1) \oplus f(r_2)$, for all $r_1, r_2 \in R_1$.
2. $f(r_1 \cdot r_2) = f(r_1) \odot f(r_2)$, for all $r_1, r_2 \in R_1$ [5].

Definition 2.2.19.

The map

$$f : \mathbb{R}_1 \to \mathbb{S}_1$$

is said to be an **epimorphism** if it is a surjective homomorphism such that:

$$p \oplus q = \cup\{f(r_1 + r_2) \mid f(s_1) = p, f(s_2) = q\}, \text{ for all } r_1, r_2 \in \mathbb{R}_1, p, q \in \mathbb{S}_1 \text{ [57]}.$$

Definition 2.2.20.

The map

$$f : \mathbb{R}_1 \to \mathbb{S}_1$$

is called **isomorphism** if it is bijective homomorphism satisfying:

$$f(r_1 + r_2) = f(r_1) \oplus f(r_2), \text{ for all } r_1, r_2 \in \mathbb{R}_1 \text{ [57]}.$$

Definition 2.2.21.

A hypergroup K equipped with hyperoperation $\circ$ is called **regular hypergroup** if it has at least an identity element and all elements of K has at least an inverse (each element has at least one inverse) [3].

In other words there exists $e \in K$, for all $k_1 \in K$, such that

$$k_1 \in (k_1 \circ e) \cap (e \circ k_1) \tag{2.2}$$

and also there exists $k_1^{'} \in K$ such that

$$e \in (k_1 \circ k_1^{'}) \cap (k_1^{'} \circ k_1) \tag{2.3}$$

The element $k_1^{'}$ satisfying Equation (2.3) is called inverse of k_1.

Example 2.2.22.

Let $K = \{t_1, t_2, t_3, t_4\}$ and define the hyperproduct '$\circ$' on K as follows [27]:

Let $e = t_1$. From Table 2.8, it can be seen that

TABLE 2.8: Regular Hypergroup with Hyperproduct '$\circ$'

$\circ$	t_1	t_2	t_3	t_4
t_1	$\{t_1\}$	$\{t_1\}$	$\{t_1, t_2, t_3\}$	$\{t_1, t_2, t_4\}$
t_2	$\{t_1\}$	$\{t_1\}$	$\{t_1, t_2, t_3\}$	$\{t_1, t_2, t_4\}$
t_3	$\{t_1, t_2, t_3\}$	$\{t_1, t_2, t_3\}$	$\{t_1, t_2, t_3\}$	$\{t_3, t_4\}$
t_4	$\{t_1, t_2, t_4\}$	$\{t_1, t_2, t_4\}$	$\{t_3, t_4\}$	$\{t_1, t_2, t_4\}$

$$t_2 \notin t_2 \circ t_1$$

Hence t_1 is not an identity element of K.

Again, from Table 2.8

$$t_2 \notin t_2 \circ t_2$$

so t_2 is also not an identity element of K.

By taking $e = t_3$, it can be seen from Table 2.8,

$$t_3 \in t_3 \circ t_1$$

$$t_3 \in t_3 \circ t_2$$

$$t_3 \in t_3 \circ t_3$$

$$t_3 \in t_3 \circ t_4$$

Therefore, $t_3 \in K$ satisfies Equation (2.2) and hence t_3 is an identity element of K.

Similary, for $e = t_4$, from Table 2.8, it is evaluated that:

$$t_4 \in t_4 \circ t_1,$$

$$t_4 \in t_4 \circ t_2,$$

$$t_4 \in t_4 \circ t_3,$$

$$t_4 \in t_4 \circ t_4.$$

Hence K has only two identity elements t_3 and t_4

The set of all identities of K will be denoted by $Id(K)$, such that

$$Id(K) = \{t_3, t_4\}.$$

The inverses of K can be computed by using Equation (2.3).

If $e = t_3$, then by using Equation (2.3), it can be seen from Table 2.8, that the inverse of t_1 w.r.t. t_3 is t_3 as it only belong to $t_1 \circ t_3$, such that

$$In_{t_3}(t_1) = \{t_3\}.$$

Similarly,

$$t_3(t_2) = \{t_3\}.$$

Also, by using Equation (2.3)

$$In_{t_3}(t_3) = \{t_1, t_2, t_3\}.$$

As from Table 2.8, it can be seen that

$$t_3 \in t_3 \circ t_1,$$

$$t_3 \in t_3 \circ t_2,$$

and

$$t_3 \in t_3 \circ t_3.$$

Moreover, the inverse of t_4 w.r.t identity element t_3 is given by

$$In_{t_3}(t_4) = \{t_4\}.$$

Similary, by taking $e = t_4$, the inverses of all elements of K w.r.t identity element t_4 computed by using Equation (2.3), are given by:

$$In_{t_4}(t_1) = \{t_4\},$$

$$In_{t_4}(t_2) = \{t_4\},$$

and

$$In_{t_4}(t_4) = \{t_1, t_2, t_4\}.$$

Further, inverse of t_3 w.r.t identity element t_4 is given by

$$In_{t_4}(t_3) = \{t_3\}.$$

Here the set of inverses of an element with respect to an identity element e is denoted by $In_e(k)$.

Definition 2.2.23.
If the following conditions are statisfied, then the hypergroup K is called **reversible hypergroup**.

1. K has atleast one identity e.
2. Every element $t_1 \in K$ has atleast an inverse *i.e.*, $In(t_1) \neq \emptyset$.
3. $t_1 \in t_2 \circ t_3 \Rightarrow t_2 \in t_1 \circ (-t_3)$ and $t_3 \in (-t_2) \circ t_1$, where $-t_3 \in In(t_3)$ and $-t_2 \in In(t_2)$ [3].

Definition 2.2.24.
$\mathcal{H}$ is a **subhypergroup** if and only if the following conditions are satisfied:

1. $h_1 \circ h_2 \subseteq \mathcal{H}$, for all $h_1, h_2 \in \mathcal{H}$.
2. $h_1 \circ \mathcal{H} = \mathcal{H} \circ h_1 = \mathcal{H}$, for all $h_1 \in \mathcal{H}$ [3].

Definition 2.2.25.
A hypergroupoid $\mathcal{H}$ equipped with a hyperoperation $\circ$ is called a H_v**-group** if it satisfies the following axioms:

1. $h_1 \circ (h_2 \circ h_3) \cap (h_1 \circ h_2) \circ h_3 \neq \emptyset$, for all $h_1, h_2, h_3 \in \mathcal{H}^3$ (Weak associativity).
2. $h_1 \circ \mathcal{H} = \mathcal{H} \circ h_1 = \mathcal{H}$, for all $h_1 \in \mathcal{H}$ (Reproduction).

2.3 Cryptographic Background

This section is about cryptogrpahic background in which reader will first study about cryptology and then will study about one of the important type of cryptology which is known as cryptogrphy.

2.3.1 Cryptology

The term cryptology is comes from two Greek words, Kryptos which means "hidden" and logos which means "words". It deals with conversion of plain text into cipher text and vice versa. Each user being transform the data using a secret key or keys.*i.e.*, information which is only known to them. The resulting encrypted text may be decrypted by anybody who knows the key to recover the hidden information. Cryptology has two main branches.

- Cryptography
- Cryptanalysis

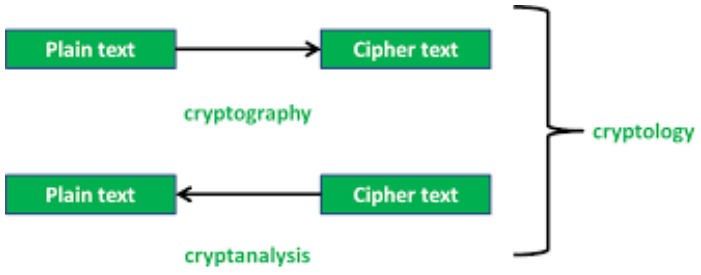

FIGURE 2.1: Types of Cryptology

2.3.2 Cryptography

The term cryptography was initially used by Thomas Browne, a British physician and writer [7]. It is originated from the Greek words: krypto, which means "hidden" and graphein means "writing or studying". It deals with the strategies

for securing information from anauthorized person. It is a method of preventing the public from accessing private communications. For this purpose there are alogorithms called Encryption and Decryption algorithm. The **encryption algorithm** is used for transforming plain text P(original information) into cipher text C(encrypted text), whereas the **decryption algorithm** is used for converting cipher text back into the plain text with the help of secrete **key** K. The key is a sensitive part of information that is used to convert plaintext to ciphertext during encryption process. A system that converts plain text into cipher text or cipher text back to the plain text using an encryption or decryption mechanism is known as **cryptosystem**.

The process of encryption and decryption is shown in Figure 2.2.

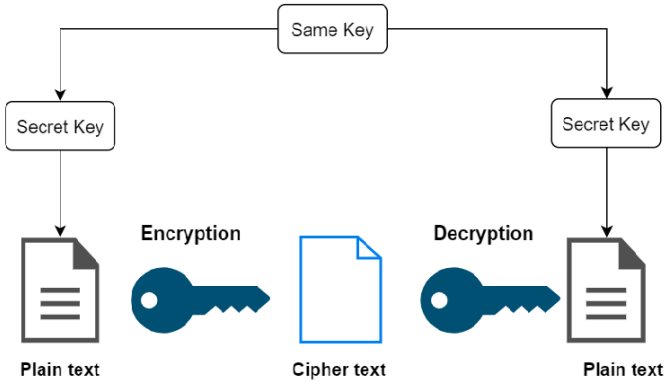

FIGURE 2.2: Cryptography

The cryptosystem consists of following basic components [60]:

- Plain text (P).
- Encryption algorithm (E).
- Cipher text (C).
- Decryption algorithm (D).
- Encryption Key (K_1).
- Decryption Key (K_2).

Cryptography consists of two main types:

1. Private Key Cryptography
2. Public Key Crpytography.

2.3.3 Private Key Cryptography

The private key cryptography is also known as Symmetric key cryptography. It is a system in which only a single key is shared between sender and reciever to encrypt as well as decrypt the data. The algorithm used for encryption and decrytion is known as Private key algorithm or symmetric algorithm.The key for encryption and decryption had to be known to all recipients otherwise the message could not be decrytped. It is very fast and simpler [20].
The examples of Symmetric key cryptography includes data encryption standard (DES) [23] and advanced encryption standard (AES) [23]. The process of private key cryptography is shown in the Figure 2.3.

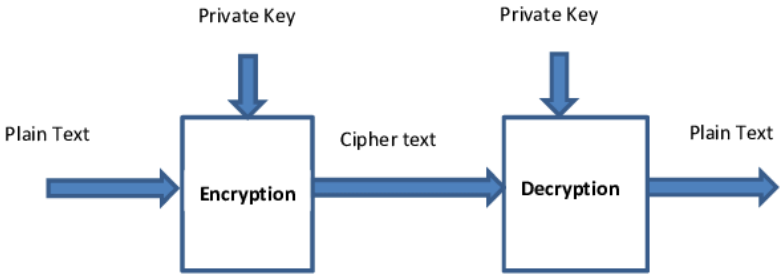

FIGURE 2.3: Private Key Cryptography

2.3.4 Public Key Cryptography

Public key cryptography was invented by whitefield Diffie and Marten Hellman in 1976 [21]. Public key cryptography is also known as Asymmetric key cryptography. In this cryptography two keys are required. One key is for encryption while other is for decryption. A key which is used for encrypting the actual information is

known as public key and the one which is for decrypting the encrypted information is known as private key. The public key is freely accessible for anyone, but the private key is kept strictly confidential [30].

Example of public key cryptography includes Digital signature algorithm(DSA) [40] and Elliptic curve cryptography (ECC) [8] and Rivest-Shamir-Adleman (RSA) [53].

The algorithm for Public key cryptography is shown in Figure 2.4.

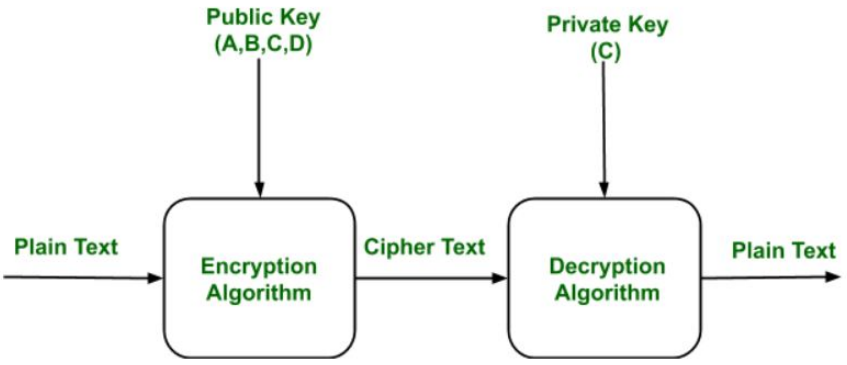

FIGURE 2.4: Public Key Cryptography

Chapter 3

Elliptic Curves

In this chapter we will discuss the basis concept related to real elliptic curve (EC) and elliptic curves over over finite field. It will help the reader to differentiate between the two. Also Elliptic Curve Cryptography (ECC) which is one of the branch of Public Key Cryptography will also be discussed.

3.1 Elliptic Curves over Real Numbers

Definition 3.1.1.

Let $(\mathbb{R}, +, \cdot)$ be a field and $u, v \in \mathbb{R}$. An **elliptic curve over real numbers** $\mathbb{E}_{u,v}(\mathbb{R})$ [11], denoted as $\mathbb{E}(\mathbb{R})$ is given by:

$$\mathbb{E}(\mathbb{R}) = \{(h, k) \in \mathbb{R}^2 | k^2 = h^3 + uh + v\} \cup \{\mathcal{O}\}. \tag{3.1}$$

where u and v are elements in $\mathbb{R}$. The Equation 3.1 is known as the **Weierstrass Equation**. The discriminant $\triangle = 16(4u^3 + 27v^2) \neq 0$. It impliesd that there is no singular point on the curve. For more details of elliptic curves, we refers to [69] [68].

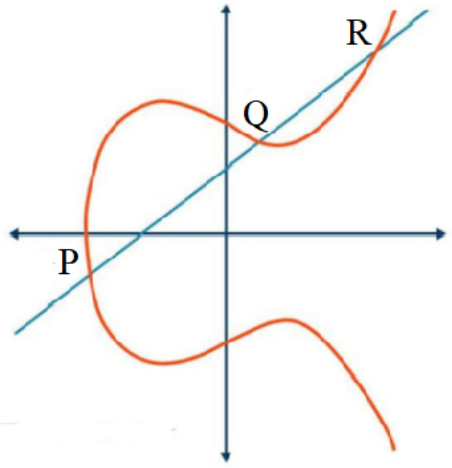

FIGURE 3.1: Elliptic Curve

3.1.1 Operations on Elliptic Curves over Real Numbers

The analytical formulae for adding two points on an elliptic curve over real numbers [11] are described here .

Consider the Weierstrass equation $k^2 = h^3 + uh + v$ on a field $\mathbb{R}$ and the two points $R = (h_1, k_1)$ and $S = (h_2, k_2)$ on elliptic curve $\mathbb{E}(R)$.

1. **Point Addition**

   If $R \neq S$, then the addition of these two points R and S is $R + S = T$, where $T = (h_3, k_3)$. The values of h_3 and k_3 are computed as follows:

   (i) $h_3 = s^2 - h_1 - h_2$.

   (ii) $k_3 = s(h_1 - h_3) - k_1$.

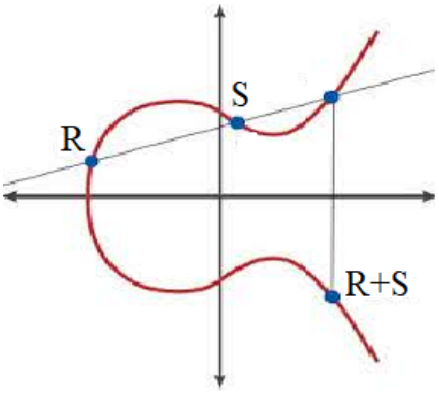

FIGURE 3.2: Points Addition

where $s = \dfrac{k_2 - k_1}{h_2 - h_1}$ is the slope of the line containing points R and S. The addition of these two points is shown in the Figure 3.2.

Note:

(a) If $R = \mathcal{O}$, then $R + \mathcal{O} = R$ (here $\mathcal{O}$ is the neutral element of group) for any point R.

(b) If $R = -S$, then $R + S = (-S) + S = 0$, ($-S$ is the inverse of S w.r.t group operation).

2. **Point Doubling**

If $R = S$, then $R + R = 2R$ where $2R = (h_3, k_3)$ and the values of h_3 and k_3 are computed as follows:

(i) $h_3 = s^2 - 2h_1$.

(ii) $k_3 = s(h_1 - h_3) - k_1$.

where $s = \dfrac{3h_1^2 + u}{2k_1}$.

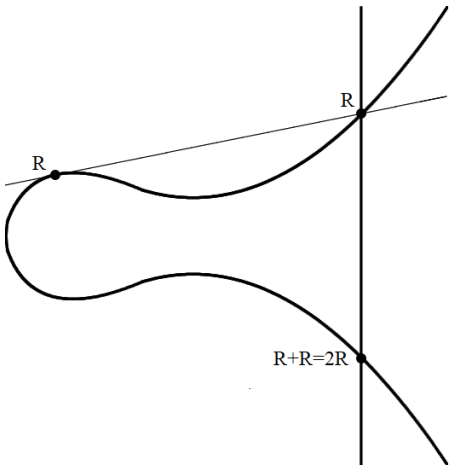

FIGURE 3.3: Point Doubling

The point doubling of these two points is shown in Figure 3.3.

3.2 Elliptic Curves over Finite Field $\mathbb{F}_p$

Definition 3.2.1.

Let $(\mathbb{F}, +, \cdot)$ be a field and $u, v \in \mathbb{F}$. An **elliptic curve** $E_{u,v}$ over finite field $\mathbb{F}_p$ denoted as $E_{u,v}(\mathbb{F}_p)$ is given by:

$$E_{u,v}(\mathbb{F}_p) = \{(h, k) \in \mathbb{F}^2 | k^2 = h^3 + uh + v\} \mod p. \tag{3.2}$$

where u and v are elements in $\mathbb{F}_p$. The Equation (3.2) is known as the **Weierstrass equation**.

3.2.1 Operations on Elliptic Curves over $\mathbb{F}_p$

1. **Point Addition**

   If $R \neq S$, then the addition of these two points R and S is $R + S = T$. The values of $T = (h_3, k_3)$ are computed as follows:

   (i) $h_3 = s^2 - h_1 - h_2 \mod p$.

