ELLIPTIC CURVES OVER A FINITE FIELD AND APPLICATIONS TO CRYPTOGRAPHY

by

Ahmet YAŞAR

August 2006

ELLIPTIC CURVES OVER A FINITE FIELD AND APPLICATIONS TO CRYPTOGRAPHY

by

Ahmet YAŞAR

A thesis submitted to
The Graduate Institute of Sciences and Engineering

of

Fatih University

in partial fulfillment of the requirements for the degree of
Master of Science

in

Mathematics

August 2006
Istanbul, Turkey

APPROVAL PAGE

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Ali ŞAHİN
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Barış KENDİRLİ
Supervisor

Examining Committee Members

Prof. Dr. Barış KENDİRLİ

Assist. Prof. Tevfik BİLGİN

Assist. Prof. Nizamettin BAYYURT

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate Institute of Sciences and Engineering.

Assist. Prof. Nurullah ARSLAN
Director

August 2006

ELLIPTIC CURVES OVER A FINITE FIELD AND APPLICATIONS TO CRYPTOGRAPHY

Ahmet YAŞAR

M.S. Thesis – Mathematics
August 2006

Supervisor: Prof. Dr. Barış KENDİRLİ

ABSTRACT

In this thesis, elliptic curves, elliptic curves over a finite field and cryptography applications of elliptic curves are basically investigated. Especially, I give information about encryption and decryption methods for the cryptosystems which can be defined over a finite field such as Diffie – Hellman , Massey – Omura and ElGamal. These concepts were also supported by the cited examples.

Keywords: Cryptography, encryption, decryption, finite fields, elliptic curves, maple, discriminant, quadratic residue.

SONLU BİR CİSİM ÜZERİNDE ELİPTİK EĞRİLER VE KRİPTOGRAFİ UYGULAMALARI

Ahmet YAŞAR

Yüksek Lisans Tezi – Matematik
Ağustos 2006

Tez Yöneticisi: Prof. Dr. Barış KENDİRLİ

ÖZ

Bu tez çalışmasında, temel seviyede eliptik eğriler, sonlu bir cisim üzerinde eliptik eğriler ve bu eğrilerin Kriptografi uygulamaları incelenmiştir. Özellikle Diffie – Hellman , Massey – Omura ve ElGamal gibi kriptosistemlerinin sonlu bir cisim üzerindeki şifreleme ve deşifre etme yöntemleri hakkında bilgiler verdim. Ayrıca bu sistemler örneklerle desteklendi.

Anahtar Kelimeler: Kriptografi, şifreleme, deşifre, sonlu cisimler, eliptik eğriler, maple, diskriminant, ikinci dereceden kalan.

DEDICATION

To my family

for their endless love and support

ACKNOWLEDGEMENT

I express sincere appreciation to Prof. Dr. Barış KENDİRLİ for his guidance and insight throughout the research.

Thanks go to the other faculty members, Assist. Prof. Tevfik BİLGİN, Assist. Prof. Yaşar SÖZEN, and Assist. Prof. Ali ŞAHİN, for their valuable suggestions and comments.

Lastly, I am glad to thank to my parents, especially, Selman YAŞAR and Mesut YAŞAR for their understanding and endless support.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

Figure

LIST OF SYSMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION	
$\Re^{+}$	Positive Real Numbers
$\Re$	Real Numbers
$\mathbb{C}$	Complex Numbers
$\mathbb{Q}$	Rational Numbers
$\mathbb{Z}$	Integers
$\mathbb{Z}^{+}$	Positive Integers
$F[x]$	Polynomial Ring
$g.c.d(a,n)$	Greatest common divisor of a and n
$d \mid a$	d divides a
$d \nmid a$	d does not divide a
λ	lambda
$a \equiv b(\bmod n)$	congruent
F.L.L	Fermat’s Little Theorem
F_q	Finite field with q elements
$\left(\frac{a}{p}\right)$	Legendre Symbol
E	Elliptic curve E
$E(F_q)$	Elliptic curve over the finite field F_q
∞	Infinite
Δ	Discriminant
$\mid \; \mid$	Absolute value

CHAPTER 1

INTRODUCTION

1.1 WHAT IS CRYPTOGRAPHY

As the field of cryptography has advanced, the dividing lines for what is and what is not cryptography have become blurred. Cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. *Cryptanalysis* is the study of how to compromise (defeat) cryptographic mechanisms, and *cryptology* (from the Greek *kryptós lógos*, meaning ``hidden word") is the discipline of cryptography and cryptanalysis combined. To most people, cryptography is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. However, this is only one part of today's cryptography.

Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. *Decryption* is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form.

Encryption and decryption generally require the use of some secret information, referred to as a *key*. For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different .

Today's cryptography is more than encryption and decryption. *Authentication* is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives - when we sign our name to some document for instance - and, as we move to a world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication.

Cryptography provides mechanisms for such procedures. A *digital signature* binds a document to the possessor of a particular key, while a *digital timestamp* binds a document to its creation at a particular time. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation, or a pay-per-view TV channel.

The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronic money , to prove we know certain information without revealing the information itself, and to share a secret quantity in such a way that a subset of the shares can reconstruct the secret .

While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge, such as decrypting an encrypted message or signing some digital document. The problem may also be hard because it is intrinsically difficult to complete, such as finding a message that produces a given hash value.

1.2 TECHNIQUES IN CRYPTOGRAPHY

1.2.1 Rsa

The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures. Ronald Rivest, Adi Shamir and Leonard Adleman developed the RSA system in 1977; RSA stands for the first letter in each of its inventors' last names.

The RSA algorithm works as follows: take two large primes, p and q, and compute their product $n = pq$; n is called the modulus. Choose a number, e, less than n and relatively prime to $(p\text{-}1)(q\text{-}1)$, which means e and $(p\text{-}1)(q\text{-}1)$ have no common factors except 1. Find another number d such that $(ed - 1)$ is divisible by $(p\text{-}1)(q\text{-}1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). The factors p and q may be destroyed or kept with the private key.

It is currently difficult to obtain the private key d from the public key (n, e). However if one could factor n into p and q, then one could obtain the private key d. Thus the security of the RSA system is based on the assumption that factoring is difficult. The discovery of an easy method of factoring would "break" RSA.

Here is how the RSA system can be used for encryption and digital signatures (in practice, the actual use is slightly different.

1.2.2 Encryption

Suppose Alice wants to send a message m to Bob. Alice creates the ciphertext c by exponentiating: $c = m^e$ mod n, where e and n are Bob's public key. She sends c to Bob. To decrypt, Bob also exponentiates: $m = c^d$ mod n; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt this message.

1.2.3 Digital Signature

Suppose Alice wants to send a message m to Bob in such a way that Bob is assured the message is both authentic, has not been tampered with, and from Alice. Alice creates a digital signature s by exponentiating: $s = m^d$ mod n, where d and n are Alice's private key. She sends m and s to Bob. To verify the signature, Bob exponentiates and checks that the message m is recovered: $m = s^e$ mod n, where e and n are Alice's public key.

Thus encryption and authentication take place without any sharing of private keys: each person uses only another's public key or their own private key. Anyone can send an encrypted message or verify a signed message, but only someone in possession of the correct private key can decrypt or sign a message.

1.2.4 Elliptic curve cryptosystem.

Elliptic curve cryptosystems were first proposed independently by Victor Miller and Neal Koblitz in the mid-1980s. At a high level, they are analogs of existing public-key cryptosystems in which modular arithmetic is replaced by operations defined over elliptic curves. The elliptic curve cryptosystems that have appeared in the literature can be classified into two categories according to whether they are analogs to the RSA system or to discrete logarithm based systems.

Just as in all public-key cryptosystems, the security of elliptic curve cryptosystems relies on the underlying hard mathematical problems. It turns out that elliptic curve analogs of the RSA system are mainly of academic interest and offer no practical advantage over the RSA system, since their security is based on the same underlying problem, namely integer factorization. The situation is quite different with elliptic curve variants of discrete logarithm based systems. The security of such systems depends on the following hard problem: Given two points G and Y on an elliptic curve such that $Y = kG$ (that is, Y is G added to itself k times), find the integer k. This problem is commonly referred to as the *elliptic curve discrete logarithm problem*.