   (ii) $k_3 = s(h_1 - h_3) - k_1 \mod p$.

   where $s = \dfrac{k_2 - k_1}{h_2 - h_1} \mod p$
   is the slope of the line containing points R and S.

   Note:

   (a) If $R = \mathcal{O}$, then $R + \mathcal{O} = R \mod p$ (here $\mathcal{O}$ is the neutral element of the group) for any point R).

   (b) If $R = -S$, then $R + S = (-S) + S = \mathcal{O} \mod p$, ($-S$ is the inverse of S w. r. t group operation).

2. **Point Doubling**

   If $R = S$, then $R + R = 2R = (h_3, k_3)$ and the values of h_3 and k_3 are computed as follows:

   (i) $h_3 = s^2 - 2h_1 \mod p$.

(ii) $k_3 = s(h_1 - h_3) - k_1 \mod p.$

where $s = \dfrac{3h_1^2 + u}{2k_1} \mod p.$

Example 3.2.2.

The points on elliptic curve $E_{0,2}(\mathbb{Z}_7)$ [61] are computed as follows:

The Weierstrass equation with $u = 0$ and $v = 2$ is $k^2 = (h^3 + 2) \mod p$. The points of this equation can be computed as follows:

h	$(h^3+2) \mod 7.$
0	2
1	3
2	3
3	1
4	3
5	1
6	1

k	$k^2 \mod 7.$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

From the above tables only those points of h and k are selected which will satisfy the Weierstrass equation.

As it can be seen from table that at point $h = 0$ and at $k = 3$ and $k = 4$ we get

2. So we have points $(0, 3)$ and $(0, 4)$.

Similarly,

at $h = 3$ and $k = 1$,

at $h = 5$ and $k = 1$,

and

at $h = 6$ and $k = 1$,

we get 1, so points of (h, k) are $(3, 1), (5, 1)$ and $(6, 1)$. Also, at $h = 3$ and $k = 6$,

at $h = 5$ and $k = 6$,

and

at $h = 6$ and $k = 6$,

we get the same value *i.e.*, 1, then we have $(3, 6), (5, 6)$ and $(6, 6)$.

Then the following points lies on elliptic curve $E_{0,2}$:

$$(0,3),(0,4),(3,1),(3,6),(5,1),(5,6)$$

The values of $E_{0,2}(\mathbb{F}) + E_{0,2}(\mathbb{F})$ can be computed by using subsection 3.2.1.

$$\begin{aligned} E_{0,2}(\mathbb{F}) + E_{0,2}(\mathbb{F}) &= \{\mathcal{O},(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\} \\ &+ \{\mathcal{O},(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\} \end{aligned}$$

1. $\mathcal{O} + \mathcal{O} = \mathcal{O}$. It is obvious.

2. $\mathcal{O} + (0,3) = (0,3)$ by using point addition 1.
   Similarly, addition of all other points with $\mathcal{O}$ is computed.

3. Now computing $(0,3) + (0,3)$. As both points are same *i.e.*, $R = S$ so by using 2, the values of h_3 and k_3 are calculated.
   First, calculating the value of s as follows:

$$\begin{aligned} s &= \frac{3h_1^2 + u}{2k_1} \mod 7 \\ s &= \frac{3(0)+0}{2(3)} \mod 7 \\ &= \frac{0}{6} \mod 7 \\ &= 0. \end{aligned}$$

   The value of h_3 is computed as follows by using point doubling 2:

$$\begin{aligned} h_3 &= s^2 - 2h_1 \\ &= 0 - 2(0) \mod 7 \\ &= 0. \end{aligned}$$

   The value of k_3 is calculated as follows:

$$\begin{aligned} k_3 &= s(h_1 - h_3) - k_1 \mod p \\ &= \{0(0-0) - 3\} \mod 7 \\ &= -3 \mod 7 \\ &= 4. \end{aligned}$$

Then the values of (h_3, k_3) are:

$$(h_3, k_3) = (0, 4)$$

Point doubling of all other points which are same can be computed in the same way by using 2.

The calculation of all points which are not same *i.e.*, if $R \neq S$, can be computed by using 1.

Now computing the addition of points $(3, 1)$ and $(6, 6)$ as follows:

4. $(3, 1) + (6, 6)$.

First calculating the value of s as follows:

$$\begin{aligned} s &= \frac{6-1}{6-3} \mod 7 \\ &= \frac{5}{3} \mod 7 \\ &= 5(3)^{-1} \mod 7 \\ &= 5(5) \mod 7 = 25 \mod 7 \\ &= 4. \end{aligned}$$

Here $(3)^{-1} \mod 7 = 5$. The inverse of 3 mod 7 is calculated by using Algorithm 2.1.15.

Now the value of h_3 is computed by using 1:

$$\begin{aligned} h_3 &= \{s^2 - h_1 - h_2\} \mod 7 \\ &= (16 - 3 - 6) \mod 7 \\ &= 0. \end{aligned}$$

The value of k_3 is computed as follows by using 1:

$$\begin{aligned} k_3 &= \{s(h_1 - h_3) - k_1\} \mod 7 \\ &= (4(3-0) - 1) \mod 7 \\ &= 4. \end{aligned}$$

So, we have

$$(h_3, k_3) = (5, 6).$$

After computing all the points of $E_{0,2}(\mathbb{F})$ mod 7 the Cayley table is given as follows:

TABLE 3.1: Cayley Table of $E_{0,2}(\mathbb{F})$

$+$	$\mathcal{O}$	$(0,3)$	$(0,4)$	$(3,1)$	$(3,6)$	$(5,1)$	$(5,6)$	$(6,1)$	$(6,6)$
$\mathcal{O}$	$\mathcal{O}$	$(0,3)$	$(0,4)$	$(3,1)$	$(3,6)$	$(5,1)$	$(5,6)$	$(6,1)$	$(6,6)$
$(0,3)$	$(0,3)$	$(0,4)$	$\mathcal{O}$	$(6,1)$	$(5,6)$	$(3,1)$	$(6,6)$	$(5,1)$	$(3,6)$
$(0,4)$	$(0,4)$	$\mathcal{O}$	$(0,3)$	$(5,1)$	$(6,6)$	$(6,1)$	$(3,6)$	$(3,1)$	$(5,6)$
$(3,1)$	$(3,1)$	$(6,1)$	$(5,1)$	$(3,6)$	$\mathcal{O}$	$(6,6)$	$(0,3)$	$(5,6)$	$(0,4)$
$(3,6)$	$(3,6)$	$(5,6)$	$(6,6)$	$\mathcal{O}$	$(3,1)$	$(0,4)$	$(6,1)$	$(0,3)$	$(5,1)$
$(5,1)$	$(5,1)$	$(3,1)$	$(6,1)$	$(6,6)$	$(0,4)$	$(5,6)$	$\mathcal{O}$	$(3,6)$	$(0,3)$
$(5,6)$	$(5,6)$	$(6,6)$	$(3,6)$	$(0,3)$	$(6,1)$	$\mathcal{O}$	$(5,1)$	$(0,4)$	$(3,1)$
$(6,1)$	$(6,1)$	$(5,1)$	$(3,1)$	$(5,6)$	$(0,3)$	$(3,6)$	$(0,4)$	$(6,6)$	$\mathcal{O}$
$(6,6)$	$(6,6)$	$(3,6)$	$(5,6)$	$(0,4)$	$(5,1)$	$(0,3)$	$(3,1)$	$\mathcal{O}$	$(6,1)$

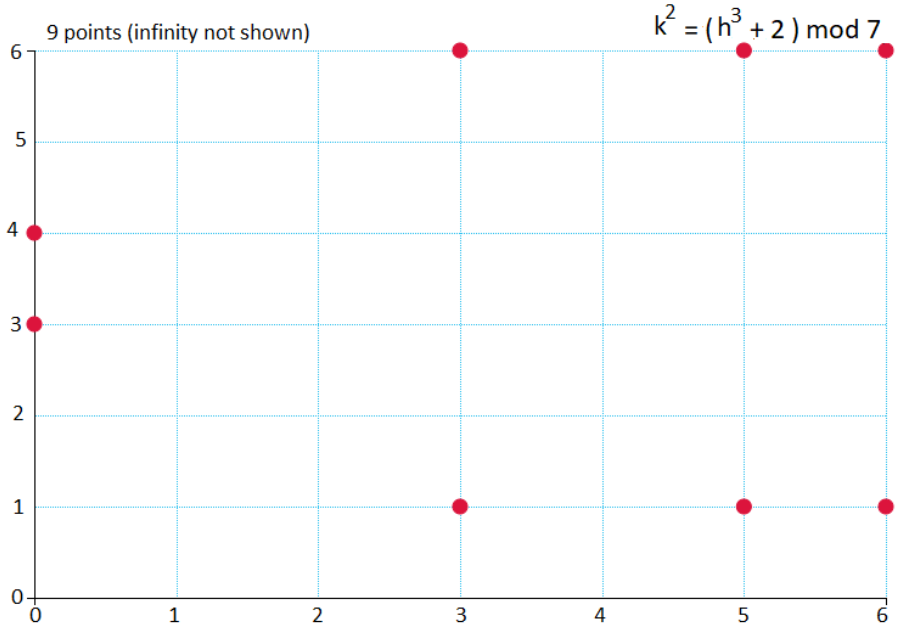

FIGURE 3.4: Graphical Representation of $k^2 = h^3 + 2 \mod 7$

The Figure 3.4 shows the graphical representation of base points of $E_{0,2}(\mathbb{F})$.

3.3 Elliptic Curve Cryptography

Miller and Koblitz [36] introduced one of the method based on elliptic curves is known as elliptic curve cryptography. Elliptic Curve Cryptography is a modern public-key encryption technology in which elliptic cutrves are used for generating smaller cryptographic keys. ECC is commonly used to encrypt data so that only authorised parties can decode it. RSA [53] and Diffie-Helman [21] are examples of elliptic curve cryptography.

3.3.1 ECC Deffie-Hellman Key Exchange

Deffie and **Hellman** [21] introduced public key cryptography in 1976. They key exchange [42] between users A and B using elliptic curves of the form $\mathbb{E}(u, v)(\mathbb{F}_p)$ in the following way:

1. User A chooses an integer $n_A < n$. Here n_A is private key. Then user A generates a public key:

$$P_A = n_A\, G \mod p.$$

2. similarly $n_B < n$ is a private key of user B. Public key generated by B is:

$$P_B = n_B\, G \mod p.$$

3. Secrete key generated by user A and user B are:

$$K_1 = n_A\, P_A$$
$$K_2 = n_B\, P_B$$

respectively. where G is the point on elliptic curve whose order is very large. The Deffie-Hellman Key Exchange protocol is given in Figure 3.5.

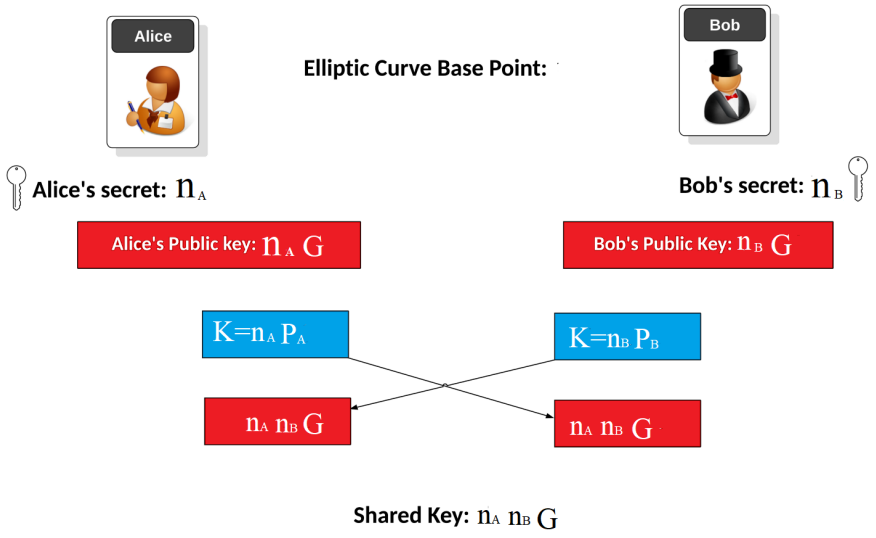

FIGURE 3.5: Deffie-Hellman Key Exchange

Definition 3.3.1.

Let E be an elliptic curve over a finite field $\mathbb{F}_p$, where $q = p^n$ and p is an integer. Problem to find an integer a given points $P, Q \in \mathbb{E}(F_p)$ in an equation:

$$Q = aP \mod p$$

is called **Elliptic Curve Discrete Logarithm Problem (ECDLP)** [47].
ECDLP is the basis of elliptic curve cryptography. It has been a important area of research in computing number theory and cryptography in last many decades. ECC security is dependent on the ECDLP.

Group Law

A commutative group structure is naturally defined by the points of elliptic curves. The **Group law** [26] is built mathematically, as follows:
Consider two points $R = (h_1, k_1)$ and $S = (h_2, k_2)$ on elliptic curve as shown in Figure 3.6.

1. Reflected point of R on elliptic curve E are denoted as $-R = (h_1, -k_1)$ with respect to x-axis.

   If $R \neq -S$, the line formed between R and S will cross the elliptic curve at precisely another point, represented by $R * S$. The point $R + S$ which is

addition of two points R and S is obtained by the reflection of $R * S$ with respect to x-axis on the elliptic curve E.

2. If $S = -R$, then the line formed between these point will not cross the elliptic curve at any other point. Because we need to define $R + (-R)$ as well, an extra point $\mathcal{O}$ is created as an ideal point at infinity. So $R + (-R) = \mathcal{O}$.

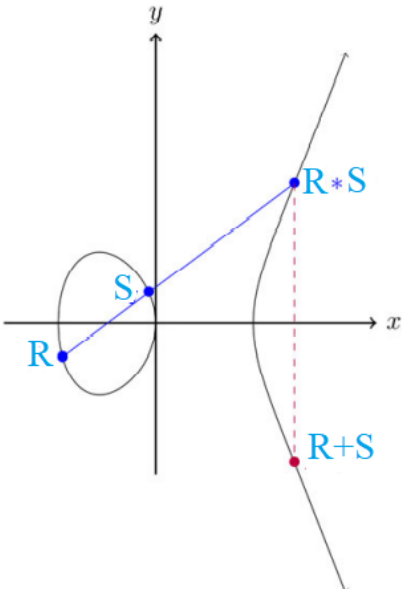

FIGURE 3.6: Points Addition on curve $k^2 = h^3 - 2h$

Note

The binary operation '+' defined in Definition 3.3.1 gives the set $E(\mathbb{F})$ which has an abelian group structure. In this set $\mathcal{O}$ is the identity element and the reflection of a point is representing the inverse of that point.

Chapter 4

Elliptic Hypercurves

The concept of elliptic hypercurve on a Krasner hyperfield is introduced in this chapter. The hyperoperations as a generalised group operation on field using elliptic hypercurves is highlighted in this chapter. We also investigate various characteristics of the related hypergroup and Hv-group. At the end of this chapter a class of canonical hypergroup will be constructed.

4.1 Elliptic Hypercurves

Definition 4.1.1.
By using Definition 2.2.15, let $\overline{F} = \left(\frac{\mathbb{F}}{G}, \oplus, \odot\right)$ be a Krasner quotient hyperfield and $\overline{U}, \overline{V} \in \overline{\mathbb{F}}^2$. Then the relation $\overline{k}^2 \in \overline{h}^3 \oplus \overline{Uh} \oplus \overline{V}$, for all $(\overline{h}, \overline{k}) \in \overline{\mathbb{F}}^2$, is called the **Generalized Weierstrass Equation**. Moreover, the set

$$E_{\overline{U},\overline{V}} = \{(\overline{h}, \overline{k}) \in \overline{F}^2 | \in \overline{k}^2 \in \overline{h}^3 \oplus \overline{Uh} \oplus \overline{V}\} \tag{4.1}$$

is called the **Weierstrass Hypercurves** on the Krasner hyperfield $\overline{\mathbb{F}}$ [61].
If

$$0 \notin \triangle_{\overline{U},\overline{V}} = \{4h^3 + 27k^2 | (h, k) \in \overline{U} \times \overline{V}\}$$

and the following implications holds:

$$E_{u,v} \cap E_{w,z} \neq \phi \Rightarrow E_{u,v} = E_{w,z}$$

for all $u, w \in \overline{U}, v, z \in \overline{V}$, where $E_{p,q} = \{(h,k) \in \mathbb{F}^2 \mid k^2 = h^3 + ph + q\}$, for all $(p,q) \in \mathbb{F}^2$, then $E_{\overline{U},\overline{V}}(\mathbb{F})$ is an elliptic hypercurve over $\overline{\mathbb{F}}$.

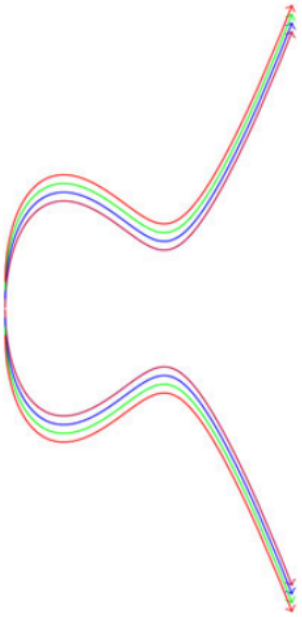

FIGURE 4.1: The Elliptic Hypercurve $E_{\overline{U},\overline{V}}(\mathbb{F})$

Theorem 4.1.

Let $\mathbb{F}$ be a field and $\mathbb{G}$ be a single group of $\mathbb{F}^*$. If $(\overline{U}, \overline{V}) \in \overline{\mathbb{F}}^2$, then the Weierstrass hypercurve

$$E_{\overline{U},\overline{V}} = \bigcup_{(u,v)\in\overline{U}\times\overline{V}} \overline{E}_{u,v}$$

where $\overline{E}_{u,v} = \{(\overline{h}, \overline{k}) \mid (h,k) \in E_{u,v}\}$.

Proof.

In order to prove that $E_{\overline{U},\overline{V}}$ which can be written as $\cup_{(u,v)\in\overline{U}\times\overline{V}}\overline{E}_{u,v}$. Consider $(\overline{h}, \overline{k})$ be an arbitrary elements in $E_{\overline{U},\overline{V}}$ such that by using Definition 4.1.1,

$$
\begin{aligned}
(\overline{h},\overline{k}) \in E_{\overline{U},\overline{V}} &\Rightarrow \overline{y}^2 \in \overline{h}^3 \oplus \overline{Uh} \oplus \overline{V} \\
&\Rightarrow \overline{k}^2 \in \overline{h^3 + \overline{U}h + \overline{V}} \\
&\Rightarrow \overline{k}^2 = \overline{h^3 + uh + v}, \text{ for some} (u,v) \in \overline{U} \times \overline{V} \\
&\Rightarrow k^2 g = h^3 + uh + v, \text{ for some} g \in \mathbb{G} \\
&\Rightarrow (hc)^2 = h^3 + uh + v, c^2 = g, \text{ for some} c \in \mathbb{G} \\
&\Rightarrow (h, kc) \in E_{u,v}, \text{for some} (u,v) \in \overline{U} \times \overline{V} \\
&\Rightarrow (\overline{h},\overline{k}) \in \bigcup_{(u,v)\in\overline{U}\times\overline{V}} \overline{E}_{u,v}.
\end{aligned}
$$

Thus $E_{\overline{U},\overline{V}} \subseteq \cup_{(u,v)\in\overline{U}\times\overline{V}}\overline{E}_{u,v}$. It is obvious that $\cup_{(u,v)\in\overline{U}\times\overline{V}}\overline{E}_{u,v} \subseteq E_{\overline{U},\overline{V}}$. □

Remarks 4.1.2.

Because $\mathcal{O}$ does not belong to $E_{\overline{U},\overline{V}}$ it follows that $(E_{u,v} \cup \{\mathcal{O}\}, \bullet_{uv})$ is an elliptic curve group, for all $(u,v) \in \overline{U} \times \overline{V}$, where $\bullet_{uv}$ is the group operation on the elliptic curve $E_{u,v} \cup \mathcal{O}$.

Example 4.1.3.

Let $\mathbb{F} = \mathbb{Z}_7$ be the field of the integers modulo 7. By using Example 2.2.17, then $\mathbb{G} = \{1, 2, 4\}$, where $\mathbb{G}$ is a normal subgroup of $(\mathbb{F}^*, \cdot)$ by Definition 2.2.13 and $\overline{\mathbb{F}} = \{\overline{0}, \overline{1}, \overline{3}\}$. The hyperoperations $(\oplus, \odot)$ defined on $\overline{\mathbb{F}}$ are as follows:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{3}$
$\overline{0}$	$\{\overline{0}\}$	$\{\overline{1}\}$	$\{\overline{3}\}$
$\overline{1}$	$\{\overline{1}\}$	$\{\overline{1},\overline{3}\}$	$\{\overline{0},\overline{1},\overline{3}\}$
$\overline{3}$	$\{\overline{3}\}$	$\{\overline{0},\overline{1},\overline{3}\}$	$\{\overline{1},\overline{3}\}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{3}$
$\overline{0}$	$\{\overline{0}\}$	$\{\overline{0}\}$	$\{\overline{0}\}$
$\overline{1}$	$\{\overline{0}\}$	$\{\overline{1}\}$	$\{\overline{3}\}$
$\overline{3}$	$\{\overline{0}\}$	$\{\overline{3}\}$	$\{\overline{1}\}$

where $\overline{0} = \{0\}$, $\overline{1} = \overline{2} = \overline{4}$, $\overline{3} = \overline{5} = \overline{6}$. The values of these tables are computed by using Definition 2.2.15. Points of elliptic hypercurve $E_{\overline{0},\overline{1}}$ are computed as follows:

$$E_{\overline{0},\overline{1}} = \{(\overline{h},\overline{k}) \in \overline{F}^2 | \overline{k}^2 \in \overline{h}^3 \oplus \overline{1}\} \mod 7$$

is a **Generalized Weierstrass Equation**. Where $\overline{U} = \overline{0}, \overline{V} = \overline{1}$.

TABLE 4.1: $(\overline{h}^3 \oplus \overline{1}) \mod 7$

$\overline{h}$	$(\overline{h}^3 \oplus \overline{1}) \mod 7$
$\overline{0}$	$\overline{0} \oplus \overline{1} = \{\overline{1}\}$.
$\overline{1}$	$\overline{1} \oplus \overline{1} = \{\overline{1}, \overline{3}\}$.
$\overline{3}$	$\overline{6} \oplus \overline{1} = \overline{3} \oplus \overline{1} = \{\overline{0}, \overline{1}, \overline{3}\}$.

TABLE 4.2: $\overline{k}^2 \mod 7$

$\overline{k}$	$\overline{k}^2 \mod 7$
$\overline{0}$	$\{\overline{0}\}$
$\overline{1}$	$\{\overline{1}\}$
$\overline{3}$	$\{\overline{1}\}$

From Table 4.1 and 4.2, points of elliptic hypercurve $E_{\overline{0},\overline{1}}$ can be computed. Only those points will be selected which are satisfying the generalized Weierstrass equation (4.1).

At $\overline{k} = \overline{0}$, from Table 4.2, we have

$$\overline{k}^2 \mod 7 = \{\overline{0}\}$$

and from Table 4.1, at $\overline{h} = \overline{3}$, we have

$$(\overline{h}^3 \oplus \overline{1}) \mod 7 = \{\overline{0}, \overline{1}, \overline{3}\}.$$

Hence, it can be seen that the pair $(\overline{h}, \overline{k}) = (\overline{3}, \overline{0})$ is satisfying Equation (4.1), such that

$$\{\overline{0}\} \in \{\overline{0}, \overline{1}, \overline{3}\}.$$

Therefore, $(\overline{h}, \overline{k}) = (\overline{3}, \overline{0})$.

Again, at $\overline{k} = \overline{1}$,

$$\overline{k}^2 \mod 7 = \{\overline{1}\}$$

and from Table 4.1, at $\overline{h} = \overline{1}$,

$$(\overline{h}^3 \oplus \overline{1}) \mod 7 = \{\overline{1}, \overline{3}\}.$$

Hence, it can be seen that the pair $(\overline{h}, \overline{k}) = (\overline{1}, \overline{1})$ is satisfying Equation (4.1), such that

$$\{\overline{1}\} \in \{\overline{1}, \overline{3}\}.$$

Similary, the following pairs of $(\overline{h}, \overline{k})$ satisfies the Equation (4.1)

$$(\overline{h}, \overline{k}) = (\overline{0}, \overline{1}).\ (\overline{h}, \overline{k}) = (\overline{3}, \overline{1}).\ (\overline{h}, \overline{k}) = (\overline{0}, \overline{3}).\ (\overline{h}, \overline{k}) = (\overline{1}, \overline{3}).\ (\overline{h}, \overline{k}) = (\overline{3}, \overline{3}).$$

Therefore,

$$E_{\overline{0},\overline{1}} = \{(\overline{3}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1}), (\overline{3}, \overline{1}), (\overline{0}, \overline{3}), (\overline{1}, \overline{3}), (\overline{3}, \overline{3})\}$$
$$0 \notin \triangle_{\overline{0},\overline{1}} = \{4h^3 + 27k^2 | (h, k) \in \overline{0} \times \overline{1}\}$$

Note that, $\overline{0} = \{0\}$ and $\overline{1} = 1 \times \{1, 2, 4\} = \{1, 2, 4\}$.
Hence,

$$\overline{0} \times \overline{1} = \{(0, 1), (0, 2), (0, 4)\}.$$

The values of $\triangle_{\overline{0},\overline{1}}$ can be computed by using values of (h, k) which are $(0, 1)$, $(0, 2)$ and $(0, 4)$.
At $h = 0, k = 1$,

$$\begin{aligned}(4h^3 + 27k^2) \mod 7 &= \left(4(0) + 27(1)^2\right) \mod 7 \\ &= 27 \mod 7 \\ &= 6.\end{aligned}$$

At $h = 0, k = 2$,

$$\begin{aligned}(4h^3 + 27k^2) \mod 7 &= \left(4(0) + 27(2)^2\right) \mod 7 \\ &= 108 \mod 7 \\ &= 3.\end{aligned}$$

and at $h = 0, k = 4$,

$$\begin{aligned}(4h^3 + 27k^2) \mod 7 &= \left(4(0) + 27(4)^2\right) \mod 7 \\ &= 432 \mod 7 \\ &= 5.\end{aligned}$$

Therefore,

$$\triangle_{\overline{0},\overline{1}} = \{3, 5, 6\}.$$

Points of $E_{0,1} : k^2 = (h^3 + 1) \mod 7$ can be computed by using Example 3.2.2 and are given as:

$$E_{0,1} = \{(3,0), (5,0), (6,0), (0,1), (0,6), (1,3), (2,3), (4,3), (1,4), (2,4), (4,4)\}.$$

Now computing the points of $\overline{E}_{0,1}$ by using Theorem 4.1,

$$\overline{E}_{u,v} = \{(\overline{h}, \overline{k}) | (h,k) \in E_{u,v}\}$$

we have,

$$\overline{E}_{0,1} = \{(\overline{3},\overline{0}), (\overline{5},\overline{0}), (\overline{6},\overline{0}), (\overline{0},\overline{1}), (\overline{0},\overline{6}), (\overline{1},\overline{3}), (\overline{2},\overline{3}), (\overline{4},\overline{3}), (\overline{1},\overline{4}), (\overline{2},\overline{4}), (\overline{4},\overline{4})\}.$$
$$\overline{E}_{0,1} = \{(\overline{0},\overline{1}), (\overline{0},\overline{3}), (\overline{1},\overline{3}), (\overline{1},\overline{1}), (\overline{3},\overline{0})\}.$$

Similarly the points of $E_{0,2} : k^2 = (h^3 + 2) \mod 7$ computed by using Example 3.2.2 are given as:

$$E_{0,2} = (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)$$

then,

$$\overline{E}_{0,2} = \{(\overline{0},\overline{3}), (\overline{0},\overline{4}), (\overline{3},\overline{1}), (\overline{3},\overline{6}), (\overline{5},\overline{1}), (\overline{5},\overline{6}), (\overline{6},\overline{1}), (\overline{6},\overline{6})\}.$$
$$\overline{E}_{0,2} = \{(\overline{0},\overline{3}), (\overline{0},\overline{1}), (\overline{3},\overline{1}), (\overline{3},\overline{3})\}.$$

Again by using Example 3.2.2 , points of $E_{0,4} : k^2 = (h^3 + 4) \mod 7$ are calculated and we get the following points:

$$E_{0,4} = \{(0, 2), (0, 5)\}$$

then,

$$\overline{E}_{0,4} = \{(\overline{0}, \overline{2}), (\overline{0}, \overline{5})\}$$
$$\overline{E}_{0,4} = \{(\overline{0}, \overline{1}), (\overline{0}, \overline{3})\}.$$

Also,
$\overline{E}_{0,1} \cup \overline{E}_{0,2} \cup \overline{E}_{0,4}$.
$= \{(\overline{0}, \overline{1}), (\overline{0}, \overline{3}), (\overline{1}, \overline{3}), (\overline{1}, \overline{1}), (\overline{3}, \overline{0})\} \cup \{(\overline{0}, \overline{3}), (\overline{0}, \overline{1}), (\overline{3}, \overline{1}), (\overline{3}, \overline{3})\} \cup \{(\overline{0}, \overline{1}), (\overline{0}, \overline{3})\}$.
$= \{(\overline{3}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1}), (\overline{3}, \overline{1}), (\overline{0}, \overline{3}), (\overline{1}, \overline{3}), (\overline{3}, \overline{3})\}$.
$= E_{\overline{0},\overline{1}}$.
In this case $E_{\overline{0},\overline{1}}(F)$ is an elliptic hypercurve because, $0 \notin \triangle_{\overline{0},\overline{1}}$ and from $E_{0,1}$, $E_{0,2}$ and $E_{0,4}$, we have

$$E_{0,1} \cap E_{0,2} = E_{0,1} \cap E_{0,4} = E_{0,2} \cap E_{0,4} = \emptyset.$$

4.2 Expanding Group operation to a Hyperoperation

The hyperoperations which are the expansions of group operations on elliptic curves will be described in the next section. Assume $\mathbb{F}$ is a random field and $\mathbb{G}$ is a single subgroup of $(\mathbb{F}^*, \cdot)$. Consider the subrgroup $\mathcal{G}$ of $\mathbb{F}^*$ defined by:

$$\mathcal{G} = \begin{cases} \mathbb{G} & \text{if } \mathbb{G} = \{1\} \\ \{h \in \mathbb{F} | h^2 = 1_{\mathbb{F}}\}, & \text{if } \mathbb{G} \neq \{1\} \end{cases} \tag{4.2}$$

where 1 is the identity element of the group $\mathbb{G}$ and $|\mathcal{G}| = 2$ *i.e.*, $\mathcal{G} = \{1_{\mathbb{F}}, -1_{\mathbb{F}}\}$ when $\mathbb{G}$ is the group which consists of more than one element (trivial group).

4.2.1 Hyperoperation $\circ_{\mathbb{G}}$

If $E_{\overline{U},\overline{V}}$ is an elliptic hypercurve with $\overline{U}$and $\overline{V}$, $\{\mathcal{O}\} \notin \cup_{(u,v)\in\overline{U}\times\overline{V}} E_{u,v}$, define a hyperoperation $\circ_{\mathbb{G}}$ on the set

$$E_{\overline{U},\overline{V}}(\mathbb{F}) = \cup_{(u,v)\in\overline{U}\times\overline{V}} E_{u,v}(\mathbb{F})$$

where $E_{u,v}(\mathbb{F}) = E_{u,v} \cup \{\mathcal{O}\}$, as follows:
Let $(h,k) \in E_{u,v}$ and $(h^{'},k^{'}) \in E_{u^{'},v^{'}}$, for arbitrary $(u,v),(u^{'},v^{'}) \in \overline{U}\times\overline{V}$. Then define

$$(h,k) \circ_{\mathbb{G}} (h^{'},k^{'}) = \begin{cases} \left\{(h,gk) \bullet_{u,v} (h^{'},g^{'}k^{'}) | g,g^{'} \in \mathcal{G}\right\}, & \text{if } (u,v) = (u^{'},v^{'}) \\ \{E_{u,v} \cup E_{u^{'},v^{'}}\} & \text{if } (u,v) \neq (u^{'},v^{'}) \end{cases} \tag{4.3}$$

Here $\bullet_{u,v}$ is an elliptic curve group operation. Moreover,

$$\mathcal{O} \circ_{\mathbb{G}} (h,k) = (h,k) \circ_{\mathbb{G}} \mathcal{O} = \{(h,gk) | g \in \mathcal{G}\}, \text{ for all } \mathcal{O} \notin \cup_{(u,v)\in\overline{U}\times\overline{V}} E_{u,v} \tag{4.4}$$

and

$$\mathcal{O} \circ_{\mathbb{G}} \mathcal{O} = \mathcal{O} \tag{4.5}$$

Theorem 4.2.
The set $E_{\overline{U},\overline{V}}(\mathbb{F})$ is a regular hypergroup under the hyperoperation $\circ_{\mathbb{G}}$.

Proof.
Let $\{L,M,N\} \subseteq E_{\overline{U},\overline{V}}(\mathbb{F})$ (an elliptic hypercurve). If $L = \mathcal{O}$ or $M = \mathcal{O}$ or $N = \mathcal{O}$, then clearly associativity property is satisfied.
Consider that, $L = (h,k) \in E_{u,v}$, $y = (h^{'},k^{'}) \in E_{u^{'},v^{'}}$ and $Z = (h^{''},k^{''}) \in E_{u^{''},v^{''}}$, where $S = \{(u,v),(u^{'},v^{'}),(u^{''},v^{''})\} \subseteq \overline{U}\times\overline{V}$, then we have the following cases:
Case 1: $|S| = 1$.

This implies that $E_{u,v} = E_{u',v'} = E_{u'',v''}$.
Let $(a,b) \in [(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''})$. Then there exists

$$(h_1,k_1) \in (h,k) \circ_{\mathbb{G}} (h^{'},k^{'})$$

such that,

$$(a,b) = (h_1,k_1) \circ_{\mathbb{G}} (h^{''},(k^{''}).$$

Hence

$$(h_1,k_1) = (h,gk) \bullet_{u,v} (h^{'},g^{'}k^{'}), \text{ for some } g,g^{'} \in \mathcal{G}$$

So

$$(a,b) = (h_1,g_1k_1) \bullet_{u,v} (h^{''},g^{''}k^{''}), \text{ for some } g_1,g^{''} \in \mathcal{G}.$$

Thus,

$$\begin{aligned}(a,b) &= [(h,g_1k_1) \bullet_{uv} (h^{'},g^{'}k^{'})] \bullet_{uv} (h^{''},k^{''}) \\ &= (h,g_1k_1) \bullet_{uv} [(h^{'},g^{'}k^{'}) \bullet_{uv} (h^{''},k^{''})] \\ &= (h,\ell k) \bullet_{uv} [(h^{'},g_1g^{'}k^{'}) \bullet_{uv} (h^{''},g_1g^{'''}k^{''})] \\ &= (h,\ell k) \bullet_{uv} (h^{'''},g_1k^{'''}),\end{aligned}$$

where $g^{''} = g_1g^{'''}$, for some $g^{'''} \in \mathcal{G}$, $l = g_1g$, $(h^{'''},k^{'''}) = (h^{'},g^{'}k^{'}) \bullet_{uv} (h^{''},g^{'''}k^{''})$.
So,

$$(h^{'''},k^{'''}) \in (h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})$$

and

$$(a,b) = (h,lk) \bullet_{uv} (h^{'''},g_1k^{'''}) \in (h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})].$$

It follows that,

$$[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) \subseteq (h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})]. \tag{4.6}$$

similarly, let $(a,b) \in (h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})]$, then there exists $(h_2,k_2) \in (h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})$, such that

$$(a,b) = (h,k) \circ_{\mathbb{G}} (h_2,k_2).$$

Hence

$$(h_2,k_2) = (h^{'},k^{'}) \bullet_{uv} (h^{''},g^{''}k^{''}), \text{ for some } g^{'},g^{''} \in \mathcal{G}.$$

So

$$(a,b) = (h,gk) \bullet_{uv} (h_2,k_2), \text{ for some } g_1,g^{''} \in \mathcal{G}.$$

Thus,

$$\begin{aligned}(a,b) &= (h,gk) \bullet_{uv} [(h^{'},g_2g^{'}k^{'} \bullet_{uv} (h^{''},g_2g^{''}k^{''})] \\ &= [(h,gk) \bullet_{uv} (h^{'},g_2g^{'}k^{'})] \bullet_{uv} (h^{''},g_2g^{''}k^{''}) \\ &= [(h,g_2g^{'''}k) \bullet_{uv} (h^{'},g_2g^{'}k^{'})] \bullet_{uv} (x^{''},\ell^{'}k^{''}) \\ &= (h^{'''},g_2k^{'''}) \bullet_{uv} (h^{''},\ell^{'}k^{''}),\end{aligned}$$

where $g_2g^{'''} = g$, for some $g^{'''} \in \mathcal{G}$, $g_2g^{''} = \ell^{'}$, $(h^{'''},k^{'''}) = (h,g^{'''}) \bullet_{uv} (h^{'},g^{'}k^{'})$.
So

$$(h^{'''},k^{'''}) \in (h,k) \circ_{\mathbb{G}} (h^{'},k^{'})$$

and

$$(a,b) = (h^{'''},g_2k^{'''}) \bullet_{uv} (h^{'''},\ell^{'}k^{''}) \in [(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}).$$

It follows that

$$(h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] \subseteq [(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}). \tag{4.7}$$

From Equation (4.6) and (4.7),

$$[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) = (h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] \tag{4.8}$$

Case 2: $|S| = 2$, there exists three possibilities.