Presently, the methods for computing general elliptic curve discrete logarithms are much less efficient than those for factoring or computing conventional discrete logarithms. As a result, shorter key sizes can be used to achieve the same security of conventional public-key cryptosystems, which might lead to better memory requirements and improved performance. One can easily construct elliptic curve encryption, signature, and key agreement schemes by making analogs of ElGamal, DSA, and Diffie-Hellman. These variants appear to offer certain implementation advantages over the original schemes, and they have recently drawn more and more attention from both the academic community and the industry.

1.2.5 Are elliptic curve cryptosystem secure?

In general, the best attacks on the elliptic curve discrete logarithm problems have been general brute-force methods. The current lack of more specific attacks means that shorter key sizes for elliptic cryptosystems appear to give similar security as much larger keys that might be used in cryptosystems based on the discrete logarithm problem and integer factorization. For certain choices of elliptic curves there do exist more efficient attacks. Menezes, Okamoto, and Vanstone have been able to reduce the elliptic curve discrete logarithm problem to the traditional discrete logarithm problem for certain curves, thereby necessitating the same size keys as is used in more traditional public-key systems. However these cases are readily classified and easily avoided.

In 1997, elliptic curve cryptography began to receive a lot more attention; by the end of 1999, there were no major developments as to the security of these cryptosystems. The longer this situation continues, the more confidence will grow that they really do offer as much security as currently appears. However, a sizeable group of very respected researchers have some doubts as to whether this situation will remain unchanged for many years. In particular, there is some evidence that the use of special elliptic curves, sometimes known as Koblitz curves, which provide very fast implementations, might allow new specialized attacks. As a starting point, the basic brute-force attacks can be improved when attacking these curves. While RSA Laboratories believes that continued research into elliptic curve cryptosystems might eventually create the same level of wide-spread trust as is enjoyed by other public-key techniques (provided there are no upsets), the use of special purpose curves will most likely always be viewed with extreme skepticism.

1.2.6 Diffie-Hellman cryptosystem.

The Diffie-Hellman key agreement protocol (also called exponential key agreement) was developed by Diffie and Hellman in 1976 and published in the ground-breaking paper "New Directions in Cryptography." The protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.

The protocol has two system parameters *p* and *g*. They are both public and may be used by all the users in a system. Parameter *p* is a prime number and parameter *g* (usually called a generator) is an integer less than *p*, with the following property: for every number *n* between 1 and *p*-1 inclusive, there is a power *k* of *g* such that $n = g^k$ mod p.

Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows: First, Alice generates a random private value *a* and Bob generates a random private value *b*. Both *a* and *b* are drawn from the set of integers. Then they derive their public values using parameters p and g and their private values. Alice's public value is g^a mod p and Bob's public value is g^b mod p. They then exchange their public values. Finally, Alice computes $g^{ab} = (g^b)^a$ mod p, and Bob computes $g^{ba} = (g^a)^b$ mod p. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

The protocol depends on the discrete logarithm problem for its security. It assumes that it is computationally infeasible to calculate the shared secret key $k = g^{ab}$ mod p given the two public values g^a mod p and g^b mod p when the prime p is sufficiently large. Maurer has shown that breaking the Diffie-Hellman protocol is equivalent to computing discrete logarithms under certain assumptions.

The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.

The authenticated Diffie-Hellman key agreement protocol, or Station-to-Station (STS) protocol, was developed by Diffie, van Oorschot, and Wiener in 1992 to defeat the man-in-the-middle attack on the Diffie-Hellman key agreement protocol.

The immunity is achieved by allowing the two parties to authenticate themselves to each other by the use of digital signatures and public-key certificates.

Roughly speaking, the basic idea is as follows. Prior to execution of the protocol, the two parties Alice and Bob each obtain a public/private key pair and a certificate for the public key. During the protocol, Alice computes a signature on certain messages, covering the public value g^a mod p. Bob proceeds in a similar way. Even though Carol is still able to intercept messages between Alice and Bob, she can not forge signatures without Alice's private key and Bob's private key. Hence, the enhanced protocol defeats the man-in-the-middle attack.

In recent years, the original Diffie-Hellman protocol has been understood to be an example of a much more general cryptographic technique, the common element being the derivation of a shared secret value (that is, key) from one party's public key and another party's private key. The parties' key pairs may be generated anew at each run of the protocol, as in the original Diffie-Hellman protocol. The public keys may be certified, so that the parties can be authenticated and there may be a combination of these attributes.

In chapter 2, the basic definitions of groups, rings and fields are given.
In chapter 3, finite fields are defined with the basic theorems.
In chapter 4, the cryptosystems such as Massey – Omura and ElGamal are defined over a finite field.
In chapter 5, Quadratic residues and Legendre Symbol are defined.
In chapter 6, the operations on elliptic curves are defined.
In chapter 7, I define elliptic curves over a finite field by an example.
Finally, in chapter 8, elliptic curve cryptosystems over a finite field are defined.

CHAPTER 2

GROUPS RINGS AND FIELDS

2.1 GROUPS

Definition 2.1.1(Herstein, 1996) A nonempty set *G* is said to be a *group* if in G there is defined an operation $*$ such that :

i) a,b$\in G$ implies that $a*b \in G$ (We describe this by saying that *G* is closed under $*$).

ii) Given $a,b,c \in G$, then

$$a*(b*c) = (a*b)*c$$

This is described by saying that the associative law holds in *G*.

iii) There exists a special element $e \in G$ such that

$$a*e = e*a = a \text{ for all } a \in G$$

e is called the *identity* or *unit element* of *G*.

$i\nu$) For every $a \in G$ there exists an element $b \in G$ such that

$$a*b = b*a = e$$

We describe this element *b* as a^{-1} and call it the inverse of *a* in *G*.

These four defining postulates are called *group axioms*.

Example2.1.1 Let $\Re^+$ be the set of all *positive real numbers* and let the operation $*$ on $\Re^+$

Be the ordinary product of *real numbers.* $\Re^+$ is a *group* under $*$.

Definition 2.1.2(Herstein, 1996) A group *G* is said to be *abelian* if

$$a*b = b*a \text{ for all } a,b\in G.$$

Lemma 2.1.1 If G is a group then

i) Its identity element is *unique*.

ii) Every $a \in G$ has a *unique inverse* $a^{-1} \in G$.

iii) If $a \in G \quad (a^{-1})^{-1} = a$

iv) For $a,b \in G \quad (ab)^{-1} = b^{-1}a^{-1}$

2.2 RINGS

Definition2.2.1 A nonempty set R is said to be a *ring* if in R there are two operations + and $\cdot$ such that:

$i)$ $a,b \in R$ implies that $a+b \in R$

$ii)$ $a+b=b+a$ for $a,b \in R$

$iii)$ $(a+b)+c = a+(b+c)$ for $a,b,c \in R$.

iv) There exists an element $\mathrm{O} \in R$ such that $\mathrm{O}+a=a$ for every $a \in R$.

v) Given $a \in R$ there exists $b \in R$ such that $a+b=0$

vi) $a,b \in R$ implies that $a \cdot b \in R$

vii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for $a,b,c \in R$

$viii$) $a.(b+c) = a.b + a.c$ and

$(b+c).a = b.a + c.a$ for $a,b,c \in R$.

Definition 2.2.2(Commutative Ring) A *commutative ring* is a ring R that satisfies this axioms:

$$ab = ba \quad \text{for all} \quad a,b \in R$$

Example2.2.1 The set of integers Z,with the usual addition and multiplication, is a *commutative ring* with identity.

Example2.2.2 The set of *odd integers* with the usual addition and multiplication is not a *ring*.Because the sum of two *odd integers* is not *odd*.

2.3 FIELDS

Definition2.3.1 A *field* is a set F , containing at least two elements, on which two operations + and $\cdot$(called *addition* and *multiplication* ,respectively) are defined so that for each pair of elements x,y in F there are unique elements $x+y$ *and* $x \cdot y$(often written xy) in F for which the following conditions hold for all $x,y,z \in F$:

$i)$ $x+y=y+x$ (commutativity of addition)

$ii)$ $(x+y)+z=x+(y+z)$ (associativity of addition)

$iii)$ There is an element $0 \in F$ called zero, such that $x+0=x.$ (existence of an additive identity)

$iv)$ For each x there is an element $-x \in F$ such that $x+(-x)=0$ (existence of additive inverses)

$v)$ $xy=yx$ (commutativity of multiplication)

$vi)$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)

$vii)$ $(x+y) \cdot z = x \cdot z + y \cdot z$ and $x \cdot (y+z) = x \cdot y + x \cdot z$ (distributivity)

$viii)$ There is an element $1 \in F$, such that $1 \neq 0$ and $x \cdot 1 = x$ (existence of a multiplicative identity)

$ix)$ If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. (existence of multiplicative inverses)

Definition2.3.2(Herstein, 1996) A commutative ring R is an *integral domain* if $a \cdot b = 0$ in R implies that $a=0$ or $b=0$.