Let $E_{u,v} = E_{u^{'},v^{'}} \neq E_{u^{''},v^{''}}$, then from Equation 4.3, we have

$$\begin{aligned}[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) &= [(h,gk) \bullet_{uv} (h^{'},g^{'}k^{'}) | g,g^{'} \in \mathcal{G}] \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= \cup_{(s,t)\in(h,k)\circ_{\mathbb{G}}(h^{'},k^{'})}(s,t) \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= E_{u,v} \cup E_{u^{''},v^{''}}.\end{aligned}$$

On the other hand

$$\begin{aligned}(h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] &= (h,k) \circ_{\mathbb{G}} [E_{u^{'},v^{'}} \cup E_{u^{''},v^{''}}] \\ &= (h,k) \circ_{\mathbb{G}} E_{u,v} \cup (h,k) \circ_{\mathbb{G}} E_{u^{''},v^{''}} \\ &= E_{u,v} \cup E_{u^{''},v^{''}}.\end{aligned}$$

If $E_{u,v} \neq E_{u^{'},v^{'}} = E_{u^{''},v^{''}}$.

$$\begin{aligned}[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) &= (E_{u,v} \cup E_{u^{'},v^{'}}) \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= E_{u,v} \circ_{\mathbb{G}} (h^{''},k^{''}) \cup E_{u^{'},v^{'}} \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= E_{u,v} \cup E_{u^{'},v^{'}}.\end{aligned}$$

On the other hand

$$\begin{aligned}(h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] &= (h,k) \circ_{\mathbb{G}} [\{(h^{'},g^{'}k^{'}) \bullet_{uv} (h^{''},g^{''}k^{''})\}] \\ &= \cup_{(s,t)\in(h^{'},k^{'})\circ_{\mathbb{G}}(h^{''},k^{''})}(h,k) \circ_{\mathbb{G}} (s,t) \\ &= E_{u^{'},v^{'}} \cup E_{u,v}.\end{aligned}$$

If $E_{u,v} = E_{u^{''},v^{''}} \neq E_{u^{'},v^{'}}$, then

$$\begin{aligned}[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) &= [E_{u,v} \cup E_{u^{'},v^{'}}] \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= E_{u,v} \cup E_{u^{'},v^{'}}.\end{aligned}$$

As,
$$\begin{aligned}(h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] &= (h,k) \circ_{\mathbb{G}} [E_{u^{'},v^{'}} \cup E_{u,v}] \\ &= E_{u,v} \cup E_{u^{'},v^{'}}.\end{aligned}$$

Case 3: $|S| = 3$, then $E_{u,v} \neq E_{u',v'} \neq E_{u'',v''} \neq E_{u,v}$

$$\begin{aligned}[(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})] \circ_{\mathbb{G}} (h^{''},k^{''}) &= [E_{u,v} \cup E_{u',v'}] \circ_{\mathbb{G}} (h^{''},k^{''}) \\ &= E_{u,v} \cup E_{u',v'} \cup E_{u'',v''}.\end{aligned}$$

Also,

$$\begin{aligned}(h,k) \circ_{\mathbb{G}} [(h^{'},k^{'}) \circ_{\mathbb{G}} (h^{''},k^{''})] &= (h,k) \circ_{\mathbb{G}} [E_{u',v'} \cup E_{u'',v''}] \\ &= E_{u,v} \cup E_{u',v'} \cup E_{u'',v''}.\end{aligned}$$

This shows that, the hyperoperation $\circ_{\mathbb{G}}$ holds the associativity.

The reproduction axiom on $E_{\overline{U},\overline{V}}(\mathbb{F})$ is also satisfied. To prove this axiom, consider the following two cases:

Case 1: If $|\overline{U} \times \overline{V}| = 1$,

then $\overline{\mathbb{F}} = \mathbb{F}$ and $E_{\overline{U},\overline{V}}(\mathbb{F}) = E_{u,v}(F)$, where $u \in \overline{U}$, $v \in \overline{V}$.

This means that $(E_{\overline{U},\overline{V}}(\mathbb{F}), \circ_{\mathbb{G}})$ is an elliptic curve group and the reproduction axiom is clearly satisfied for $\circ_{\mathbb{G}}$.

Case 2: If $|\overline{U} \times \overline{V}| > 1$, consider an arbitary element $(h,k) \in E_{u,v}(\mathbb{F}) \subseteq E_{\overline{U},\overline{V}}(\mathbb{F})$, then

$$\begin{aligned}(h,k) \circ_{\mathbb{G}} E_{\overline{U},\overline{V}}(\mathbb{F}) &= \Big((h,k) \circ_{\mathbb{G}} \bigcup_{u \neq r \in \overline{U}, v \neq s \in \overline{V}} E_{r,s}(\mathbb{F})\Big) \cup E_{u,v}(\mathbb{F}) \\ &= \bigcup_{r \in \overline{U}, s \in \overline{V}} \Big(E_{r,s}(\mathbb{F}) \cup E_{u,v}(\mathbb{F})\Big) \\ &= \Big(\bigcup_{u \neq r \in \overline{U}, v \neq s \in \overline{V}} \circ_{\mathbb{G}} E_{r,s}(\mathbb{F})\Big) \cup E_{u,v}(\mathbb{F}) \\ &= E_{\overline{U},\overline{V}}(\mathbb{F}).\end{aligned}$$

So reproduction axiom is satisfied. It is also a regular hypergroup with $\mathcal{O}$ as an identity element. □

Remarks 4.2.1.

"If $\mathbb{G} = \{1\}$, *i.e.*, trivial group of $\mathbb{F}^*$ then $\overline{\mathbb{F}} = \mathbb{F}$ and thus an elliptic hypercurve on

$\overline{\mathbb{F}}$ is practically an elliptic curve on F. The associated hypergroup $(E_{\overline{U},\overline{V}}(\mathbb{F}), \circ_{\mathbb{G}})$ is called the elliptic curve group on $(E_{u,v}(\mathbb{F}), \bullet_{u,v})$" [61].

Example 4.2.2.

Continue with Example 4.1.3, where $\mathbb{F} = \mathbb{Z}_7$, $\mathbb{F}^* = \{\mathbb{Z}_7 \setminus 0\} = \{1,2,3,4,5,6\}$, $\overline{\mathbb{F}} = \{\overline{0}, \overline{1}, \overline{3}\}$ and $G = \{1,2,4\} \neq \{1\}$ and by using Equation (4.2), the subgroup $\mathcal{G}$ of $\mathbb{F}^*$ is given by:

$$\mathcal{G} = \{h \in \mathbb{Z}_7 | h^2 = 1\} = \{1,6\}$$

also,

$$E_{\overline{0},\overline{1}} = \{(\overline{0},\overline{1}), (\overline{1},\overline{1}), (\overline{3},\overline{1}), (\overline{0},\overline{3}), (\overline{1},\overline{3}), (\overline{3},\overline{3}), (\overline{3},\overline{0})\}$$

and, from Example 4.1.3, we have

$$E_{0,1} = \{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),(4,3),(4,4),(5,0),(6,0),(3,0)\}$$
$$E_{0,2} = \{(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\}$$
$$E_{0,4} = \{(0,2),(0,5)\}.$$

Therefore,

$$E_{\overline{0},\overline{1}} = E_{0,1} \cup E_{0,2} \cup E_{0,4}$$

and

$$\begin{aligned} E_{\overline{0},\overline{1}}(\mathbb{F}) &= \{\mathcal{O}\} \cup E_{\overline{0},\overline{1}} \\ &= \{\mathcal{O}\} \cup E_{0,1} \cup E_{0,2} \cup E_{0,4}. \end{aligned}$$

as computed in Example 4.1.3.

Consider two subsets I and J of $E_{\overline{0},\overline{1}}(\mathbb{F})$ from Example 4.1.3,

$$I = E_{0,4}(\mathbb{F}) = \{\mathcal{O},(0,2),(0,5)\}.$$
$$J = E_{0,2}(\mathbb{F}) = \{\mathcal{O},(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\},$$

which are reversible subhypergroups of $E_{\overline{0},\overline{1}}(\mathbb{F})$ by using Definition 2.2.23.

The values of $E_{0,2} \circ_{\mathbb{G}} E'_{0',2'}$ can be computed by using Equation (4.3).
By using Equation (4.5), it is obvious that

$$\mathcal{O} \circ_{\mathbb{G}} \mathcal{O} = \mathcal{O}.$$

Now computing, $\mathcal{O} \circ_{\mathbb{G}} (0,3)$ by using Equation (4.4)
Taking $g = 1$, then

$$\begin{aligned} \mathcal{O} \circ_{\mathbb{G}} (0,3) &= \mathcal{O} \bullet_{02} (0,(1)(3)) \bmod 7 \\ &= (0,3), \end{aligned}$$

and taking $g = 6$, we have

$$\begin{aligned} \mathcal{O} \circ_{\mathbb{G}} (0,3) &= \mathcal{O} \bullet_{02} (0,(6)(3)) \bmod 7 \\ &= (0,18) \bmod 7 \\ &= (0,4). \end{aligned}$$

Then,

$$\mathcal{O} \circ_{\mathbb{G}} (0,3) = \{(0,3),(0,4)\}.$$

Similarly Equation (4.4) can be used for computing other values of (h,k) of $E_{0,2}$ with $\mathcal{O}$.
The value of $(3,1) \circ_{\mathbb{G}} (3,1)$ can be computed by using Equation (4.3) where $(u,v) = (u',v')$. Taking $u = u' = 0$ and $v = v' = 2$.
Here in Equation (4.3), $\bullet_{uv}$ is elliptic curve group so all points will be computed by using point addition 1 and point doubling 2 formulae of elliptic curve over finite field.
Here $(h,k) = (3,1)$ and $(h',k') = (3,1)$.
By using Equation (4.3) and taking $g = 1 = g'$

$$\begin{aligned} (3,1) \circ_{\mathbb{G}} (3,1) &= (3,(1)(1)) \bullet_{02} (3,(1)(1)) \bmod 7 \\ &= (3,1) \bullet_{02} (3,1) \bmod 7 \\ &= (3,6), \end{aligned}$$

here $(3,1) = (3,1)$. Then this point is computed by using elliptic curve point doubling 2 as solved in Example 3.2.2.
Now for $g = 1$ and $g^{'} = 6$, we get

$$\begin{aligned}(3,1) \circ_{\mathbb{G}} (3,1) &= (3,(1)(1)) \bullet_{02} (3,(6)(1)) \mod 7 \\ &= (3,1) \bullet_{02} (3,6) \mod 7 \\ &= (3,1) \bullet_{02} (3,6) \\ &= \mathcal{O},\end{aligned}$$

here $(3,1) \neq (3,6)$. Then this point is computed by using elliptic curve point addition 1 as solved in Example 3.2.2.
For $g = 6$ and $g^{'} = 1$, we get

$$\begin{aligned}(3,1) \circ_{\mathbb{G}} (3,1) &= (3,(6)(1)) \bullet_{02} (3,(1)(1)) \mod 7 \\ &= (3,6) \bullet_{02} (3,1) \mod 7 \\ &= \mathcal{O},\end{aligned}$$

here $(3,1) \neq (3,6)$, so again elliptic curve point addition is used for computing this point.
Finally, for $g = 6 = g^{'}$, we get

$$\begin{aligned}(3,1) \circ_{\mathbb{G}} (3,1) &= (3,(6)(1)) \bullet_{02} (3,(6)(1)) \mod 7 \\ &= (3,6) \bullet_{02} (3,6) \mod 7 \\ &= (3,1),\end{aligned}$$

here $(3,6) = (3,6)$, so elliptic curve point doubling is used for computing this point.

Hence,

$$(3,1) \circ_{\mathbb{G}} (3,1) = \{\mathcal{O}, (3,1), (3,6)\}.$$

Similarly, the other values of $(h,k) \circ_{\mathbb{G}} (h^{'},k^{'})$ can be computed by using Equation (4.3). After computation of all values the Cayley table of $E_{0,2}$ is given as follows:

TABLE 4.3: Cayley Table of $E_{0,2}$

$(J, \circ_{\mathbb{G}})$	$\mathcal{O}$	$(0,3),(0,4)$	$(3,1),(3,6)$	$(5,1),(5,6)$	$(6,1),(6,6)$
$\mathcal{O}$	$\mathcal{O}$	$(0,3),(0,4)$	$(3,1),(3,6)$	$(5,1),(5,6)$	$(6,1),(6,6)$
$(0,3),(0,4)$	$(0,3),(0,4)$	$\mathcal{O},(0,3),(0,4)$	$(6,1),(6,6),(5,1),(5,6)$	$(3,1),(3,6),(6,1),(6,6)$	$(5,6),(5,1),(3,1),(3,6)$
$(3,1),(3,6)$	$(3,1),(3,6)$	$(5,6),(5,1),(6,1),(6,6)$	$\mathcal{O},(3,1),(3,6)$	$(0,3),(0,4),(6,1),(6,6)$	$(0,3),(0,4),(5,1),(5,6)$
$(5,1),(5,6)$	$(5,1),(5,6)$	$(3,1),(3,6),(6,1),(6,6)$	$(0,3),(0,4),(6,1),(6,6)$	$\mathcal{O},(5,1),(5,6)$	$(0,3),(0,4),(3,1),(3,6)$
$(6,1),(6,6)$	$(6,1),(6,6)$	$(3,1),(3,6),(5,1),(5,6)$	$(0,3),(0,4),(5,1),(5,6)$	$(0,3),(0,4),(3,1),(3,6)$	$\mathcal{O},(6,1),(6,6)$

Here the first column of Cayley table is representing all values of $(h,k) \in E_{0,2}$ and first row is representing all values of $(h^{'},k^{'}) \in E^{'}_{0^{'},2^{'}}$.

Similarly, the values of Cayley table of $E_{0,4}$ can be computed and are given as follows:

TABLE 4.4: Cayley Table of $E_{0,4}$

$(I, \circ_{\mathbb{G}})$	$\mathcal{O}$	$(0,2)$	$(0,5)$
$\mathcal{O}$	$\mathcal{O}$	$(0,2),(0,5)$	$(0,2),(0,5)$
$(0,2)$	$(0,2),(0,5)$	$\mathcal{O},(0,2),(0,5)$	$\mathcal{O},(0,2),(0,5)$
$(0,5)$	$(0,2),(0,5)$	$\mathcal{O},(0,2),(0,5)$	$\mathcal{O},(0,2),(0,5)$

Theorem 4.3.

Let a non-empty subset K of the hypergroup $E_{\overline{U},\overline{V}}(\mathbb{F})$. Then K is a subhypergroup of $E_{\overline{U},\overline{V}}(\mathbb{F})$ if and only if there exists a unique couple of indices $(r,s) \in \overline{U} \times \overline{V}$ such that K is a subhypergroup of $E_{r,s}(\mathbb{F})$, or it can be written as $K = \cup_{(r,s)\in J} E_{r,s}(\mathbb{F})$, where $J = \{(u,v) \in \overline{U} \times \overline{V} | K \cap E_{u,v}(\mathbb{F}) \neq \emptyset\}$.

Proof.

Consider a subhypergroup K of $E_{\overline{U},\overline{V}}(\mathbb{F}) = (\cup_{(u,v)\in\overline{U}\times\overline{V}} E_{u,v}) \cup \{\mathcal{O}\}$.

Assume that, $K \nleq E_{r,s}(F)$, for all $(r,s) \in \overline{U} \times \overline{V}$.

It follows that there exists $(r,s) \neq (w,t) \in \overline{U} \times \overline{V}$ such that:

$$K \cap E_{r,s} \neq \emptyset \neq K \cap E_{w,t}.$$

Set $J = \{(r,s) \in \overline{U} \times \overline{V} | K \cap E_{r,s}(\mathbb{F}) \neq \emptyset\}$. Thus,

$$K \subseteq \cup_{(r,s)\in J} E_{r,s}(\mathbb{F}) \subseteq \cup_{(w,t),(r,s)\in J}(E_{r,s} \cap K) \circ (E_{w,t} \cap K) \subseteq K.$$

Hence

$$K = \cup_{(r,s)\in J} E_{r,s}(\mathbb{F}).$$

Conversely,

Suppose that $K \subseteq E_{r,s}(\mathbb{F})$. We have to prove that $K \subseteq E_{\overline{U},\overline{V}}(\mathbb{F})$.

Because

$$K \subseteq E_{r,s}(\mathbb{F})_{(r,s)\in\overline{U}\times\overline{V}} \subseteq E_{\overline{U},\overline{V}}(\mathbb{F}).$$

Hence

$$K \subseteq E_{\overline{U},\overline{V}}(\mathbb{F}).$$

□

Theorem 4.4.

Every $E_{r,s}(\mathbb{F})$ with $(r,s) \in \overline{U}\times\overline{V}$, is a regular reversible subhypergroup of $(E_{\overline{U},\overline{V}}, \circ_{\mathbb{G}})$ for any $(\overline{U},\overline{V}) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$.

Proof.

By using Theorem 4.2 and Equation (4.3), only the reversibility property can be proved because subhypergroups of regular hypergroup are reversible. For this purpose consider, (h,k), $(h',k') \in E_{r,s}(\mathbb{F})$. Here there are three possibilities.