Definition2.3.3(Herstein, 1996) A ring R with unit is said to be a *division ring* if for every $a \neq 0$ in R there is an element $b \in R$ (usually written as a^{-1}) such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Definition2.3.4 A ring R is said to be a *field* if R is a *commutative division ring.*

Example2.3.1 Let $R = Z_6$ the integers mod 6, with the addition and the multiplication defined by

$$[a]+[b]=[a+b] \text{ and } [a][b]=[ab].$$

Note that $[0]$ is the 0 required by our axioms for a ring, and $[1]$ is the unit element of R. Note however, that Z_6 is *not an integral domain*, for $[2][3]=[6]=[0]$, yet $[2] \neq [0]$ and $[3] \neq [0]$.R is *commutative ring* with unit.

This example suggests the

Definition2.3.5(Herstein,1996) An element $a \neq 0$ in ring R is a *zero-divisor* in R if $ab=0$ for some $b \neq 0$ in R.

Note that both $[2]$ and $[3]$ in Z_6 are zero-divisors.An integral domain is, of course, a commutative ring without zero-divisors.

Example2.3.2 The set $\Re$ *real numbers* with the usual addition and multiplication, is a *field.*

Example2.3.3 if p is prime, then Z_p is a *field*.

2.3.1 Properties of a Field

1) A *vector space* can be defined over any field F by the same properties that are used to define a vector space over the real numbers.Any vector space has a *basis*, and the number of elements in a basis is called its *dimension*. An *extension field*, i.e., a bigger field containing F is automatically a vector space over F. We call it a *finite extension* if it is a finite dimensional vector space.By the degree of a finite extension we mean its dimension as a vector space. One common way of obtaining extension fields is to *adjoin* an element to F : we say that $K = F(\alpha)$ if K is the field consisting of all rational expressions formed using α and elements of F.(Koblitz, 1994)

2) The *polynomial ring* can be defined over any field F. It is denoted $F[x]$; it consists of all finite sums of powers of x with coefficients in F . One adds and multiplies polynomials in $F[x]$ in the same way as one does with polynomials over the reals.The *degree* d of a polynomial is the largest power of x which occurs with nonzero coefficient; in a *monic* polynomial the coefficient of x^d is 1. We say that *g divides f,* where $f, g \in F\,[x]$, if there exists a polynomial $h \in F\,[x]$ such that *fg=h.* The polynomial $p(x) \in F[x]$ is *irreducible* if $p(x)$ is of positive degree and given any polynomial *f(x)* in $F[x]$, then either $p(x)/f(x)$ or *p(x)* is relatively prime to *f(x).*

3) Given any polynomial $f(x) \in F[x]$ there is an extension field K of F such that *f(x)* splits into a product of linear factors (equivalently, had d roots in K, counting multiplicity,where d is its degree) and such that K is the smallest extension field containing those roots.K is called the *splitting field* of *f.* For example, $Q(\sqrt{2})$ is the splitting field of $f(x) = x^2 - 2$, and to obtain the splitting field of $f(x) = x^3 - 2$ one must adjoin to Q both $\sqrt[3]{2}$ and $\sqrt{-3}$.(Koblitz, 1994)

2.3.2 Characteristic of a Field

Definition2.3.6 If F is a field of k elements for any $a \in F$; na=0 if there exists $n \in Z^{+}$ the smallest number of these positive integers is called the *characteristic* of the field.If there is no such an integer then the characteristic of F is 0.

Example2.3.4 The field of rational numbers Q, the field of real numbers $\Re$ and the field of complex numbers $\mathbb{C}$ has characteristic 0.

CHAPTER 3

FINITE FIELDS

3.1 FINITE FIELDS

Definition3.1.1 Finite field is field which contains finite number of elements.Denoted as F_q where q is the number of elements in it.

Theorem3.1.1 Suppose that F_q is a finite field of q number of elements and characteristic is p with prime subfield F_p .Then we can regard F_q as a vector space over F_p with the dimension of n .We can find a basis $\{e_1, e_2, ..., e_n\}$ for F_q over F_p .Every element F_q of is uniquely expressible in the form;

$$a = e_1\alpha_1 + e_2\alpha_2 + ... + e_n\alpha_n$$

There are just p choices for each coordinate α_i , so the total number of elements in F_q is

$$\underbrace{p.p.p.......p}_{n-times} = p^n$$

3.1.1 Existence of multiplicative generators of finite fields

There are q-1 nonzero elements, and, by the definition of a field, they form an *abelian group* with respect to multiplication.This means that the product of two nonzero elements is nonzero, the associative law and commutative law hold, there is an identity element 1, and any nonzero element has an inverse.It is a general fact finite groups that the order of any element must divide the number of elements in the group. For the sake of completeness, we give a proof of this in the case of our group F_q^* .

Proposition 3.1.1(Koblitz, 1994) The order of any $a \in F_q^*$ divides q-1.

Proof. Let d be the smallest power of a which equals 1. (Note that there is a finite power of a that is 1, since the powers of a in the finite set F_q^* can not all be distinct, and as soon as $a^i = a^j$ for $j > i$ we have $a^{j-i} = 1$.) Let $S = \{1, a, a^2, ..., a^{d-1}\}$ denote the set of all powers of a, and for any $b \in F_q^*$ let bS denote the coset consisting of all elements of the form ba^j .It is easy to see that any two cosets are either identical or distinct (namely: if some b_1a^i in b_1S is also in b_2S, i.e. , if it is of the form b_2a^j , then any element $b_1a^{i'}$ in b_1S is of the form to be in b_2S , because $b_1a^{i'} = b_1a^i \; a^{i'-1} = b_2a^{j+i'-i}$). And each coset contains exactly d elements. Since the union of all the cosets exhausts F_q^*, this means that F_q^* is a disjoint union of d-element sets; hence $d \,|\, (q\text{-}1)$.

Definition3.1.2(Koblitz, 1994) A *generator* g of a finite field F_q is an element of order $q-1$; equivalently, the powers of g run through all of the elements of F_q^* .

Proposition3.1.2(Koblitz, 1994) Every finite field has a generator. If g is a *generator* of F_q^*, then g^j is also a generator if and only if *g.c.d (j,q-1)*=1. In particular , there a total of $\varphi(q-1)$ different generators of F_q^* .

Proof. Suppose that $a \in F_q^*$ has order d, i.e., $a^d = 1$ and no lower power of a gives 1. By proposition(3.1.1), d divides q-1. Since a^d is the smallest power which equals 1, it follows thatthe elements $a, a^2, ...a^d = 1$ are distinct. We claim that the elements of order d are precisely the $\varphi(d)$ values a^j for which $g.c.d(j,d) = 1$. First, since the d distinct powers of a all satisfy the equation $x^d = 1$, these are all of the roots of the equation. Any element of order d must thus be among the powers of a. However, not all powers of a have order d, since if $g.c.d(j,d) = d'$>1, then a^j has lower order : because d/d' and j/d' are integers, we can write $(a^j)^{(d/d')} = (a^d)^{j/d'} = 1$. Conversely, we now show that a^j does have order d whenever $g.c.d(j,d) = 1$.If j is prime to d and if a^j had a smaller order d'', then $a^{d''}$ raised to either the j-th or the d-th power would give 1, and hence $a^{d''}$ raised to the power $g.c.d(j,d)=1$ would give 1. But this contradicts the fact that *a* is of order *d* and so $a^{d''}\neq 1$.Thus ,a^{j} has order d if and only if $g.c.d(j,d)=1$.This means that, if there is an element *a* of order d , then there are exactly $\varphi(d)$ elements of order *d*. So for every $d \mid (q-1)$ there are only two possibilities: no element has order d , or exactly $\varphi(d)$ elements have order d .Now every element has some order $d \mid (q-1)$. And there are either 0 or $\varphi(d)$ elements of order *d*. But

$$\sum_{d\mid(q-1)} \varphi(d) = q-1$$

which is the number of elements in F_q^*.Thus the only way that element can have some order $d \mid (q-1)$ is if there are always $\varphi(d)$ (and never 0)elements of order *d*. In particular, there are $\varphi(q-1)$ elements of order $q-1$; and, if *g* is any element of order $q-1$, then the other elements of order $q-1$ are precisely the powers g^{j} for which $g.c.d(j,q-1)=1$. This completes the proof.

3.1.2 Existence and uniquness of finite fields with prime power number of elements

Proposition3.1.3(Koblitz, 1994) If F_q is a field of $q=p^{f}$ elements, then every element satisfies the equation $x^{q}-x=0$ and F_q is precisely the set of roots of that equation. Conversely, for every prime power $q=p^{f}$ the *splitting field* over F_q of the polynomial $x^{q}-x$ is a field of *q* elements.

Proof. First suppose that F_q is a finite field. Since the order of any nonzero element satisfies the equation $x^{q-1}=1$, and hence, if we multiply both sides by *x* the equation $x^{q}=x$. Of course, the element 0 also satisfies the latter equation. Thus, all *q* elements of F_q are roots of the degree –*q* polynomial $x^{q}-x$. Since this polynomial cannot have more than *q* roots, its roots are precisely the elements of F_q. Notice that this means that F_q is the splitting field of the polynomial $x^{q}-x$, that is , the smallest field extension of F_q which contains all of its roots.

Conversely, let $q = p^f$ be a prime power, and let F be the splitting field over F_p of the polynomial $x^q - x$. Note that $x^q - x$ has derivative $qx^{q-1} - 1 = -1$(because the integer q is a multiple of p and so is 0 in field F_p); hence, the polynomial $x^q - x$ has no common roots with its derivative and therefore has no multiple roots. Thud F must contain at least q distinct roots of $x^q - x$. But we claim that the set of q roots is already a *field*. The key point is that a sum or product of two roots is again a root. Namely, if a and b satisfies the polynomial we have $a^q = a, \quad b^q = b$ and hence $(ab)^q = ab$, i.e., the product is also a root.

Example3.1.1 Consider $Z/(5)$, is isomorphic to $F_5 = \{0,1,2,3,4\}$ with the isomorphism given by: $[0] \to 0,\ [1] \to 1,\ [2] \to 2,\ [3] \to 3,\ [4] \to 4$. The tables for the two operations $+$ *and* $\cdot$ for elements in F_5 are as follows:

Table 3.1 Operations $+$ *and* $\cdot$ for elements in F_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	3

Corollary3.1.1 A finite field has prime characteristic.

Example3.1.2 There is no a finite field containing 6 elements. Because we can not write 6 as p^n i.e., $6 \neq p^n$

Corollary3.1.2 A finite field F has always a subfield with a prime number of elements.

Theorem3.1.2(Lidl and Niederreiter,1994) For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F.

Example3.1.3 Let $f(x) = x^2 + x + 1 \in F_2[x]$. Then $F_2[x]/(f)$ has the $p^n = 2^2$ elements $[0], [1], [x], [x+1]$. The operation tables for this residue class ring are obtained by performing the required operations with the polynomials determining the residue classes and by carrying out $\bmod f$ if necessary:

Table 3.2 Operation tables for residue class ring

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$	$\bullet$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$	$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$	$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$	$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

By inspecting these tables, or from the irreducibility of f over F_2 and theorem(3.1.2), it follows that $F_2[x]/(f)$ is a field. This is an example for which the number of elements is not a prime.

Definition3.1.3 For a finite field F_q we denote by F_q^* the multiplicative group of nonzero elements of F_q.

Theorem3.1.3(Lidl and Niederreiter, 1994) For every finite field F_q the multiplicative group F_q^* of nonzero elements of F_q is cyclic.

Example3.1.4 Construct F_9.

Since $9 = 3^2$ we consider monic irreducible polynomials of degree 2 over F_3: $x^2+1,\ x^2+2,\ x^2+2x+2$. For example letting α be a root of x^2+1 i.e., $\alpha^2+1=0$, so $\alpha^2 = 2$ we can write out the powers of α.

$$\alpha^1 = \alpha\,,$$

$$\alpha^2 = 2\,,$$

$$\alpha^3 = 2\alpha\,,$$

$$\alpha^4 = 2\alpha(\alpha) = 2\alpha^2 = 2(2) = 1$$

and so α has order 4 and does not generate the cyclic group of order 8, i.e., α is not a primitive element. On the other hand, consider λ a root of the polynomial x^2+x+2, so that $\lambda^2+\lambda+2=0$ *or* $\lambda^2 = 2\lambda+1$. Now the powers of λ gives us :

$\lambda^1 = \lambda$

$\lambda^2 = 2\lambda + 1$

$\lambda^3 = \lambda(2\lambda + 1) = 2\lambda^2 + \lambda = 2(2\lambda + 1) + \lambda = 2\lambda + 2$

$\lambda^4 = 2\lambda^2 + 2\lambda = \lambda + 2 + 2\lambda = 2$

$\lambda^5 = 2\lambda$

$\lambda^6 = 2\lambda^2 = \lambda + 2$

$\lambda^7 = \lambda^2 + 2\lambda = 2\lambda + 1 + 2\lambda = \lambda + 1$

$\lambda^8 = \lambda^2 + \lambda = 2\lambda + 1 + \lambda = 1$

So λ is a primitive element and we have represented the elements of F_9 as the 8 powers of λ together with 0.

3.1.3 Automorphisms of Fields

Two fields are said to be *isomorphic* if there exists a bijection from one to the other which preserves both binary operations. If F and K are isomorphic fields then there exists a bijection $f : F \to K$ such that

$$f(x + y) = f(x) + f(y) \text{ and}$$
$$f(xy) = f(x)f(y)$$

for all x and y in F. The map f is called an *isomorphism*.

Definition3.1.4 An isomorphism from a field to itself is called an *automorphism*.

Theorem3.1.4 If F is a finite field of characteristic *p*, then the mapping φ defined by $\varphi(a) = a^p$ is an automorphism of *F*.

Proof. $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$, so φ preserves multiplication. $\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b)$ and addition is preserved. The middle step follows from the binomial theorem and the fact that p is a prime, so all the intermediate coefficients have a factor of p and therefore 0. That φ is a bijection follows from the fact that $\varphi(a) = 0$ implies $a = 0$.

Definition3.1.5 The automorphism $x \to x^p$ is called *Frobenius automorphism* .

Lemma3.1.1 If $q(x)$ in $Z_p[x]$ is irreducible of degree n, then $q(x) \mid (x^m - x)$ where $m = p^n$.

Theorem3.1.5 If K and L are finite fields having the same number of elements, then K and L are isomorphic fields.

Proof. Suppose that K and L have p^n elements. By theorem(3.1.3) L^* is a cyclic group generated, say by the element b in L. Then certainly, $Z_p(b)$- the field obtained by adjoining b to Z_p - is all of L. Since $\lfloor L : Z_p \rfloor = n$, b is algebraic over Z_p of degree *n*, with $n = \deg(q(x))$ where $q(x)$ is the minimal polynomial in $Z_p[x]$ for *b*, and is irreducible in $Z_p[x]$.

The mapping $\psi : Z_p[x] \to L = Z_p(b)$ defined by $\psi(f(x)) = f(b)$ is a homomorphism of $Z_p[x]$ onto *L* with kernel $(q(x))$ the ideal of $Z_p[x]$ generated by $q(x)$. So

$$L \cong Z_p[x]/(q(x))$$

Because $q(x)$ is irreducible in $Z_p[x]$ of degree n by lemma(3.1.1) $q(x)$ must divide $x^m - x$, where $m = p^n$. However, the polynomial $x^m - x$ factors in $K[x]$ as

$$x^m - x = (x - a_1)(x - a_2).....(x - a_m)$$

where $a_1, a_2,.....a_m$ are all the elements of K .Therefore, $q(x)$ divides $(x - a_1)(x - a_2)....(x - a_m)$. Here $q(x)$ can not be relatively prime to all the $x - a_i$ in $K[x]$, hence for some *j,* $q(x)$ and $x - a_j$ have a common factorof degree at least 1.In short $x - a_j$ must divide $q(x)$ in $K[x]$, so $q(x) = (x - a_j)h(x)$ for some $h(x)$ in $K[x]$. Therefore, $q(a_j) = 0$.