Case 1: If $(h',k') \neq (h,gk)$, for each $g \in \mathcal{G}$, then from $(h'',k'') \in (h,k) \circ_{\mathbb{G}} (h',k')$. As a result there exists $g, g' \in \mathcal{G}$ such that

$$(h'',k'') = (h,gk) \bullet_{rs} (h', g'k').$$

Then

$$(h'',gk'') = (h,k) \bullet_{rs} (h', gg'k').$$

It follows that:

$$(h,k) = (h^{''}, gk^{''}) \bullet_{rs} (h^{'}, gg^{'}k^{'})^{-1} = (h^{''}, gk^{''}) \bullet_{rs} (h^{'}, -gg^{'}k^{'}).$$

Therefore,

$$(h,k) \in (h^{''}, k^{''}) \ \circ_{\mathbb{G}} \ (h^{'}, -k^{'}).$$

Case 2: If $(h^{'}, k^{'}) = (h, gk)$, for some $g \in \mathcal{G}$, then
$(h,k) \circ_{\mathbb{G}} (h^{'}, k^{'}) = (h,k) \circ_{\mathbb{G}} (h, gk) \subseteq \{(h,k) \bullet_{rs} (h,k), (h,k) \bullet_{rs} (h,-k) = \mathcal{O}, (h,-k) \bullet_{rs}$
$(h,-k), (h,-k) \bullet_{rs} (h,k) = \mathcal{O}\}$, for some $g \in \mathcal{G}$.
So, if we represent $A = (h,k)$ and $B = (h, gk)$, for some $g \in \mathcal{G}$, then

$$A \circ_{\mathbb{G}} B = \{A \bullet_{rs} A, R \bullet_{rs} R, \mathcal{O}\},$$

where $R \bullet_{rs} A = \mathcal{O}$ as shown in Figure 4.2.

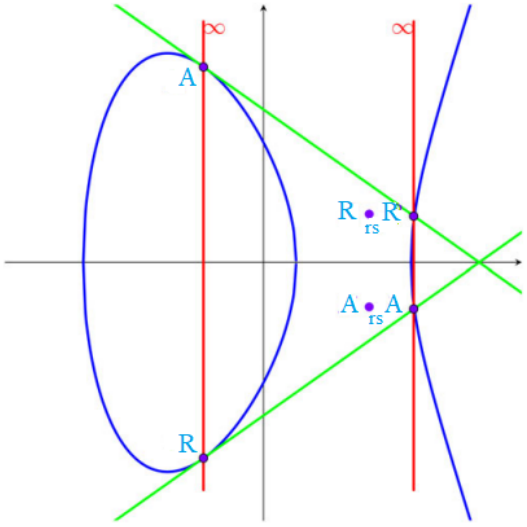

FIGURE 4.2: Composition on an elliptic curve

Now Consider $(h^{''}, k^{''}) \in (h,k) \ \circ_{\mathbb{G}} \ (h^{'}, k^{'})$.
If,

$$(h^{''}, k^{''}) = (h,k) \bullet_{rs} (h,k)$$

then,

$$(h,k) = (h,k)^{-1} \bullet_{rs} (h^{''},k^{''}) = (h,-k) \bullet_{rs} (h^{''},k^{''}).$$

So,

$$(h,k) \in (h,k) \circ_{\mathbb{G}} (h^{''},k^{''}).$$

Similarly,

$$(h,k) \in (h^{''},k^{''}) \circ_{\mathbb{G}} (h,k),$$

here (h,k) is an inverse of (h,k) with respect to $\circ_{\mathbb{G}}$. Similarly we can prove all other subcases.

Case 3: If $(h,k) = \mathcal{O}$ or $(h^{'},k^{'}) = \mathcal{O}$, then from

$$(h^{''},k^{''}) \in \mathcal{O} \circ_{\mathbb{G}} (h^{'},k^{'}) = \{(h^{'},gk^{'}) | g^{'} \in \mathcal{G}\}$$

as a result,

$$\mathcal{O} \in (h^{'},gk^{'}) \ \circ_{\mathbb{G}} \ (h^{'},k^{'}) = \{(h^{'},g^{'}gk^{'} \bullet_{rs} (h^{'},g^{''}k^{'}) | g,g^{'},g^{''} \in \mathcal{G}\}$$

and

$$(h^{'},k^{'}) \in \mathcal{O} \ \circ_{\mathbb{G}} \ (h^{'},gk^{'}).$$

Now it is concluded that $E_{r,s}(\mathbb{F})$ is a reversible subhypergroup of $(E_{\overline{U},\overline{V}}, \circ_{\mathbb{G}})$, for $(r,s) \in \overline{U} \times \overline{V}$. □

Theorem 4.5.

Let H be a subhypergroup of $(E_{\overline{U},\overline{V}}(\mathbb{F}))$. Then H is reversible if and only if H is a subhypergroup of $E_{r,s}(\mathbb{F})$, for some $(r,s) \in \overline{U} \times \overline{V}$.

Proof.

Consider H be a reversible subhypergroup. Suppose that H is not a subhypergroup of $E_{r,s}(\mathbb{F})$, $(r,s) \notin \overline{U} \times \overline{V}$. Then from Theorem 4.3

$$H = \bigcup_{(r,s)\in j} E_{r,s}(\mathbb{F})$$

so there exist $(r,s) \neq (w,t) \in J$. Such that

$$H \cap E_{r,s}(\mathbb{F}) \neq \phi \neq H \cap E_{w,t}(\mathbb{F}).$$

Take an arbitrary $(h,k) \in H \cap E_{r,s}(\mathbb{F})$ and $(h^{'},k^{'}) \in H \cap E_{w,t}(\mathbb{F})$.
Consider,

$$(h^{''},k^{''}) \in (h,k) \circ_{\mathbb{G}} (h^{'},k^{'}) \cap E_{r,s}(\mathbb{F}).$$

Since H is reversible, it follows that:

$$(h^{'},k^{'}) \in (h,gk) \circ_{\mathbb{G}} (h^{''},k^{''}) \subseteq E_{r,s}(\mathbb{F})$$

for some, $g \in \mathcal{G}$. So that

$$(h^{'},k^{'}) \in E_{w,t}(\mathbb{F}) \cap E_{r,s}(\mathbb{F})$$

which is a contradiction because $E_{\overline{U},\overline{V}}$ is an elliptic hypercurve.
Conversely, by Theorem 4.4, H is subhypergroup of $E_{r,s}(\mathbb{F})$. Each $E_{r,s}(\mathbb{F})$ is a regular reversible subhypergroup of $E_{\overline{U},\overline{V}}$. This implies that H is a regular reversible subhypergroup of $E_{\overline{U},\overline{V}}$.
i.e., $H = \cup_{(r,s)} E_{r,s}(\mathbb{F})$. (Here each $E_{r,s}(\mathbb{F})$ is a regular reversible subhypergroup so $H = \cup_{(r,s)} E_{r,s}(\mathbb{F})$ is a regular reversible subhypergroup). □

We'll look at some of the criteria under which two elliptic curves are isomorphic hypergroups in the next section. First, we introduce some notations. For some point $(h,k) \in E_{u,v}$, is defined $\widehat{(h,k)} = \{(h,k),(h,-k)\}$ and $\widehat{E_{u,v}} = \{\widehat{(h,k)} | (h,k) \in E_{u,v}\}$.

Proposition 4.2.3.
If $|\widehat{E_{u_1,v_1}} \cap \widehat{E_{u_2,v_2}}| \geq 2$, then $E_{u_1,v_1} = E_{u_2,v_2}$.

Proof.

Consider $\{(h_1, k_1), (h_2, k_2)\} \subseteq \widehat{E_{u_1,v_1}} \cap \widehat{E_{u_2,v_2}}$, with $h_1 \neq h_2$. So,

$$k_i^2 = h_i^3 + u_j h_j + v_j, \text{ for } i, j = 1, 2$$
$$k_i^2 - h_i^3 = u_j h_j + v_j \qquad (a)$$

putting $i = 1 = j$ in Equation (a),

$$k_1^2 - h_1^3 = u_1 h_1 + v_1 \qquad (I)$$

putting $i = 2 = j$ in Equation (a),

$$k_2^2 - h_2^3 = u_2 h_2 + v_2 \qquad (II)$$

If $u_1 = u_2$ and $v_1 = v_2$, then subtracting Equation (II) from Equation (I)

$$k_1^2 - h_1^3 - (k_2^2 - h_2^3) = u_1 h_1 + v_1 - (u_1 h_2 + v_1)$$
$$k_1^2 - k_2^2 - h_1^3 + h_2^3 = u_1(h_1 - h_2)$$
$$u_1 = u_2 = \frac{y_1^2 - k_2^2 - h_1^3 + h_2^3}{h_1 - h_2} \qquad (III)$$

putting the value of u_1 in Equation (I)

$$k_1^2 - h_1^3 = (\frac{k_1^2 - k_2^2 - h_1^3 + h_2^3}{h_1 - h_2})h_1 + v_1$$
$$k_1^2 - h_1^3 = \frac{(k_1^2 - k_2^2 - h_1^3 + h_2^3) + v_1(h_1 - h_2)}{h_1 - h_2}$$
$$(h_1 - h_2)(k_1^2 - k_2^2) = (k_1^2 - k_2^2 - h_1^3 + h_2^3) + v_1(h_1 - h_2)$$
$$h_1 k_1^2 - h_1 h_1^3 - h_2 k_1^2 + h_2 h_1^3 = h_1 k_1^2 - h_1 k_2^2 - h_1 h_1^3 + h_1 h_2^3 + v_1(h_1 - h_2)$$
$$-h_2 k_1^2 + h_2 h_1^3 - h_1 h_2^3 + h_1 k_2^3 = v_1(h_1 - h_2)$$
$$v_1 = v_2 = \frac{h_1(k_2^2 - h_2^3) - k_2(k_1^2 - h_1^3)}{h_1 - h_2}. \qquad (IV)$$

Hence $E_{u_1,v_1} = E_{u_2,v_2}$. □

An equivalence relation $\sim$ on $\mathbb{F}^2$ is defined as follows:

$$(r,s) \sim (w,t) \Longleftrightarrow r = a^4 w, s = a^6 t,$$

for some $a \in \mathbb{F}^*$. If $(r,s) \sim (w,t)$ then (r,s) and (w,t) are uniform.

Proposition 4.2.4.
Let a finite single subgroup of the group $\mathbb{F}^*$ be $\mathbb{G}$ and $\overline{r}, \overline{s} \in \overline{\mathbb{F}} = \dfrac{\mathbb{F}}{\mathbb{G}}$, then the cardinality $m_{r,s}$ on $\overline{r} \times \overline{s}$ of the equivalence class of (r,s) is:

$$m_{r,s} = \begin{cases} \{1, & \text{if } r = 0 = s \\ |\overline{1}|, & \text{if } r \neq 0 \\ |K|, & \text{if } r = 0 \neq s \end{cases} \tag{4.9}$$

where $K = \{g^3 | g \in \overline{1}\}$.

Proof.
First we prove that if there exists $a \in \mathbb{F}^*$ such that $\{a^4, a^6\} \subseteq \overline{1}$, then $a \in \overline{1}$ or $-a \in \overline{1}$. For this, let $a \in F^*, g = a^6 \in \overline{1}$ and $h = a^6 \in \overline{1}$. We get

$$\begin{aligned} hg^{-1} = a^6 a^{-4} = a^2 \in \overline{1} &\Rightarrow \exists p \in \overline{1} : p^2 = a^2 \text{ (because}\mathbb{G}\text{is single)} \\ &\Rightarrow a = p \text{ or } a = -p \\ &\Rightarrow a \in \overline{1} \text{ or } -a \in \overline{1}. \end{aligned}$$

Consequently,

$$\frac{(r,s)}{\sim} \cap \overline{r} \times \overline{s} = \{(ra^4, sa^6) | a \in F^*\} \cap \overline{r} \times \overline{s} = \{(ra^4, sa^6) | a \in \overline{1}\}.$$

Now let $r \neq 0$. Since $\mathbb{G}$ is single, it implies that:

$$m_{r,s} = \left| \frac{(r,s)}{\sim} \cap \overline{r} \times \overline{s} \right| = |\{(ra^4, sa^6) | a \in \overline{1}\}| = |\{ra^4 | a \in \overline{1}\}| = |\overline{1}|.$$

If $r = 0$, we get

$$m_{r,s} = \left| \frac{(r,s)}{\sim} \cap \overline{r} \times \overline{s}| = |\{(0, sa^6) | a \in \overline{1}\} \right| = |\{sa^6 | a \in \overline{1}\}| = |\overline{K}|.$$

□

Remarks 4.2.5.

It is important to note out that here K is a subgroup of $\overline{1} = \mathbb{G}$. Generally, if $\mathbb{G}$ is single and $-1 \notin \mathbb{G} \leq \mathbb{F}^*$, then the above Proposition 4.2.4 is satisfied [61].

Proposition 4.2.6.

Let $(\mathbb{F}, +, \cdot)$ be a field and two subgroups $\mathbb{G}, \mathbb{G}^{'}$ of the group $(\mathbb{F}^*, \cdot)$. The corresponding hypergroups $(E_{r,s}(\mathbb{F}), \circ_{\mathbb{G}})$ and $(E_{w,t}(\mathbb{F}), \circ_{\mathbb{G}'})$ are isomorphic if (r, s) and (w, t) are uniform [61].

Proof.

By Proposition 4.2.3 there exists $a \in \mathbb{F}^*$ such that $r = wa^4$ and $s = ta^6$, if (r, s) and (w, t) are uniform. Define:

$$f : E_{r,s}(\mathbb{F}) \longrightarrow E_{w,st}(\mathbb{F})$$

by $f(\mathcal{O}) = \mathcal{O}$ and $f(x, y) = (a^2x, a^3y)$, for any $(x, y) \in E_{r,s}$.

We get the following equivalences:

$$\begin{aligned}
(h, k) \in E_{r,s}(\mathbb{F}) &\iff k^2 = h^3 + rh + s \\
&\iff a^6k^2 = a^6(h^3 + rh + s) \\
&\iff a^6k^2 = (a^2h)^3 + ra^4(a^2h) + sa^6 \\
&\iff (a^3k)^2 = (a^2h)^3 + w(a^2 + t \\
&\iff (a^2h, a^3k) \in E_{w,t}
\end{aligned}$$

hence f is well-defined map and f is a bijection.

Now it is to prove that f is a homomorphism. Consider $(h, k), (h^{'}, k^{'}) \in E_{r,s}(\mathbb{F})$.

Case 1: If $\mathcal{O} \notin \{(h, k), (h^{'}, k^{'})\}$ and $h \neq h^{'}$ or $h = h^{'}, k = k^{'} \neq 0$, then for all $g, g^{'} \in \mathcal{G}$, take

$$\mu_{g,g'} = \begin{cases} \{(gk - g^{'}k^{'})(h - h^{'})^{-1} & \text{if } h \neq h^{'} \\ (3h^2 + r)(2gk)^{-1}, & \text{if } h = h^{'}, k = k^{'} \neq 0. \end{cases} \tag{4.10}$$

Now recalling analytical formula for elliptic curve point addition. Take

$$(h_1, h_2) = (h, gy)$$

and

$$h_2 = (h^{'}, g^{'}k^{'}).$$

Then

$$(h_3, k_3) = (h_1, k_1) + (h_2, k_2),$$

where

$$h_3 = \mu_{g,g}^2 - (h + h^{'}),$$

and

$$\begin{aligned} k_3 &= -gk + \mu_{g,g'}(h - h_3) \\ &= -gk + \mu_{g,g'}(h - \mu_{g,g'}^2 + h + h^{'}) \\ &= -gk - \mu_{g,g'}^3 + \mu_{g,g'}(2h + h^{'}). \end{aligned}$$

Therefore

$$\begin{aligned} f[(h,k) \circ_{\mathbb{G}} (h^{'}, k^{'})] &= \{f[(h, gk) \bullet_{rs} (h^{'}, g^{'}k^{'}) | g, g^{'} \in \mathcal{G}\} \\ &= \{f(\mu_{g,g'}^2 - (h + h^{'}), -\mu_{g,g'}^3 + (2h + h^{'})\mu_{g,g'} - gk) | g, g^{'} \in \mathcal{G}\} \\ &= \{[(a\mu_{g,g'})^2 - (a^2h + a^2h^{'}), -(a\mu_{g,g'})^3 \\ &+ (2a^2h + a^2h^{'})(a\mu_{g,g'}) - a^3gk] | g, g^{'} \in \mathcal{G}\} \\ &= \{(a^2h, a^3gk) \bullet_{wt} (a^2h^{'}, a^3g^{'}k^{'}) | g, g^{'} \in \mathcal{G}\} \\ &= (a^2h, a^3gk) \circ_{\mathbb{G}'} (a^2h^{'}, a^3k^{'}) \\ &= f(h,k) \circ_{\mathbb{G}'} f(h^{'}, k^{'}). \end{aligned}$$

Case 2: If $\mathcal{O} \notin \{(h,k), (h^{'}, k^{'})\}$ and $h = h^{'}, y \neq y^{'}$, then $0 \neq k = k^{'}$. Then we have

$$f[(h,k), (h^{'}, k^{'}] = \{f(\mathcal{O}), f(\psi^2 - 2h, -\psi^3 + 3h\psi - k), f(\psi^2 - 2h, \psi^3 - 3h\psi + k)\}$$

$$
\begin{aligned}
&= \{\mathcal{O}, (a^2h, a^3k) \bullet_{wt} (a^2h^{'}, a^3k^{'})\} \\
&= (a^2h, a^3k) \circ_{\mathbb{G}'} (a^2h^{'}, a^3k^{'}) \\
&= f(h,k) \circ_{\mathbb{G}'} f(h^{'}, k^{'}),
\end{aligned}
$$

where $\psi = (3h^2 + r)(2k)^{-1}$.

Case 3:

$$
\begin{aligned}
f(\mathcal{O} \circ_{\mathbb{G}} (h,k)) &= f(\{(h, \pm k)\}) \\
&= \{(a^2h, \pm a^3k)\} \\
&= \mathcal{O} \circ_{\mathbb{G}'} (a^2h, a^3k) \\
&= f(\mathcal{O}) \circ_{\mathbb{G}'} f(h,k), \text{ for all } \quad (h,k) \in E_{r,s}(\mathbb{F}).
\end{aligned}
$$

Also, for all $(h,0) \in E_{r,s}(\mathbb{F})$,

$$
f\left((h,0) \circ_{\mathbb{G}} (h,0)\right) = f((h,0)) \circ_{\mathbb{G}'} f\left((h,0)\right),
$$

because

$$
\begin{aligned}
f((h,0) \circ_{\mathbb{G}} (h,0)) &= f(\mathcal{O}) \\
&= \mathcal{O} \\
&= (a^2h, 0) \circ_{\mathbb{G}'} (a^2h, 0) \\
&= f\left((h,0)\right) \circ_{\mathbb{G}'} f((h,0)).
\end{aligned}
$$

□

We have following two corollaries by using Propositions 4.2.4 and 4.2.6.