Since $q(x)$ is irreducible in $Z_p[x]$ and a_j is a root of $q(x)$, $q(x)$ must be the minimal polynomial for a_j in $Z_p[x]$. Thus $Z_p(a_j) \cong Z_p[x]/(q(x)) \cong L$. This tells us, among other things, that we have$[Z_p(a_j) : Z_p] = n$, and since $Z_p(a_j) \subset K$ and $[K : Z_p] = n$ we conclude that $Z_p(a_j) = K$. Therefore, $K = Z_p(a_j) \cong L$. Thus we get the result that we are after, namely, that *K* and *L* isomorphic fields. This proves the theorem.

Corollary3.1.3 If f is a prime number, then there are $(p^f - p)/f$ distinct monic irreducible polynomials of degree f in $F_p[x]$.

Example3.1.5 Let $f(x) = x^4 + x^3 + x^2 + 1$, $g(x) = x^3 + 1 \in F_2[x]$. Find $g.c.d(f, g)$ using the Euclidean algorithm for polynomials, and Express the $g.c.d$ in the form

$$u(x)f(x) + v(x)g(x)$$

Solution. Polynomial division gives us the sequence of equalities below, which lead to the conclusion that $g.c.d(f, g) = x + 1$, and the next sequence of equalities enables us working backwards, to Express x+1 as a linear combination of f and g . We have:

$$f = (x+1)g + (x^2 + x)$$
$$g = (x+1)(x^2 + x) + (x+1)$$
$$x^2 + x = x(x+1)$$

and then

$$\begin{aligned} x+1 &= g + (x+1)(x^2 + x) \\ &= g + (x+1)(f + (x+1)g) \\ &= (x+1)f + (x^2)g \end{aligned}$$

Example3.1.6 The subfields of the finite field $F_{2^{30}}$ can be determined by lisitng all positive divisors of 30. The containment relations between these various subfields are displayed in the following diagram.

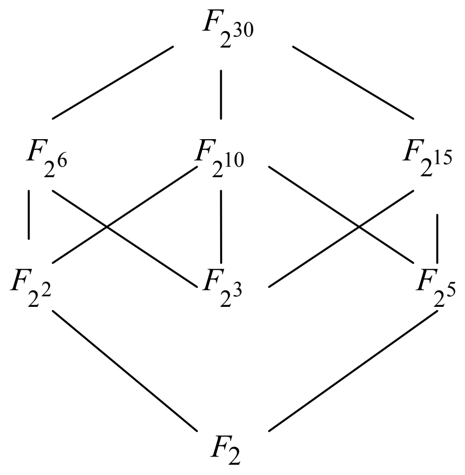


Figure 3.1 Relations between the subfields of $F_{2^{30}}$

Lemma3.1.2(Rosen, 2000) If F is a field of prime characteristic p, then

$$(\alpha+\beta)^{p^n}=\alpha^{p^n}+\beta^{p^n}$$

for all $\alpha,\beta\in F$ and all positive integers *n*.

Proof. Let $\alpha,\beta\in F$. Applying the binomial theorem to $(\alpha+\beta)^p$ we have

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

$$=\alpha^p+0\alpha^{p-1}\beta+0\alpha^{p-2}\beta^2+.....+0\alpha\beta^{p-1}+\beta^p$$

$$=\alpha^p+\beta^p\ .$$

Proceeding by induction on n , suppose that we have $(\alpha+\beta)^{p^{n-1}}=\alpha^{p^{n-1}}+\beta^{p^{n-1}}$. Then

$(\alpha+\beta)^{p^n}=[(\alpha+\beta)^{p^{n-1}}]^p=(\alpha^{p^{n-1}}+\beta^{p^{n-1}})^p=\alpha^{p^n}+\beta^{p^n}$.

CHAPTER 4

FINITE FIELD CRYPTOSYSTEMS

4.1 BASIC NOTIONS

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the *plaintext* and the disguised message is called the *ciphertext*. The plaintext and ciphertext are written some alphabet (usually, but not always, they are written in the same alphabet) consisting of a certain number N of *letters.* The term "*letter*" "(or "*character*") can refer not only to the familiar $\mathrm{A}-Z$, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the message.(If we don't include a blank , for example, then all of the words are run together, and the messages are harder to read.) The process of converting a plaintext to a ciphertext is called *enciphering* or *encryption,* and the reverse process is called *deciphering* or *decryption*.(Koblitz, 1994)

The plaintext and ciphertext are broken up into *message units*. A message unit might be a single letter, a pair of letters(*digraph*), a tirple of letters(*trigraph*), or a block of 50 letters. An *enciphering transformation* is a function that takes any plaintext message unit and gives us a ciphertext message unit. In other words, it is a map f from the set P of all possible plaintext message units to the set C of all possible ciphertext message units. We shall always assume that f is a $1-1$ correspondence. That is, given a ciphertext message unit, there is one and only one plaintext message unit for which it is the encryption.

The *deciphering transformation* is the map f^{-1} which goes back and recovers the plaintext from the ciphertext. We can represent the situation schematically by the diagram

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P \ .$$

Any such set-up is called a *cryptosystem*.

4.1.1 Representation of a message in a finite field F_{p^n}

Since F_{p^n} is an $n-dimensional$ vector space over F_p , $\exists$ a basis

$$\alpha_0, \alpha_1, \ldots\ldots, \alpha_{n-1}$$

such that any element $P \ of \ F_{p^n} \backslash \{0\}$ is uniquely represented as

$$P = a_0\alpha_0 + a_1\alpha_1 + \ldots\ldots + a_{n-1}\alpha_{n-1}$$

where $a_0, a_1, \ldots\ldots, a_{n-1} \in F_p$ not all of them zero. On the other hand ,such a nonzero *n-tuple* $(a_0, a_1, \ldots\ldots, a_{n-1})$ determines a message as an integer

$$\overline{P} = a_0 + a_1 p + a_2 p^2 + \ldots\ldots + a_{n-1}p^{n-1}$$

in

$$\mathrm{Z}_{p^n} \backslash \{0\} = \{1,2,\ldots\ldots, p^n - 1\}$$

If we use an *N*-letter alphabet with *k*-blocks such that

$$N^k \leq p^n - 1$$

then a *k*-block is represented as an integer

$$\overline{\overline{P}} = b_{k-1}N^{k-1} + b_{k-2}N^{k-2} + \ldots\ldots + b_1 N + b_0$$

in

$$\mathrm{Z}_{n^k} = \{0,1,2,\ldots\ldots, N^{k-1}\}$$

$\overline{P} = \overline{\overline{P}} + 1$ determines an element in $\mathrm{Z}_{p^n} \backslash \{0\}$ since $N^k \leq p^n - 1$, thus, an element P is determined in $F_{p^n} \backslash \{0\}$.

Remark. Let $F_{p^n} = F_p(\alpha)$ and unique monic irreducible polynomial be

$$f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots\ldots + c_1 x + c_0$$

Then

$$\{1,\alpha,\alpha^2,.....,\alpha^{n-1}\}$$

is a basis of F_{p^n} over F_p. Thus, any element $P\ in\ F_{p^n}$ can be written uniquely as

$$P = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}$$

where $a_i \in F_p$ for $i = 0,1,2,....,n-1$. Since

$$F_p(\alpha) \simeq F_p[x]\diagup <f>$$

F_{p^n} can be represented by the set of all polynomials of degree less than n,i.e.,

$$\{\, b_{n-1}x^{n-1} + ... + b_2x^2 + b_1x + b_0 : b_i \in F_i \ \text{ for } i = 0,1,2,...,n-1\}$$

where the addition of polynomials is the obvious one and the multiplication of the polynomials can be done the usual multiplication modulo

$$f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_1x + c_0$$

Example4.1.1 $p = 3$, $n = 3$. It is easy to see that $x^3 + 2x^2 + 1$ is irreducible in $Z_3[x]$. Thus,

$$Z_3[x] / < x^3 + 2x^2 + 1 > \simeq F_{3^3}$$

$$F_{3^3} \setminus \{0\} = \{1,2,x,x+1,x+2,2,2x,....,2x^2 + 2x + 2\}$$

Take $N = 26 \le 3^3 - 1$. Then

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	x	x+1	x+2	2x	2x+1	2x+2	x^2	x^2+1	x^2+2	x^2+x	x^2+x+1

N	O	P	Q	R	S	T
x^2+x+2	x^2+2x	x^2+2x+1	x^2+2x+2	$2x^2$	$2x^2+1$	$2x^2+2$

U	V	W	X	Y	Z
$2x^2+x$	$2x^2+x+1$	$2x^2+x+2$	$2x^2+x$	$2x^2+2x+1$	$2x^2+2x+2$

4.2 THE MASSEY-OMURA CRYPTOSYSTEM(For Finite Fields)

We suppose that everyone has agreed upon a finite field F_q, which is fixed and publicly known. Each user of the system secretly selects a random integer e between $0 \text{ } and \text{ } q-1$ such that $\gcd(e,q-1)=1$ and, using the euclidean algorithm, computes its inverse $d=e^{-1} \bmod q-1$ i.e., $de \equiv 1(\bmod q-1)$. If user A (Nikita) wants to send a message P to Michael, first she sends him the element P^{e_A}. This means nothing to Michael, who, not knowing d_A, con not recover P. But, without attempting to make sense of it, he raises it to his e_B, and sends $P^{e_A e_B}$ back to Nikita. The third step is for Nikita to unravel the message part of the way by raising to the $d_A - th$ power , because $P^{d_A e_A} = P$, this means that she returns P^{e_B} to Michael, who can read the message by raising this to the $d_B - th$ power.(Koblitz, 1994)

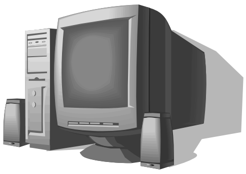
The idea behind this system is rather simple, and it can be generalized to settings where one is using other processes besides exponentiation in finite fields. However, some words of caution are in order. First of all, notice that it is absolutely necessary to use a good signature scheme along with the Massey-Omura system. Otherwise, any person C who is not supposed to know the message P could pretend to be Michael, returning to Nikita $P^{e_A e_C}$; not knowing that an intruder was using his own e_C, she would proceed to raise to the d_A and make it possible for C to read the message. Thus, the message $P^{e_A e_B}$ from Michael to Nikita must be accompained by some authentification, i.e., some message in some signature scheme which only Michael could have send.

In the second place, it is important that, after a user such as B or C has deciphered various messages P, and so knows various pairs (P, P^{e_A}), he can not use that information to determine e_A. That is suppose Michael could solve the discrete log problem in F_q^*, thereby determinig from P and P^{e_A} what e_A must be. In that case he could quickly compute $d_A = e_A^{-1} \bmod q-1$ and then intercept and read all future messages from Nikita, whether intended for him or not.

4.2.1 Massey-Omura Protocol

Nikita

Michael



1. Nikita selects a private number e_A , $0 \le e_A \le p-2$

1. Michael selects a private number $e_B, 0 \le e_B \le p-2.$

2. Nikita calculates $d_A \equiv e_A^{-1} \bmod (p-1)$

2. Michael calculates $d_B = e_B^{-1} \bmod (p-1)$

3. Nikita calculates $m^{e_A} \bmod p.$

$\boxed{m^{e_b}}$

4. Michael calculates $(m^{e_A})^{e_B} \bmod p.$

$\boxed{m^{e_A e_B}}$

5. Nikita selects a private number $(m^{e_A e_B})^{d_A} = m^{e_B} \pmod p$.

$\boxed{m^{e_B}}$

6.Michael calculates $(m^{e_B})^{d_B} \bmod p = m$

Figure 4.1 Massey-Omura Cryptosystem Protocol

Example4.2.1 Take the finite field F_{3^3} .Suppose that Alice chooses $e_A = 3$. It is correct since $g.c.d(3,26) = 1$. Its arithmetic inverse d_A=9. Alice sends plaintext

$$\text{“}go\text{”}$$

to Bob as

$$((2x+1)^3,(x^2+2x)^3)=(2x^2+2, x^2+2x+1)$$

since x^3=x^2+2. So ,Bob receives ciphertext

$$(t,p)$$

If the private key of Bob is $e_B = 5$,then $d_B = 21$ and Bob sends

$$((2x^2+2)^5 , (x^2+2x+1)^5) = (x^2+x+1 , 2x+1) = (m, g)$$

to Alice since

$$by\ Maple : (Rem(2x^2+2)^5 , x^3+2x^2+1 , x) \bmod 3 \text{ gives } x^2+x+1$$

and

$$By\ Maple : (Rem((x^2+2x+1)^5 , x^3+2x^2+1 , x)\ mod\, 3 \text{ gives } 2x+1$$

Now , Alice sends

$$((x^2+x+1)^9 , (2x+1)^9) = (2x^2+1 , x^2+x+2) = (s, n)$$

to Bob since

$$By\ Maple : (Rem\ ((x^2+x+1)^9 , x^3+2x^2+1 , x)\ mod\, 3 \text{ gives } 2x^2+1$$

$$By\ Maple : (Rem((2x+1)^9 , x^3+2x^2+1 , x)\ mod\, 3 \text{ gives } x^2+x+2 .$$

Bob can obtain the original plaintext by calculating

$$((2x^2+1)^{21} , (x^2+x+1)^{21}) = (2x+1) , x^2+2x) = (g, o)$$

since

$$By\ Maple : (Rem((2x^2+1)^{21} , x^3+2x^2+1 , x)\ mod\, 3 \text{ gives } 2x+1$$

and

$$By\ Maple : (Rem((x^2+x+1)^{21} , x^3+2x^2+1 , x)\ mod\, 3 \text{ gives } x^2+x$$

Example4.2.2 The *Massey-Omura Cryptosystem* Works as follows.

Setup

- p , a large prime number, is chosen and made public.
- Nikita chooses private integers e_A and d_A such that $e_A.d_A \equiv 1(\bmod p-1)$.

- Michael chooses private integers e_B and d_B such that $e_B.d_B \equiv 1(\bmod p-1)$.

For Nikita to send a message $m \in \{1,2,...,p-1\}$ to Michael:

- Nikita computes $c_0 = m^{e_A} \bmod p$ and sends it to Michael.
- Michael computes $c_1 = c_0^{e_B} \bmod p$ and sends it to Nikita.
- Nikita computes $c_2 = c_1^{d_A} \bmod p$ and sends it to Michael.
- Michael computes $c_3 = c_2^{d_B} \bmod p$.

Show that $m = c_3$

Since $e_A.d_A \equiv 1(\bmod p-1)$ *and* $e_B.d_B \equiv 1(\bmod p-1)$, there are integers k_A and k_B such that $e_A.d_A = k_A(p-1)+1$ *and* $e_B.d_B = k_B.(p-1)+1$.

Now,clearly

$$c_3 = m^{e_A.e_B.d_A.d_B}.$$

Note that

$$e_A.e_B.d_A.d_B = (k_A.(p-1)+1).(k_B.(p-1)+1) =$$

$$k_A.k_B(p-1)^2 + (k_A + k_B)(p-1)+1 \quad \text{and}$$

$$\begin{aligned} c_3 &\equiv m^{e_A.e_B.d_A.d_B} \\ &\equiv m^{k_A k_B (p-1)^2 + (k_A + k_B)(p-1)+1} \\ &\equiv (m^{p-1})^{k_A k_B (p-1)}.(m^{p-1})^{k_A + k_B}.m^1 \\ &\equiv (1)^{k_A k_B (p-1)}.(1)^{k_A k_B (p-1)}.m \quad \text{(By } F.L.L\text{)} \\ &\equiv m \end{aligned}$$

4.3 THE ELGAMAL CRYPTOSYSTEM(For Finite fields).

We start by fixing a very large finite field F_q and element $g \in F_q^*$ (preferably, but not necessary, a generator). We suppose that we are using plaintext message units with numerical equivalents P in F_q. Each user A randomly chooses an integer $a = a_A$, say in the range $0 < a < q-1$. This integer a is the secret deciphering key. The public enciphering key is the element $g^a \in F_q$.

To send a message P to the user A, we choose an integer k at random, and then send A the following pair of elements of F_q:

$$(g^k, Pg^{ak})$$

Notice that we can compute g^{ak} without knowing a, simply by raising g^a to the $k-th\ power$. Now A, who knows a, can recover P from this pair by raising the first element g^k to the $a-th\ power$ and dividing the result into the second element. In other words what we send A consists of a disguised form of the message $-P$ is "*wearing a mask*" g^{ak} - along with a "clue" , namely g^k, which can be used to take off the mask .