Corollary 4.2.7.

If $M_{rs} = \{E_{w,t}(\mathbb{F}) \leq E_{\overline{r},\overline{s}}(\mathbb{F}) | E_{w,t}(\mathbb{F}) \cong E_{r,s}(\mathbb{F})\}$, then $|M_{rs}| = m_{rs}$.

Corollary 4.2.8.

If $N_{r,s} = \left\{ \dfrac{(rs)}{\sim} \middle| (r,s) \in \overline{r} \times \overline{s} \right\}$.

$$|N_{r,s}| = \begin{cases} \{|\overline{1}|, & textif\ r \neq 0, j \neq 0. \\ \left|\dfrac{\overline{1}}{K}\right|, & \text{if } r = 0, j \neq 0. \\ 1 \neq, & \text{if } j = 0. \end{cases} \tag{4.11}$$

Remarks 4.2.9.

Consider $u, u^{'} \in \mathbb{F}$ and $u, u^{'} = 0$ or $u, u^{'} \neq 0$, also $v, v^{'} \in \mathbb{F}$ and $v, v^{'} = 0$ or $v, v^{'} \neq 0$. Set

$$L = \begin{cases} u^{'}u^{-1}, & \text{if} \quad u \neq 0. \\ 0, & \text{if} \quad u = 0. \end{cases}$$

and $M = \begin{cases} v^{'}v^{-1}, & \text{if} \quad v \neq 0. \\ 0, & \text{if} \quad v = 0. \end{cases}$

If $L \neq 0 \neq M$ or $L = 0 \neq M$ or $L \neq 0 = M$ and $a \notin \mathbb{F}^*$ such that

$M^2 = a^{12} = L^3$ or $M^2 = a^{12}$ or $L^3 = a^{12}$ respectively.

Then subhypergroups $E_{u,v}(\mathbb{F})$ and $E_{u^{'},v^{'}}(F)$ of $E_{\overline{U},\overline{V}}(\mathbb{F})$ and $E_{\overline{U^{'}},\overline{V^{'}}}(F)$ are not isomorphic, respectively.

There is a field extension κ of $\mathbb{F}, (\mathbb{F} \subseteq \kappa)$ and $a \in \kappa$ such that the above mentioned condition is satisfied.

Consequently, subhypergroups $E_{u,v}(\kappa)$ and $E_{u^{'},v^{'}}(\kappa)$ of $E_{\overline{U},\overline{V}}(\kappa)$ and $E_{\overline{U^{'}},\overline{V^{'}}}(\kappa)$ are isomorphic respectively.

A hyperfield extension $\overline{\kappa}$ of $\overline{\mathbb{F}}$ is induced by every field extension κ of $\mathbb{F}$ such that

$$E_{\overline{U},\overline{V}}(\mathbb{F}) \leq E_{\overline{U},\overline{V}}(\kappa)$$

and

$$E_{\overline{U^{'}},\overline{V^{'}}}(\mathbb{F}) \leq E_{\overline{U^{'}},\overline{V^{'}}}(\kappa).$$

Moreover,

$$\mathbb{F} \subseteq \kappa \Rightarrow \overline{\mathbb{F}} \subseteq \overline{\kappa}$$

$$\Rightarrow E_{u,v}(\mathbb{F}) \leq E_{u,v}(\kappa)$$

$$\Rightarrow E_{\overline{U},\overline{V}}(\mathbb{F}) \leq E_{\overline{U},\overline{V}}(\kappa).$$

4.2.2 Hyperoperation $\overline{\circ}_{\mathbb{G}}$

In [64], Vougiouuklis proposed the idea of H_v-groups as an extension of the idea of hypergroups, using weak associativity property instead of the associativity property:

$$u \circ (v \circ w) \cap (u \circ v) \circ w \neq \phi, \text{for all } u, v, w \in H$$

while keeping reproducibility property same. The following is the reason for introducing H_v-groups. We know that quotient of a group with respect to a normal subgroup is a group but with respect to any subgroup, it is a hypergroup. and in [64] it is stated that a group with respect to any partition is an H_v-group.
Now a new hyperoperation on an elliptic hypercurves is introduced, extended by a point at infity and provide it with a structure of H_v group. A hyperoperation is denoted by $\overline{\circ}_{\mathbb{G}}$. Suppose that

$$E_{\overline{U},\overline{V}}(\overline{\mathbb{F}}) = \bigcup_{(u,v)\in\overline{U},\overline{V}} E_{u,v} \cup \{\mathcal{O}\} \subseteq \overline{\mathbb{F}}^2 \cup \{\mathcal{O}\}.$$

Consider the following hyperoperation on it:

$$(\overline{h},\overline{k})\overline{\circ}_{\mathbb{G}}(\overline{h'},\overline{k'}) = \Big\{(\overline{p},\overline{q})|(p,q) \in (\overline{h}\times\overline{k}) \circ_{\mathbb{G}} (\overline{h'}\times\overline{k'})\Big\}. \tag{4.12}$$

Observe that

$$\mathcal{O} \notin \cup_{(u,v)\in\overline{U}\times\overline{V}}\overline{E}_{u,v}$$

and

$$(h,k) = \mathcal{O} \Longleftrightarrow (\overline{h},\overline{k}) = \mathcal{O} \Longleftrightarrow \overline{h}\times\overline{k} = \mathcal{O}.$$

In addition,

$$(u,v) \notin \overline{h}\times\overline{k} \text{ or } (u',v') \notin \overline{h'}\times\overline{k'} \Rightarrow (u,v) \circ_{\mathbb{G}} (u',v') = \emptyset.$$

Furthermore, in accordance with Theorem 4.1, the hyperoperation $\overline{\circ}$ is completely defined on $E_{\overline{U},\overline{V}}(\overline{F})$, and moreover we have

$$\overline{(h,k) \circ_{\mathbb{G}} (h',k')} \subseteq (\overline{h},\overline{k}) \,\overline{\circ}_{\mathbb{G}}\, (\overline{h'},\overline{k'}). \tag{4.13}$$

Proposition 4.2.10.

The elliptic hypercurve $E_{\overline{U},\overline{V}}(\overline{\mathbb{F}})$ under hyperoperation $\overline{\circ}_{\mathbb{G}}$ is an H_v-group.

Proof.

Let $(h,k),(h^{'},k^{'})$ and $(h^{''},k^{''})$ be an arbitrary elements in $E_{\overline{U},\overline{V}}(\overline{\mathbb{F}})$. Then by using Equation (4.13) we have,

$$\overline{(h,k)\circ_{\mathbb{G}}(h^{'},k^{'})\circ_{\mathbb{G}}(h^{''},k^{''})}\subseteq\Big[(\overline{h},\overline{k})\overline{\circ}_{\mathbb{G}}(\overline{h^{'}},\overline{k^{'}})\Big]\overline{\circ}_{\mathbb{G}}(\overline{h^{''}},\overline{k^{''}})$$
$$\cap\,(\overline{h},\overline{k})\overline{\circ}_{\mathbb{G}}\Big[(\overline{h^{'}},\overline{k^{'}})\overline{\circ}_{\mathbb{G}}(\overline{h^{''}},\overline{k^{''}})\Big].$$

□

Proposition 4.2.11.

The mapping

$$\varphi_{\overline{U},\overline{V}}:E_{\overline{U},\overline{V}}(\mathbb{F})\to E_{\overline{U},\overline{V}}(\overline{\mathbb{F}})$$

defined by $\varphi_{\overline{U},\overline{V}}(h,k)=\overline{(h,k)}$ is an H_v-groups epimorphism.

Proof.

Let (h,k) and $(h^{'},k^{'})$ belong to $E_{\overline{U},\overline{V}}(\mathbb{F})$. Then

$$\begin{aligned}\varphi_{\overline{U},\overline{V}}((h,k)\circ_{\mathbb{G}}(h^{'},k^{'}))&=\{\overline{(p,q)}|(p,q)\in(h,k)\circ_{\mathbb{G}}(h^{'},k^{'})\}\\&=\{(\overline{p},\overline{q})|(p,q)\in(h,k)\circ_{\mathbb{G}}(h^{'},k^{'})\}\\&\subseteq(\overline{h},\overline{k})\overline{\circ}_{\mathbb{G}}(\overline{h^{'}},\overline{k^{'}})\\&=\varphi_{\overline{U},\overline{V}}(h,k)\overline{\circ}_{\mathbb{G}}\varphi_{\overline{U},\overline{V}}(h^{'},k^{'}).\end{aligned}$$

□

Corollary 4.2.12.

If a map

$$\omega:(E_{\overline{U_1},\overline{V_1}}(\mathbb{F}),\circ_{\mathbb{G}_{\not\#}})\to(E_{\overline{U_2},\overline{V_2}}(\mathbb{F}),\circ_{\mathbb{G}_{\not\#}})$$

is an isomorphism, then there exists a homomorphism

$$\overline{\omega}:(E_{\overline{U_1},\overline{V_1}}(\mathbb{F}),\overline{\circ}_{\mathbb{G}_1})\to(E_{\overline{U_2},\overline{V_2}}(\mathbb{F}),\overline{\circ}_{\mathbb{G}_2})$$

such that

$$\overline{\omega} = \varphi_{\overline{U_1},\overline{V_1}} \circ \omega.$$

Proof.

It needs to be noted that $\overline{\omega}$ is a homomorphism. Further, by Theorem 4.1, as a result, for all $(h,k) \in E_{\overline{U_1},\overline{V_1}}(F)$,

$$\overline{\omega}(h,k) = \varphi_{\overline{U},\overline{V}} \circ \omega(h,k) = \overline{\omega(h,k)} \in E_{\overline{U_2},\overline{V_2}}(\overline{\mathbb{F}}).$$

□

Example 4.2.13.

Let's proceed with the elliptic hypercurve $E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})$ in Example 4.1.3. Where $E_{\overline{0},\overline{1}}(\mathbb{F}) = \{\mathcal{O}, (\overline{0},\overline{1}), (\overline{0},\overline{3}), (\overline{3},\overline{0}), (\overline{1},\overline{3}), (\overline{1},\overline{1}), (\overline{3},\overline{1}), (\overline{3},\overline{3})\}$.

The values of $E_{\overline{0},\overline{1}}(\overline{F}) \overline{\circ}_{\mathbb{G}} E_{\overline{0},\overline{1}}(\overline{F})$ can be computed by using Equation (4.12). According to this equation only those point on the elliptic curve will be considered which belong to

$$(\overline{h} \times \overline{k}) \circ_{\mathbb{G}} (\overline{h'} \times \overline{k'})$$

Except

$$\mathcal{O} \circ_{\mathbb{G}} (h,k).$$

Here $(u,v) \in \overline{U} \times \overline{V}$, where $\overline{U} = \overline{0}$ and $\overline{V} = \overline{1}$.

Hence, $(u,v) \in \overline{0} \times \overline{1}$.

By using Example 4.1.3,

$$\overline{0} = 0\mathbb{G} = \{0\}$$

and

$$\overline{1} = 1\mathbb{G} = \{1,2,4\}.$$

Hence,

$$\overline{0} \times \overline{1} = 0 \times 1\{1,2,4\}$$

$$= 0 \times \{1,2,4\}.$$

Then we have following possible values of (u, v)

$$\Big\{(0,1),(0,2),(0,4)\Big\}.$$

$$E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})\overline{\circ}_{\mathbb{G}}E_{\overline{0},\overline{1}}(\overline{\mathbb{F}}) = \Big\{\mathcal{O},(\overline{0},\overline{1}),(\overline{0},\overline{3}),(\overline{3},\overline{0}),(\overline{1},\overline{3}),(\overline{1},\overline{1}),(\overline{3},\overline{1}),(\overline{3},\overline{3})\Big\}$$
$$\overline{\circ}_{\mathbb{G}}\Big\{\mathcal{O},(\overline{0},\overline{1}),(\overline{0},\overline{3}),(\overline{3},\overline{0}),(\overline{1},\overline{3}),(\overline{1},\overline{1}),(\overline{3},\overline{1}),(\overline{3},\overline{3})\Big\}.$$

$$\mathcal{O}\overline{\circ}_{\mathbb{G}}\mathcal{O} = \mathcal{O}$$

The values of $\mathcal{O}\overline{\circ}_{\mathbb{G}}(\overline{0},\overline{1})$ are computed by using

$$\mathcal{O}\overline{\circ}_{\mathbb{G}}(h,k) = (h, gk)$$

where $\overline{0} = 0\mathbb{G} = \{0\}$ and $\overline{1} = 1\mathbb{G} = \{1,2,4\}$.
So,

$$\begin{aligned}\overline{0}\times\overline{1} &= 0\times\{1,2,4\}\\ &= \Big\{(0,1),(0,2),(0,4)\Big\}.\end{aligned}$$

So,

$$\mathcal{O}\circ_{\mathbb{G}}\overline{0}\times\overline{1} = \mathcal{O}\circ_{\mathbb{G}}\Big\{(0,1),(0,2),(0,4)\Big\}. \tag{4.14}$$

Selecting only those points from Equation (4.14), which lies on elliptic curves $E_{0,1}(\mathbb{F})$, $E_{0,2}(\mathbb{F})$ or $E_{0,4}(\mathbb{F})$. So from Equation (4.14) only $\mathcal{O}$ and $(0,1)$ lies on curve $E_{0,1}(\mathbb{F})$. Therefore, as in Example (4.2.2) and using Equation (4.4), we compute $\mathcal{O}\circ_{\mathbb{G}}(0,1)$ as follows:

$$\mathcal{O}\circ_{\mathbb{G}}(0,1) = \mathcal{O}\bullet_{01}(0,g(1))$$
$$\mathcal{O}\bullet_{01}(0,1) = (0,1),\ \text{for } g = 1$$
$$\mathcal{O}\bullet_{01}(0,6) = (0,6),\ \text{for } g = 6.$$

Similarly, $\mathcal{O}$ and $(0,2)$ lies on $E_{0,4}(\mathbb{F})$. Then,

$$\begin{aligned}\mathcal{O} \circ_{\mathbb{G}} (0,2) &= \mathcal{O} \bullet_{04} (0, g(2)) \\ \mathcal{O} \bullet_{04} (0,2) &= (0,2), \text{ for } g = 1 \\ \mathcal{O} \bullet_{04} (0,12) \mod 7 &= (0,5), \text{ for } g = 6\end{aligned}$$

and $\mathcal{O}$ and $(0,4)$ lies on $E_{0,2}(\mathbb{F})$. Then,

$$\begin{aligned}\mathcal{O} \circ_{\mathbb{G}} (0,4) &= \mathcal{O} \bullet_{02} (0, g(4)) \\ \mathcal{O} \bullet_{04} (0,4) &= (0,4), \text{ for } g = 1 \\ \mathcal{O} \bullet_{02} (0,24) \mod 7 &= (0,3), \text{ for } g = 6.\end{aligned}$$

Taking union of all these points we have,

$$\{(0,1),(0,6),(0,2),(0,5),(0,3),(0,4)\}.$$

Now applying bar on these values,

$$\Big\{(\overline{0},\overline{1}),(\overline{0},\overline{6}),(\overline{0},\overline{2}),(\overline{0},\overline{5}),(\overline{0},\overline{3}),(\overline{0},\overline{4})\Big\}.$$

Therefore,

$$\mathcal{O}\overline{\circ}_{\mathbb{G}}\overline{0} \times \overline{1} = \{(\overline{0},\overline{1}),(\overline{0},\overline{3})\}.$$

Similarly other values of $\mathcal{O}\overline{\circ}_{\mathbb{G}}(h,k)$ can be computed. The values of $(\overline{0},\overline{1})\overline{\circ}_{\mathbb{G}}(\overline{0},\overline{1})$ are computed by using Equation (4.12) as follows:
we know that:

$$\overline{0} \times \overline{1} = \Big\{(0,1),(0,2),(0,4)\Big\}.$$

Then,

$$\overline{0} \times \overline{1} \circ_{\mathbb{G}} \overline{0} \times \overline{1} = \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}. \tag{4.15}$$

Selecting only those points from (4.15) which are lying on elliptic curves $E_{0,1}(\mathbb{F})$, $E_{0,2}(\mathbb{F})$ and $E_{0,4}(\mathbb{F})$. It can be seen that $(0,1) \in E_{0,1}(\mathbb{F})$, $(0,2) \in E_{0,4}(\mathbb{F})$ and $(0,4) \in$

$E_{0,2}(\mathbb{F})$.

Now, first computing $(0,1) \circ_{\mathbb{G}} (0,1)$, here $(u,v) = (u^{'}, v^{'}) = (0,1)$.

So by using Equation (4.3), for $g = 1 = g^{'}$

$$(0,1) \circ_{\mathbb{G}} (0,1) = \Big(0, g(1)\Big) \bullet_{01} \Big(0, g^{'}(1)\Big) \mod 7$$
$$\Big(0,(1)(1)\Big) \bullet_{01} \Big(0,(1)(1)\Big) \mod 7 = (0,1) \bullet_{01} (0,1)$$
$$(0,1) \circ_{\mathbb{G}} (0,1) = (0,6).$$

This point is computed by using elliptic curve point doubling because,

$(3,1) = (3,1)$.

Now for $g = 1$ and $g^{'} = 6$,

$$(0,1) \circ_{\mathbb{G}} (0,1) = \Big(0, g(1)\Big) \bullet_{01} \Big(0, g^{'}(1)\Big) \mod 7$$
$$\Big(0,(1)(1)\Big) \bullet_{01} \Big(0,(6)(1)\Big) \mod 7 = (0,1) \bullet_{01} (0,6)$$
$$(0,1) \circ_{\mathbb{G}} (0,6) = \mathcal{O}.$$

Here, $(0,1) \neq (0,6)$, so elliptic curve point addition is used for this computation.