4.3.1 The ElGamal Algorithm

Key Generation

- Select a large prime p and g, a primitive element $\bmod p$.
- Recipient Michael has a secret number a and computes $b \equiv g^a (\bmod p)$

The ElGamal Encryption Algorithm

$i)$ Sender (Nikita) a random number k , $0 \le k \le p-1$

$ii)$ Computes the message key, $K \equiv b^k (\bmod p)$

$iii)$ k and K are used to compute the ciphertext (c_1, c_2) for message m

$$c_1 \equiv g^k (\bmod p)$$
$$c_2 \equiv Km (\bmod p)$$

$iv)$ This then sent to recipient

The ElGamal Decryption Algorithm

To decrypt the message is deterministic and consists of two steps:

$i)$ Extracts the message key $K \equiv c_1^a (\bmod p)$

$ii)$ K is used to unmask the plaintext message m

$$m \equiv c_2 K^{-1} (\bmod p)$$

Example4.3.1 Take the finite field F_{3^3} and $g = x$. Suppose that Bob chooses $a = 3$. Then

$$g^a = x^3 = -2x^2 - 1 = x^2 + 2$$

is public key. Suppose that Alice chooses $k = 2$. Then ,Alice sends plaintext

"*help*"

to Bob as

$$(x^2,(2x+2)x^6),(x^2,(x+2)x^6),(x^2,(x^2+2x+1)x^6)$$

Since

$$x^6 = (x)^2 = (x^2+2)^2 = x^3x + 4x^2 + 4 = (x^2+2)x + x^2 + 1$$

$$= x^3 + x^2 + 2x + 1$$

$$= x^2 + 2 + x^2 + 2x + 1$$

$$= 2x^2 + 2x$$

$(2x+2)(2x^2+2x) = 4x^3 + 8x^2 + 4x = (x^2+2) + 2x^2 + x = x + 2$,

$(x+2)(2x^2+2x) = 2x^3 + 6x^2 + 4x = 2(x^2+2) + x = 2x^2 + x + 1$,

$(x^2+x)(2x^2+2x) = 2x^4 + 4x^3 + 2x^2 =$

$2x(x^2+2) + x^2 + 2 + 2x^2 = 2(x^2+2) + 4x + 2 = 2x^2 + x$,

$(x^2+2x+1)(2x^2+2x) = 2x^4 + 6x^3 + 6x^2 + 2x =$

$2x(x^2+2) + 2x = 2(x^2+2) + 6x = 2x^2 + 1$.

Thus, Bob receives ciphertext as

"(I,E) , (I,V) , (I,U) , (I,S)"

Since it is the correspondent of

$$(x^2, x+2)\ ,\ (x^2, 2x^2+x+1)\ ,\ (x^2, 2x^2+2x)\ ,\ (x^2, 2x^2+1)\ .$$

Example4.3.2 Suppose, $p = 97$ with primitive root $g = 5$

Recipient Michael chooses secret $a = 58$ computes and publishes his public key:

$$b \equiv 5^{58} (\mathrm{mod}\, 97) = 44$$

Nikita wishes to send the message $m = 3$ to Michael.

She obtains Michael's public key $a = 58$.

She chooses random $k = 36$ and computes stream key:

$$K = b^k (\bmod p) \Rightarrow K \equiv 44^{36} (\bmod 97) = 75$$

She then computes the ciphertext pair:

$$c_1 \equiv g^k (\bmod p) \Rightarrow c_1 \equiv 5^{36} (\bmod 97) = 50$$

$$c_2 \equiv Km (\bmod p) \Rightarrow c_2 \equiv 75.3 (\bmod 97) = 31$$

and sends the ciphertext $(50,31)$ to Michael. Michael recovers the message key

$$K \equiv c_1^a (\bmod p) \Rightarrow K \equiv 50^{58} (\bmod 97) = 75$$

Michael computes the inverse

$$K^{-1} \equiv 22 (\bmod 97)$$

Michael recovers the message m

$$m \equiv 31.22 (\bmod 97) = 3$$

4.4 THE DIFFIE-HELLMAN KEY EXCHANGE SYSTEM

Because public key cryptosystems are relatively slow compared to classical crypyosystems, it is often more realistic to use them in a limited role in conjunction with a classical cryptosystem in which the actual messages are transmitted. In particular, the process of agreeing on a key for a classical cryptosystem can be accomplished fairly efficiently using a public key system. The first detailed proposal for doing this, due to W.Diffie and M.E.Hellman, was based on the discrete logarithm problem.(Koblitz, 1994)

We suppose that the key fort he classical cryptosystem is a large randomly chosen positive integer (or a collection of such integers).For example, suppose wewant to use an afine matrix transformation of pairs of digraphs.

$$C \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} P + \begin{pmatrix} e \\ f \end{pmatrix} \bmod N^2$$

where $0 \le a,b,c,d,e,f \le N^2$ and P is a column vector consisting of the numerical equivalents of two successive plaintext digraphs in a $N - letter$ alphabet. Once we have a randomly selected k

$$0 < k < N^{12}$$

We can take a , b , c , d , e ,f to be the six digits in k written to the base N^2.(We must check that $ad-bc$ is invertible modulo N^2, i.e., that it has no common factor with N ; otherwise we choose another random integer k .)
We observe that choosing a random integer in some interval is equivalent to choosing a random element of a large finite field of roughly the same size. Let us suppose, for example, that we want to choose a random positive $k < N^{12}$. If our finite field is a prime field of p elements, we simply let an element of F_p correspond to an integer from 0 *to* $p-1$ in the usual way; if the resulting integer is larger than N^{12}, we reduce it modulo N^{12}.

We now describe the Diffie-Hellman method for generating a random element of a large finite field F_q. We suppose that q is public knowledge; everyone knows what finite field our key will be in. We also suppose that g is some fixed element of F_q, which is also not kept secret. Ideally, g should be a generator of F_q^*; however, this is not absolutely necessary. The method described below for generating a key will lead only to elements of F_q which are powers of g; thus, if we really want our random element of F_q^* to have a chance of being any element, g must be a generator.

Suppose that two users N (Nikita) and M (Michael) want to agree upon a key which they will use to encrypt their subsequent messages to one another. Nikita chooses a random integer a between 1 *and* $q-1$, which she keeps secret, and computes $g^a \in F_q$, which she makes public. Michael does the same: He chooses a random b and makes public g^b. The secret key they use is then g^{ab}. Both users compute this key. For example, Nikita knows g^b and her own secret a.

4.4.1 Diffie-Hellman Setup

All users agree on global parameters:

- Large prime integer or polynomial q
- α a primitive root mod q

Each user generates their key

- Chooses a secret key (number): $x_N < q$
- Compute their public key: $y_N = \alpha^{x_N} \bmod q$

Each user makes public that key y_N

4.4.2 Diffie - Hellman Key Exchange

Shared session key for users $N \ and \ M$ is K_{NM} :

$$K_{NM} = \alpha^{x_N . x_M} \bmod q$$

$$= y_N^{x_M} \bmod q \quad \text{(which M can compute)}$$

$$= {y_M}^{x_N} \bmod q \quad \text{(which N can compute)}$$

K_{NM} is used as session key in private-key encryption scheme between Nikita and Micheal. If Nikita and Micheal subsequently communicate, they will have the same key as before, unless they choose new public-keys attacker needs an x, must solve discrete log.