Note that:

$$(0,6) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}.$$

Therefore, this point will be neglected by using Equation (4.12). Similarly, for $g = 6$ and $g^{'} = 1$, we get

$$(0,1) \circ_{\mathbb{G}} (0,1) = \Big(0, g(1)\Big) \bullet_{01} \Big(0, g^{'}(1)\Big) \mod 7$$
$$\Big(0,(6)(1)\Big) \bullet_{01} \Big(0,(1)(1)\Big) \mod 7 = (0,6) \bullet_{01} (0,1)$$
$$(0,6) \circ_{\mathbb{G}} (0,1) = \mathcal{O}.$$

This point will also be neglected as because,

$$(0,6) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}.$$

Finally, for $g = 6 = g^{'}$, we get

$$(0,1) \circ_{\mathbb{G}} (0,1) = \Big(0, g(1)\Big) \bullet_{01} \Big(0, g^{'}(1)\Big) \mod 7$$
$$\Big(0,(6)(1)\Big) \bullet_{01} \Big(0,(6)(1)\Big) \mod 7 = (0,6) \bullet_{01} (0,6)$$
$$(0,6) \circ_{\mathbb{G}} (0,6) = (0,1).$$

This point will also be neglected by using (4.12). Thus,

$$(0,1) \circ_{\mathbb{G}} (0,1) = \{\mathcal{O}, (0,1)\}.$$

Now computing $(0,1) \circ_{\mathbb{G}} (0,2)$.
Here $(u,v) \neq (u^{'}, v^{'})$ because both points $(0,1)$ and $(0,2)$ lies on different elliptic curves. Then by using Equation 4.3, taking union of both elliptic curves.

$$E_{0,1} \cup E_{0,4} = \Big\{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),(4,3),(4,4),(6,0),$$
$$(5,0),(3,0)\Big\} \cup \Big\{(0,2),(0,5)\Big\}$$
$$(0,1) \circ_{\mathbb{G}} (0,2) = \Big\{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),(4,3),(4,4),(6,0),$$
$$(5,0),(3,0),(0,2),(0,5)\Big\}.$$

Now computing $(0,2) \circ_{\mathbb{G}} (0,2)$ as follows:
Here $(u,v) = (u^{'}, v^{'}) = (0,4)$ because both points lies on the same elliptic curves. Then by using Equation (4.3), for $g = 1, g^{'} = 1$

$$(0,2) \bullet_{04} (0,2) = (0,5),$$

for $g = 1, g^{'} = 6$

$$(0,2) \bullet_{04} (0,5) = \mathcal{O}.$$

Neglecting this point by using (4.12) because,

$$(0,5) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}.$$

For $g = 6, g^{'} = 1$, we get

$$(0,5) \bullet_{04} (0,5) = (0,2).$$

This point will also be rejected by using Equation (4.12).

Finally for $g = 6 = g^{'}$, we get,

$$(0,5) \bullet_{04} (0,2) = \mathcal{O}.$$

Here also,

$$(0,5) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}$$

Therefore, we have

$$(0,2) \circ_{\mathbb{G}} (0,2) = \Big\{\mathcal{O},(0,5),(0,2)\Big\}.$$

$(0,2) \circ_{\mathbb{G}} (0,4)$, where $(u,v) \neq (u^{'},v^{'})$. Here $(0,2)$ and $(0,4)$ lies on different elliptic curves. Then by using Equation (4.3) it is computed as follows:

$$\begin{aligned} E_{0,2} \cup E_{0,4} &= \Big\{(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\Big\} \\ &\cup \Big\{(0,2),(0,5)\Big\} \\ &= \Big\{(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6),(0,2),(0,5)\Big\}. \end{aligned}$$

Now computing, $(0,4) \circ_{\mathbb{G}} (0,4)$, here $(u,v) = (u^{'},v^{'}) = (0,2)$ because both points lies on same elliptic curves then, we have

for $g = 1, g^{'} = 1$

$$(0,4) \bullet_{02} (0,4) = (0,3),$$

for $g = 1, g^{'} = 6$

$$(0,4) \bullet_{02} (0,3) = \mathcal{O}.$$

Also, for $g = 6, g^{'} = 1$

$$(0,3) \bullet_{02} (0,4) = \mathcal{O}$$

here,

$$(0,3) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\},$$

hence this point will be neglected. Also, for $g = 6, g^{'} = 1$

$$(0,3) \bullet_{02} (0,4) = \mathcal{O}$$

here,

$$(0,3) \notin \Big\{(0,1),(0,2),(0,4)\Big\} \circ_{\mathbb{G}} \Big\{(0,1),(0,2),(0,4)\Big\}$$

hence both these points will be neglected and finally, for $g = 6, g^{'} = 6$

$$(0,3) \bullet_{02} (0,3) = (0,4).$$

Therefore,

$$(0,4) \circ_{\mathbb{G}} (0,4) = \{\mathcal{O},(0,4)\}.$$

After all these computations, we get

$$\Big\{(0,1),(0,6),(1,3),(1,4),(2,3),(2,4),(4,3),(4,4),(6,0),(5,0),(3,0),(0,2),(0,5),$$
$$(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\Big\}.$$

Now taking bar of these values, we have
$\Big\{(\overline{0},\overline{1}),(\overline{0},\overline{6}),(\overline{1},\overline{3}),(\overline{1},\overline{4}),(\overline{2},\overline{3}),(\overline{2},\overline{4}),(\overline{4},\overline{3}),(\overline{4},\overline{4}),(\overline{6},\overline{0}),(\overline{5},\overline{0}),(\overline{3},\overline{0}),(\overline{0},\overline{2}),$
$(\overline{0},\overline{5}),(\overline{0},\overline{3}),(\overline{0},\overline{4}),(\overline{3},\overline{1}),(\overline{3},\overline{6}),(\overline{5},\overline{1}),(\overline{5},\overline{6}),(\overline{6},\overline{1}),(\overline{6},\overline{6})\Big\}$.
Therefore,

$$\begin{aligned}(\overline{0},\overline{1})\overline{\circ}_{\mathbb{G}}(\overline{0},\overline{1}) &= \Big\{(\overline{0},\overline{1}),(\overline{0},\overline{3}),(\overline{1},\overline{3}),(\overline{1},\overline{1}),(\overline{3},\overline{0}),(\overline{3},\overline{1}),(\overline{3},\overline{3})\Big\} \\ &= E_{\overline{0},\overline{1}}.\end{aligned}$$

Similarly, the values of $(\overline{3},\overline{0})\overline{\circ}_{\mathbb{G}}(\overline{3},\overline{1})$ are computed as follows:

$$\overline{3} \times \overline{0} \circ_{\mathbb{G}} \overline{3} \times \overline{1} = \Big\{(3,0),(5,0),(6,0)\Big\} \circ_{\mathbb{G}} \Big\{(3,1),(5,1),(6,1)\Big\}, \tag{4.16}$$

here, $(3,0),(5,0),(6,0) \in E_{0,1}$ and $(3,1),(5,1),(6,1) \in E_{0,2}$, then by using Equation (4.3)

$$(3,0) \circ_{\mathbb{G}} (3,1) = E_{0,1} \cup E_{0,2},$$

here, $(u,v) \neq (u^{'},v^{'})$, because both points lies on different elliptic curves. Similarly,

$$(3,0) \circ_{\mathbb{G}} (5,1) = E_{0,1} \cup E_{0,2}.$$

$$(3,0) \circ_{\mathbb{G}} (6,1) = E_{0,1} \cup E_{0,2}.$$

$$(5,0) \circ_{\mathbb{G}} (3,1) = E_{0,1} \cup E_{0,2}.$$

$$(5,0) \circ_{\mathbb{G}} (5,1) = E_{0,1} \cup E_{0,2}.$$

$$(5,0) \circ_{\mathbb{G}} (6,1) = E_{0,1} \cup E_{0,2}.$$

$$(6,0) \circ_{\mathbb{G}} (3,1) = E_{0,1} \cup E_{0,2}.$$

$$(6,0) \circ_{\mathbb{G}} (5,1) = E_{0,1} \cup E_{0,2}.$$

$$(6,0) \circ_{\mathbb{G}} (6,1) = E_{0,1} \cup E_{0,2}.$$

Also from Equation (4.16), no point lies on $E_{0,4}$.

After all these computations, taking union and bar of these values we have,

$$(\overline{3},\overline{0})\overline{\circ}_{\mathbb{G}}(\overline{3},\overline{1}) = \overline{E}_{0,1} \cup \overline{E}_{0,2}.$$

Now computing values of $(\overline{3},\overline{1})\overline{\circ}_{\mathbb{G}}(\overline{3},\overline{3})$ are computed as follows:

$$\overline{3} \times \overline{1} \circ_{\mathbb{G}} \overline{3} \times \overline{3} = \Big\{(3,1),(5,1),(6,1)\Big\} \circ_{\mathbb{G}} \Big\{(3,6),(5,6),(6,6)\Big\}. \tag{4.17}$$

From Equation (4.17), $(3,1),(5,1),(6,1),(3,6),(5,6),(6,6) \in E_{0,2}$ and no point lies on $E_{0,4}$ and $E_{0,1}$.

All points lies on the same curve *i.e.*, $(u,v) = (u^{'},v^{'}) = (0,2)$, so by using (4.3), first computing:

$$(3,1) \circ_{\mathbb{G}} (3,6).$$

For $g = 1$ and $g^{'} = 1$

$$(3,1) \bullet_{02} (3,6) = \mathcal{O},$$

for $g = 1$ and $g^{'} = 6$

$$(3,1) \bullet_{02} (3,1) = (3,6),$$

for $g = 6$ and $g^{'} = 1$

$$(3,6) \bullet_{02} (3,6) = (3,1)$$

and finally, for $g = 6$ and $g^{'} = 6$

$$(3,6) \bullet_{02} (3,1) = \mathcal{O}.$$

Therefore,

$$(3,1) \circ_{\mathbb{G}} (3,6) = \{\mathbb{O}, (3,6), (3,1)\}.$$

Similarly,

$$(3,1) \circ_{\mathbb{G}} (5,6).$$

For $g = 1$ and $g^{'} = 1$

$$(3,1) \bullet_{02} (5,6) = (0,3),$$

for $g = 1$ and $g^{'} = 6$

$$(3,1) \bullet_{02} (5,1) = (6,6),$$

for $g = 6$ and $g^{'} = 1$

$$(3,6) \bullet_{02} (5,6) = (6,1),$$

and for $g = 6$ and $g^{'} = 6$

$$(3,6) \bullet_{02} (5,1) = (0,4).$$

Therefore,

$$(3,1) \circ_{\mathbb{G}} (5,6) = \{(0,3), (0,4), (6,1), (6,6)\}.$$

Now computing,

$$(3,1) \circ_{\mathbb{G}} (6,6).$$

For $g = 1$ and $g^{'} = 1$

$$(3,1) \bullet_{02} (6,6) = (0,4),$$

for $g = 1$ and $g^{'} = 6$

$$(3,1) \bullet_{02} (6,1) = (5,6),$$

for $g = 6$ and $g^{'} = 1$

$$(3,6) \bullet_{02} (6,6) = (5,1),$$

and for $g = 6$ and $g^{'} = 6$

$$(3,6) \bullet_{02} (6,1) = (0,3).$$

Therefore, we have

$$(3,1) \circ_{\mathbb{G}} (6,6) = \{(0,4),(0,3),(5,1),(5,6)\}.$$

Similarly, computing all other points of Equation (4.17) and we have,

$$\begin{aligned}
(5,1) \circ_{\mathbb{G}} (3,6) &= \{(0,4),(6,6),(6,1),(0,3)\} \\
(5,1) \circ_{\mathbb{G}} (5,6) &= \{\mathcal{O},(5,6),(5,1)\} \\
(5,1) \circ_{\mathbb{G}} (6,6) &= \{(0,3),(0,4),(3,1),(3,6)\} \\
(6,1) \circ_{\mathbb{G}} (3,6) &= \{(0,3),(5,6),(5,1),(0,4)\} \\
(6,1) \circ_{\mathbb{G}} (5,6) &= \{\mathcal{O},(0,4),(0,3),(5,1),(5,6)\} \\
(6,1) \circ_{\mathbb{G}} (6,6) &= \{\mathcal{O},(6,6),(6,1)\}.
\end{aligned}$$

Therefore, we have

$$\{\mathcal{O},(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\}.$$

Taking bar of these values

$$\mathcal{O},(\overline{0},\overline{3}),(\overline{0},\overline{4}),(\overline{5},\overline{1}),(\overline{5},\overline{6}),(\overline{6},\overline{1}),(\overline{6},\overline{6}).$$

Hence,

$$\Rightarrow (\overline{3},\overline{1})\overline{\circ}_{\mathbb{G}}(\overline{3},\overline{3}) = \mathcal{O},(\overline{0},\overline{3}),(\overline{0},\overline{1}),(\overline{3},\overline{1}),(\overline{3},\overline{3}).$$

Similarly all other values can be computed by using Equation (4.3) and (4.12).

All these lengthy calculations gives the following cayley table of $E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})$:

TABLE 4.5: Cayley Table of $E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})$

$\overline{\circ}_{\mathbb{G}}$	$\mathcal{O}$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{3})$	$(\overline{3},\overline{0})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{1})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{3})$
$\mathcal{O}$	$\mathcal{O}$	$(\overline{0},\overline{1}),(\overline{0},\overline{3})$	$(\overline{0},\overline{1}),(\overline{0},\overline{3})$	$(\overline{3},\overline{0})$	$(\overline{1},\overline{3}),(\overline{1},\overline{1})$	$(\overline{1},\overline{3}),(\overline{1},\overline{1})$	$(\overline{3},\overline{1}),(\overline{3},\overline{3})$	$(\overline{3},\overline{1}),(\overline{3},\overline{3})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$
$(\overline{0},\overline{3})$	$(\overline{0},\overline{1}),(\overline{0},\overline{3})$	$E_{\overline{0},\overline{1}}(\overline{\mathbb{F}})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$
$(\overline{3},\overline{0})$	$(\overline{3},\overline{0})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$\mathcal{O},(\overline{3},\overline{0})$	$(\overline{1},\overline{3}),(\overline{0},\overline{3})$	$(\overline{0},\overline{1}),(\overline{1},\overline{1})$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$
$(\overline{1},\overline{3})$	$(\overline{1},\overline{1}),(\overline{1},\overline{3})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$(\overline{1},\overline{3}),(\overline{0},\overline{3})$	$(\overline{0},\overline{1}),(\overline{1},\overline{1})$	$\mathcal{O},(\overline{3},\overline{0})$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1}),(\overline{1},\overline{3})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$(\overline{0},\overline{1}),(\overline{1},\overline{1})$	$\mathcal{O},(\overline{3},\overline{0})$	$(\overline{0},\overline{3}),(\overline{1},\overline{3})$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$
$(\overline{3},\overline{1})$	$(\overline{3},\overline{1}),(\overline{3},\overline{3})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$(\overline{3},\overline{3})$	$\mathcal{O},(\overline{0},\overline{3}),(\overline{0},\overline{1}),(\overline{3},\overline{1}),(\overline{3},\overline{3})$
$(\overline{3},\overline{3})$	$(\overline{3},\overline{1}),(\overline{3},\overline{3})$	$E_{\overline{0},\overline{1}}$	$E_{\overline{0},\overline{1}}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\overline{E}_{0,1}\cup\overline{E}_{0,2}$	$\mathcal{O},(\overline{0},\overline{3}),(\overline{0},\overline{1}),(\overline{3},\overline{1}),(\overline{3},\overline{3})$	$(\overline{3},\overline{1})$

First column of Table 4.5 is representing all values of $(\overline{h},\overline{k})$ and first row is representing all values of $(\overline{h'},\overline{k'})$.

4.3 Applications of Elliptic Hypercurves in cryptography

Elliptic curve cryptography (ECC) is a relatively new branch of public-key cryptography. In comparison with RSA, ECC offers numerous benefits (the most popular public key cryptosystem). ECC can give the same level of security as RSA while using smaller keys; it has enormous capability in a smart card or mobile setting, as well as anywhere strong security is required [29].

Berardi et al. utilised hyperstructures to build some more advanced cryptography systems [10]. Let a finite set A, referred to as *alphabet*, and a non-empty subset $\mathcal{H}$ of $\mathcal{A}$, referred to as *key-set*. Then consider $*$ to be a hyperoperation on $\mathcal{A}$ utilized by the author of [10] satisfying the following condition:

$$a * h = h * a \Rightarrow h = k, \text{ for all } (h,k) \in \mathcal{A}^2, a \in \mathcal{H}.$$

Now consider the sybhypergroup $(E_{m,n}(\mathbb{F}),\circ_{\mathbb{G}})$ of the hypergroup $(E_{\overline{m},\overline{n}}(\mathbb{F}),\circ_{\mathbb{G}})$. The *alphabet set* is defined as:

$$\mathcal{A} = \{u_h | h \in E_{m,n}(\mathbb{F})\}. \tag{4.18}$$

where $u_h = In(h)$ is the inverses of h and $h = (w, t)$, for all $(w, t) \in \mathbb{F}^2$. Observe that

$$In(h) = \{(w, gt)|g \in \mathcal{G}\},\ In(\mathcal{O}) = \mathcal{O}. \tag{4.19}$$

Define the hyperoperation $\diamond$ on $\mathcal{A}$ as follows:

$$u_h \diamond u_k = \{u_x | x \in h \circ_{\mathbb{G}} k\}. \tag{4.20}$$

Theorem 4.6.

$\mathcal{A}$ under hyperoperation '$\diamond$' is a commutative polygroup (canonical hypergroup) which satisfies Berardi's condition [61].

Proof.

Let $(u_h, u_k) = (u_{h'}, u_{k'}) \in A^2$. Then $u_h = u_{h'}$ and $u_k = u_{k'}$. Therefore $h' \in \{h, -h\}$ and $k' \in \{k, -k\}$.

Because

$$h \circ_{\mathbb{G}} k = (-h) \circ_{\mathbb{G}} k = h \circ_{\mathbb{G}} (-k) = (-h) \circ_{\mathbb{G}} (-k).$$

The hyperoperation $\diamond$ is well defined.

Now considered that $(u_h, u_k, u_x) \in A^3$. We have

$$\begin{aligned}(u_h \diamond u_k) \diamond u_x & \\ &= \{u_t | t \in (h \circ_{\mathbb{G}} k) \circ_{\mathbb{G}} x\} \\ &= \{u_t | t \in h \circ_{\mathbb{G}} (k \circ_{\mathbb{G}} x)\} \\ &= u_h \diamond (u_k \diamond u_x).\end{aligned}$$

Further,

$$u_{\mathcal{O}} \diamond u_h = u_h \diamond u_{\mathcal{O}} = u_h.$$

Also $u_{\mathcal{O}} \in u_h \diamond u_k$ if and only if $k = h$. In addition,

suppose that

$$u_h \diamond u_k = u_h \diamond u_x$$

Then

$$h \circ_{\mathbb{G}} k = h \circ_{\mathbb{G}} x.$$

and so $k \in \{x, -x\}$. Hence

$$u_k = u_x.$$

□

Example 4.3.1.

Consider $\mathcal{H} = E_{0,2}(\mathbb{F}) = \{\mathcal{O}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$ from Example 4.2.2.

The values of set $\mathcal{A}$ (set of inverses of $\mathcal{H}$) can be computed by using Equation 4.19.

By Equation 4.19, the inverse of $\mathcal{O}$ is $\mathcal{O}$.

The inverse of $(0,3)$ is computed as follows:

for $g = 1$

$$\begin{aligned}(0,3) &= \{(0, g(3)) | g \in \mathcal{G}\} \\ &= (0,3),\end{aligned}$$

and for $g = 6$, we have

$$\begin{aligned}(0,3) &= \{(0, g(3)) | g \in \mathcal{G}\} \\ &= \Big(0, (6)(3)\Big) \mod 7 \\ &= (0,4).\end{aligned}$$

By Theorem 4.6, $u_h = u_h^{'}$, so

$$(0,3) = (0,4).$$

Similarly, the inverse of $(3,1)$ is computed as follows: for $g = 1$

$$\begin{aligned}(3,1) &= \{(3, g(1)) | g \in \mathcal{G}\} \\ &= (3,1),\end{aligned}$$

and for $g = 6$, we have

$$\begin{aligned}(3,1) &= \{(3, g(1)) | g \in \mathcal{G}\} \\ &= \Big(3, (6)(1)\Big) \mod 7 \\ &= (3,6).\end{aligned}$$

and by Theorem 4.6, $(3,1) = (3,6)$.

Similarly the inverses of $(5,1), (5,6), (6,1)$ and $(6,6)$ can be computed and we have:

$(5,1) = (5,6)$ and $(6,1) = (6,6)$.

So we have the following *alphabet sets*:

Either,

$$\mathcal{A}_1 = \{u_{\mathcal{O}}, u_{(0,3)}, u_{(3,1)}, u_{(5,1)}, u_{(6,1)}\}.$$

Or

$$\mathcal{A}_2 = \{u_{\mathcal{O}}, u_{(0,4)}, u_{(3,6)}, u_{(5,6)}, u_{(6,6)}\}.$$

Now by considering $\mathcal{A}_1$,

$$\mathcal{A}_1 \diamond \mathcal{A}_1 = \{u_{\mathcal{O}}, u_{(0,3)}, u_{(3,1)}, u_{(5,1)}, u_{(6,1)}\} \diamond \{u_{\mathcal{O}}, u_{(0,3)}, u_{(3,1)}, u_{(5,1)}, u_{(6,1)}\}. \quad (4.21)$$

These values can be computed as follows:

$$u_{\mathcal{O}} \diamond u_{(0,3)} = u_{(0,3)},$$

because

$$u_{\mathcal{O}} \diamond u_h = u_h.$$

Similarly other values of $u_h \diamond \mathcal{O}$ can be computed. The value of $u_{(3,1)} \diamond u_{(6,1)}$ is computed as follows:

Here we have $h = (3,1)$ and $k = (6,1)$.

Now by using Equation (4.20), first compute $h \diamond k$. This is computed by using

Equation (4.3).

$$\begin{aligned} u_{(3,1)} \diamond u_{(6,1)} &= (3,1) \circ_{\mathbb{G}} (6,1) \\ &= (3, g(1)) \bullet_{uv} (6, g^{'}(1)) \mod 7. \end{aligned}$$

Now for $g = 1 = g^{'}$, we have

$$(3,1) \bullet_{04} (6,1) = (5,6),$$

for $g = 1$ and $g^{'} = 6$

$$(3,1) \bullet_{04} (6,6) = (0,4),$$

and for $g = 6$ and $g^{'} = 1$

$$(3,6) \bullet_{04} (6,1) = (0,3),$$

here, $(5,6), (0,4), (0,3) \notin \mathcal{A}_1$, so these points will be neglected.
Finally, for $g = 6$ and $g^{'} = 6$, we get

$$(3,6) \bullet_{04} (6,6) = (5,1),$$

so we have

$$(3,1) \circ_{\mathbb{G}} (6,1) = \{(0,3), (5,1)\}.$$

Therefore,

$$u_{(3,1)} \diamond u_{(6,1)} = u_{(0,3)}, u_{(5,1)}.$$

Similarly compute other values of $u_h \diamond u_k$ can be computed. After computation of all values, cayley table of $\mathcal{A}_1$ is given as follows:

TABLE 4.6: Cayley Table of $\mathcal{A}_1$

$\diamond$	$u_{\mathcal{O}}$	$u_{(0,3)}$	$u_{(3,1)}$	$u_{(5,1)}$	$u_{(6,1)}$
$u_{\mathcal{O}}$	$u_{\mathcal{O}}$	$u_{(0,3)}$	$u_{(3,1)}$	$u_{(5,1)}$	$u_{(6,1)}$
$u_{(0,3)}$	$u_{(0,3)}$	$u_{\mathcal{O}}, u_{(0,3)}$	$u_{(6,1)}, u_{(5,1)}$	$u_{(3,1)}, u_{(6,1)}$	$u_{(5,1)}, u_{(3,1)}$
$u_{(3,1)}$	$u_{(3,1)}$	$u_{(6,1)}, u_{(5,1)}$	$u_{\mathcal{O}}, u_{(3,1)}$	$u_{(0,3)}, u_{(6,1)}$	$u_{(0,3)}, u_{(5,1)}$
$u_{(5,1)}$	$u_{(5,1)}$	$u_{(3,1)}, u_{(6,1)}$	$u_{(0,3)}, u_{(6,1)}$	$u_{(\mathcal{O})}, u_{(5,1)}$	$u_{(0,3)}, u_{(3,1)}$
$u_{(6,1)}$	$u_{(6,1)}$	$u_{(3,1)}, u_{(5,1)}$	$u_{(0,3)}, u_{(5,1)}$	$u_{(0,3)}, u_{(3,1)}$	$u_{\mathcal{O}}, u_{(6,1)}$

In Table 4.6, first column is reprsenting all values of u_h and first row is representing all values of u_k. In the same way, by considering A_2, the values of cayly table of $\mathcal{A}_2$ can be computed.

Note: After computing $h \circ_{\mathbb{G}} k = x$ for value of $g = 1, 6$ and $g^{'} = 1, 6$, only those values of x will be considered which belongs to $\mathcal{A}_1$ or $\mathcal{A}_2$.

Chapter 5

Conclusion and Future work

5.1 Conclusion

The aspect of algebraic hyperstructure theory has been a point of emphasis in the last 10 years, where Krasner hyperfield has proven to be a strong tool for solving number of complex problems that are unsolved in classical algebra [61]. Krasner [18] proposed the concepts of hyperfield and hyperring as a generalization of classical fields and rings. The addition is a hyperoperation (multi-valued operation) known as hyperaddition and the set with hyperaddition is a cannonical hypergroup (not a group as in classical rings).
In order to create an appropriate background the innovation of this work is reviewd and illustrate the work in detail as mentioned below:

1. The idea of elliptic curve is extended to elliptic hypercurve over krasner hyperfield. In Krasner hyperfield, hyperoperations $\circ$ such as (hyperaddition $\oplus$, hypermultiplication $\odot$) are used instead of classical operations $+$ and $\cdot$. The elements of elliptic hypercurves are in the form of $\bar{p} = p\mathbb{G}$, where $\mathbb{G}$ is a single group.

2. Three hyperoperations $\circ_{\mathbb{G}}$, $\overline{\circ}_{\mathbb{G}}$ and $\diamond$ are defined on elliptic hypercurves. All these hyperoperations are related to elliptic curve group operations.

i) Hyperoperation $\circ_{\mathbb{G}}$ is solved by using elliptic curve group operation $\bullet_{uv}$ which is basically addition and doubling of points on elliptic curve and hence it is related to elliptic curve group operation. The values of $g, g^{'} \in \mathbb{G}$ vary according to the $\mathbb{F}_p$ given.

ii) In hyperoperation $\overline{\circ}_{\mathbb{G}}$, first elements are changed from $\bar{p}$ to $p\mathbb{G}$, then cartesian product is computed by using $\circ_{\mathbb{G}}$. Only those elements are selected from cartesian product which lies on elliptic curves. After cartestian product and selection of elements, this operation can be solved like $\circ_{\mathbb{G}}$ and hence in this way it is related to elliptic curve group operation and $\circ_{\mathbb{G}}$.

iii) As an application in cryptography, the hyperoperation $\diamond$ is also defined in which elements are in the form of u_h and u_k and this operation is also related to elliptic curve group operations and $\circ_{\mathbb{G}}$.

5.2 Future Work

Using Krasner quotient hyperfields, we may select a set of canonical hypergroups which are denoted by certain specific colours. This collection allows us to encrypt a text message by using canonical hypergroups of several collections at the same time. To improve message security, this study is expanded to more broad hyperstructures, such as Hv-rings.

Bibliography

[1] M Al Tahan and B Davvaz. On the existence of hyperrings associated to arithmetic functions. *Journal of Number Theory*, 174:136–149, 2017.

[2] M Al Tahan and B Davvaz. Strongly regular relations of arithmetic functions. *Journal of Number Theory*, 187:391–402, 2018.

[3] M Al Tahan and Bijan Davvaz. On corsini hypergroups and their productional hypergroups. *Korean Journal of Mathematics*, 27(1):63–80, 2019.

[4] Khurram Ali. *Noncommutative Cryptography using Extra Special Group and Galois Field*. PhD thesis, MPhil Thesis, Capital University of Science and Technology, Islamabad, 2019.

[5] Reza Ameri, Mansour Eyvazi, and Sarka Hoskova-Mayerova. Superring of polynomials over a hyperring. *Mathematics*, 7(10):902, 2019.

[6] Reza Ameri, Mansour Eyvazi, and Sarka Hoskova-Mayerova. Advanced results in enumeration of hyperfields. *AIMS Mathematics*, 5(6):6552–6579, 2020.

[7] Mohamed Barakat, Christian Eder, and Timo Hanke. An introduction to cryptography. *Timo Hanke at RWTH Aachen University*, pages 1–145, 2018.

[8] Minal Wankhede Barsagade and Suchitra Meshram. Overview of history of elliptic curves and its use in cryptography. *International Journal of Scientific & Engineering Research*, 5(4):467–471, 2014.

[9] John A Beachy and William D Blair. *Abstract algebra*. Waveland Press, 2019.

[10] LUIGIA Berardi, Franco Eugeni, and STEFANO Innamorati. Remarks on hypergroupoids and cryptography. 1998.

[11] Chris Christensen. Review of cryptography and network security: Principles and practice. *Cryptologia*, 35(1):97–99, 2010.

[12] Robert Churchhouse, RF Churchhouse, and RF Churchhouse. *Codes and ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge University Press, 2002.

[13] Paul Moritz Cohn. *Basic algebra: groups, rings and fields*. Springer Science & Business Media, 2012.

[14] Alain Connes and Caterina Consani. From monoids to hyperstructures: in search of an absolute arithmetic. In *Casimir force, Casimir operators and the Riemann hypothesis*, pages 147–198. de Gruyter, 2010.

[15] Alain Connes and Caterina Consani. The hyperring of adele classes. *Journal of Number Theory*, 131(2):159–194, 2011.

[16] Piergiulio Corsini. Prolegomena of hypergroup theory. *Aviani editore*, 1993.

[17] Piergiulio Corsini and Violeta Leoreanu. *Applications of hyperstructure theory*, volume 5. Springer Science & Business Media, 2013.

[18] Irina Cristea and Milica Kankaraš. The reducibility concept in general hyperrings. *Mathematics*, 9(17):2037, 2021.

[19] Bijan Davvaz and Vileta Leoreanu-Fotea. *Hyperring theory and applications*, volume 347. International Academic Press, USA, 2007.

[20] Hans Delfs and Helmut Knebl. Symmetric-key cryptography. In *Introduction to Cryptography*, pages 11–48. Springer, 2015.

[21] Whitfield Diffie. New direction in cryptography. *IEEE Trans. Inform. Theory*, 22:472–492, 1976.

[22] Andreas Enge and Pierrick Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 102:83–103, 2002.

[23] Ahmet Eskicioglu and Louis Litwin. Cryptography. *IEEE Potentials*, 20(1):36–38, 2001.

[24] John B Fraleigh. *A first course in abstract algebra*. Pearson Education India, 2003.

[25] Domenico Freni. Strongly transitive geometric spaces: Applications to hypergroups and semigroups theory. 2004.

[26] Stefan Friedl. An elementary proof of the group law for elliptic curves. *Groups Complexity Cryptology*, 9(2):117–123, 2017.

[27] Mohammad Hamidi and Violeta Leoreanu-Fotea. On (2-closed) regular hypergroups. *University Politehnica of Bucharest Scientific Bulletin- Series A-Applied Mathematics and Physics*, 80(4):173–186, 2018.

[28] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[29] Darrel Hankerson, Scott Vanstone, and Alfred Menezes. Cryptographic protocols. *Guide to Elliptic Curve Cryptography*, pages 153–204, 2004.

[30] Razi Hassan and Toheed Qamar. Asymmetric-key cryptography for contiki. Master's thesis, 2010.

[31] Kostaq Hila and Krisanthi Naka. On pure hyperradical in semihypergroups. *International Journal of Mathematics and Mathematical Sciences*, 2012, 2012.

[32] John F Humphreys, Qing Liu, and John F Humphreys. *A course in group theory*, volume 6. Oxford University Press on Demand, 1996.

[33] Zur Izhakian and Louis Rowen. Supertropical algebra. *Advances in Mathematics*, 225(4):2222–2286, 2010.

[34] Jaiung Jun. Algebraic geometry over hyperrings. *Advances in Mathematics*, 323:142–192, 2018.

[35] Jaiung Jun. Geometry of hyperfields. *Journal of Algebra*, 569:220–257, 2021.

[36] Vivek Kapoor, Vivek Sonny Abraham, and Ramesh Singh. Elliptic curve cryptography. *Ubiquity*, 2008(May):1–8, 2008.

[37] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[38] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97. Springer Science & Business Media, 2012.

[39] Marc Krasner. A class of hyperrings and hyperfields. *International Journal of Mathematics and Mathematical Sciences*, 6(2):307–311, 1983.

[40] David W Kravitz. Digital signature algorithm, July 27 1993. US Patent 5,231,668.

[41] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[42] Nan Li. Research on diffie-hellman key exchange protocol. In *2010 2nd International Conference on Computer Engineering and Technology*, volume 4, pages V4–634. IEEE, 2010.

[43] Grigory L Litvinov. Hypergroups and hypergroup algebras. *Journal of Soviet Mathematics*, 38(2):1734–1761, 1987.

[44] Prerna Mahajan and Abhishek Sachdeva. A study of encryption algorithms aes, des and rsa for security. *Global Journal of Computer Science and Technology*, 2013.

[45] Frederic Marty. Sur une generalization de la notion de groupe. In *8th congress Math. Scandinaves*, pages 45–49, 1934.

[46] Christos Massouros and Gerasimos Massouros. An overview of the foundations of the hypergroup theory. *Mathematics*, 9(9):1014, 2021.

[47] Kevin S McCurley. The discrete logarithm problem. In *Proc. of Symp. in Applied Math*, volume 42, pages 49–74. USA, 1990.

[48] Henry McKean and Victor Moll. *Elliptic curves: function theory, geometry, arithmetic*. Cambridge University Press, 1999.

[49] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[50] OKAMOTO T Menezesaj. Vantonesa. reducing elliptic curve logarithms to a finite field. *IEEE Trans. Info. Theory*, 9:1639–1646, 1993.

[51] VS Miller. Use of elliptic curves in cryptography, advances in cryptography crypto'85 (lecture notes in computer science, vol 218), 1986.

[52] S Mirvakili and B Davvaz. Applications of the $\alpha*$-relation to krasner hyperrings. *Journal of Algebra*, 362:145–156, 2012.

[53] Richard A Mollin. *RSA and public-key cryptography*. Chapman and Hall/CRC, 2002.

[54] Peter L Montgomery. A survey of modern integer factorization algorithms. *CWI quarterly*, 7(4):337–366, 1994.

[55] Anastase Nakassis. Recent results in hyperring and hyperfield theory. *International Journal of Mathematics and Mathematical Sciences*, 11(2):209–220, 1988.

[56] M Nordin A Rahman, AFA Abidin, Mohd Kamir Yusof, and NSM Usop. Cryptography: A new approach of classical hill cipher. *International Journal of Security and Its Applications*, 7(2):179–190, 2013.

[57] Steven Roman. *Fundamentals of group theory: An advanced approach*. Springer Science & Business Media, 2011.

[58] Hossein Shojaeijeshvaghani and Reza Ameri. Various kinds of quotient of a canonical hypergroup. *Sigma*, 9(1):133–141, 2018.

[59] William Stallings. *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[60] Douglas R Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.

[61] Vahid Vahedi, Morteza Jafarpour, Hossien Aghabozorgi, and Irina Cristea. Extension of elliptic curves on krasner hyperfields. *Communications in Algebra*, 47(11):4806–4823, 2019.

[62] Muthusamy Velrajan and Arjunan Asokkumar. Note on isomorphism theorems of hyperrings. *International Journal of Mathematics and Mathematical Sciences*, 2010, 2010.

[63] O Ya Viro. On basic concepts of tropical geometry. *Proceedings of the Steklov Institute of Mathematics*, 273(1):252–282, 2011.

[64] THOMAS Vougiouklis. The fundamental relation in hyperrings. the general hyperfield. In *Proc. Fourth Int. Congress on Algebraic Hyperstructures and Applications (AHA 1990), World Scientific*, pages 203–211. World Scientific, 1991.

[65] Thomas Vougiouklis. *Hyperstructures and their representations*. Hadronic Press, 1994.

[66] Thomas Vougiouklis. Fundamental relations in hyperstructures. *Bull. Greek Math. Soc*, 42:113–118, 1999.

[67] Xin Zhou and Xiaofei Tang. Research and implementation of rsa algorithm for encryption and decryption. In *Proceedings of 2011 6th international forum on strategic technology*, volume 2, pages 1118–1121. IEEE, 2011.

[68] Malik Zia and Rashid Ali. Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls. *PloS one*, 13(12):e0208857, 2018.

[69] Malik Zia and Rashid Ali. A multi recipient aggregate signcryption scheme based on elliptic curve. *Wireless Personal Communications*, 115(2):1465–1480, 2020.