Example4.4.1

Users Nikita and Micheal who wish to swap keys:

Agree on prime $q = 353$ and $\alpha = 3$

Select random secret keys:

- N chooses $x_N = 97$, M chooses $x_M = 233$

Compute public keys:

- $y_N = 3^{97} \bmod 353 = 40$ (Nikita)
- $y_M = 3^{233} \bmod 353 = 248$ (Micheal)

Compute shared session key as:

$$K_{NM} = {y_M}^{x_N} \bmod 353 = 248^{97} = 160 \qquad \text{(Nikita)}$$

$$K_{NM} = {y_N}^{x_M} \bmod 353 = 40^{233} = 160 \qquad \text{(Michael)}$$

Example4.4.2 Suppose that Alice and Bob agree to communicate using affine enciphering transformation

$$C \equiv AP + B \ mod \ \text{N}.$$

The message units are single letters in the 29- letter alphabet with A-Z corresponding to 0-25, *blank*=26, .=27, ?=28. Regard the key (A,B) as an element of

$$A + Bx \ in \ F_{29^2} \setminus \{0\}$$

Here we can take

$$x^2 + x + 1$$

as irreducible polynomial of degree 2 in $Z_{29}[x]$ and $g = x$. Let Alice chooses $a = 128$. Then

$$g^{128} = x^{128} = 28x + 28$$

$$(By\ Maple : (Rem(x^{128}, x^2 + x + 1, x) \bmod 29 \text{ gives } 28x + 28)$$

is made public by Bob.

a) The enciphering key

$$g^{ab} = (x^{128})^{220} = (28x + 28)^{220} = 28x + 28$$

b) The ciphertext of Alice corresponding to

"*are you in danger*?"

is

?*lyceoicupcz*?*pwyla*

since

(28.0+28,28.17+28,28.4+28,28.26+28,28.24+28,28.14+28,
28.20+28,28.26+28,28.8+28,28.13+28,28.26+28,28.3+28,
28.0+28,28.13+28,28.6+28,28.4+28,28.17+28,28.28+28)

is equal to

(28,11,24,2,4,14,8,2,20,15,2,25,28,15,22,24,11,0) *modulo* 29.

Example4.4.3 Suppose $p = 347$ and $g = 11 (g = 11\ generates\ Z^*_{347})$

Nikita randomly selects $x_N = 240$ computes $y_N = 11^{240} (\bmod 347) = 49$ and sends $y_N = 49$ to Michael.

Michael randomly selects $x_M = 39$ computes $y_M = 11^{39} (\bmod 347) = 285$ and sends $y_M = 285$ to Nikita. Nikita computes $y_M^{x_N} \equiv 285^{240} (\bmod 347) = 268$

Michael computes $y_N^{x_M} \equiv 49^{39} (\bmod 347) = 268$

CHAPTER 5

QUADRATIC RESIDUES AND LEGENDRE SYMBOL

5.1 QUADRATIC RESIDUES

Proposition5.1.1(Koblitz, 1994) Let g be a generator of F_q^*. Then g^j is an n-th root of unity if and only if $nj \equiv 0 \bmod q-1$. The number of n-th roots of unity is $g.c.d(n,q-1)$. In particular, F_q has a primitive n-th root of unity if and only if $n \mid q-1$. If ξ is a primitive n-th root of unity in F_q, then ξ^j is also a primitive n-th root if and only if $g.c.d(j,n)=1$.

Proof. Any element of F_q^* can be written as a power g^j of the generator g. A power of g is 1 if and if only the power is divisible by $q-1$. Thus, an element g^j is an n-th root of unity if and only if $nj \equiv 0 \bmod q-1$. Next, let $d = g.c.d(n,q-1)$. The equation $nj \equiv 0 \bmod q-1$ is equivalent to the equation $\frac{n}{d} j \equiv 0 \bmod (\frac{q-1}{d})$. Since n/d is prime to $q-1/d$, the latter congruence is equivalent to requiring j to be a multiple of $q-1/d$. In other words the d distinct powers of $g^{q-1/d}$ are precisely the n-th roots of unity. There are n such roots if and only if $d = n$, i.e., $n \mid q$-1. Finally, if n divides $q-1$, let $\xi = g^{(q-1)/n}$. Then ξ^j equals 1 if and only if $n \mid j$. The k-th power of ξ^j equals 1 if and only if $kj \equiv 0 \bmod n$. It is easy to see that ξ^j has order n. İf and only if j is prime to n. Thus there are $\varphi(n)$ different primitive n-th roots of unity if $n \mid q$-1 . This completes the proof.

Corollary5.1.1(Koblitz, 1994) If $g.c.d(n,q-1)=1$, then 1 is the only n-th root of unity.

Corollary5.1.2 The element $-1 \in F_q$ has a square root in F_q if and only if $q \equiv 1 \bmod 4$.

Definition5.1.1 Burton, 2002) Let p be an odd prime and $g.c.d(a,p)=1$. If the quadratic congruence $x^2 \equiv a \bmod p$ has a solution, then a is said to be a *quadratic residue* of p. Otherwise a is called a *quadratic nonresidue* of p.

Example5.1.1 Consider the case of the prime $p=13$. To find out how many of the integers 1,2,3,….,12 are quadratic residues of 13, we must know which of the congruences

$$x^2 \equiv a(\bmod 13)$$

are solvable when a runs through the set $\{1,2,3,\ldots.,12\}$. Modulo 13, the squares of the integers 1,2,3,….,12 are

$$\begin{gathered}1^2 \equiv 12^2 \equiv 1\\ 2^2 \equiv 11^2 \equiv 4\\ 3^2 \equiv 10^2 \equiv 9\\ 4^2 \equiv 9^2 \equiv 3\\ 5^2 \equiv 8^2 \equiv 12\\ 6^2 \equiv 7^2 \equiv 10\end{gathered}$$

Consequently, the quadratic residues of 13 are 1,3,4,9,10,12, and 2,5,6,7,8,11 are quadratic nonresidues.

Theorem5.1.1(Euler's Criterion)(Burton, 2002) Let p be an odd prime and $g.c.d(a,p)=1$. Then a is a quadratic residue of p if and only if

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

Corollary5.1.3(Burton, 2002) Let p be an odd prime and $g.c.d(a,p)=1$. Then a is a quadratic residue or nonresidue of p according to whether

$$a^{(p-1)/2} \equiv 1(\bmod p) \quad \text{or} \quad a^{(p-1)/2} \equiv -1(\bmod p)$$

Example5.1.2 In the case where $p=13$, we find that

$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1(\bmod 13)$

Thus by the Corollary(5.1.3), the integer 2 is a quadratic nonresidue of 13.

Theorem5.1.2 The number of quadratic residues is equal to the number of quadratic nonresidues.

5.2 LEGENDRE SYMBOL

Let a be an integer and p>2 a prime. We define the *Legendre symbol* $(\frac{a}{p})$ equals to 0,1 or -1 , as follows :

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue } mod\, p \text{ ;} \\ -1, & \text{if } a \text{ is a quadratic nonresidue } mod\, p \text{ .} \end{cases}$$

Thus, the Legendre symbol is simply a way of identifying whether or not an integer is a quadratic residue modulo p.(Koblitz, 1994)

Proposition5.2.1

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

Proof. If a is divisible by p, then both sides are $\equiv 0 \bmod p$. Suppose p∤a . By Fermat's Little Theorem , in F_p the square of $a^{(p-1)/2}$ is 1, so $a^{(p-1)/2}$ itself is ± 1. Let g be a generator of F_p^*, and let $a = g^j$. As we saw a is a residue if and only if j is even. And $a^{(p-1)/2} = g^{j(p-1)/2}$ is 1 if and only if $j(p-1)$ is divisible by $p-1$, i.e., if and only if j is even. Thus, both sides of the congruence in the proposition are ± 1 in F_p, and each side is +1 if and only if j is even.

5.2.1 Properties of Legendre Symbol.

Theorem5.2.1

i) If $a \equiv b (\bmod p)$, then $(a/p) = (b/p)$

ii) $(a^2/p) = 1$

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

iv) $(ab/p) = (a/p)(b/p)$

$v)\ (1/p)=1$ and $(-1/p)=(-1)^{(p-1)/2}$

$vi)\ (ab^2/p)=(a/p)(b^2/p)=(a/p)$.

Example5.2.1 Let us ascertain whether the congruence $x^2 \equiv -46(\mathrm{mod}17)$ is solvable.

This can be done by evaluating the Legendre symbol $(-47/17)$. We first appeal to properties (iv) and (v) of Theorem(5.2.1) to write

$$(-46/17)=(-1/17)(46/17)=(46/17)$$

Because $46 \equiv 12(\mathrm{mod}17)$ it follows that

$$(46/17)=(12/17)$$

Now property (vi) gives

$$(12/17)=(3.2^2/17)=(3/17)$$

But

$$(3/17)\equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1(\mathrm{mod}17)$$

where we have made appropriate use of property (iii) of theorem(5.2.1) ; hence $(3/17)=-1$. Inasmuch as $(-46/17)=-1$ the quadratic congruence $x^2 \equiv -46(\mathrm{mod}17)$ admits no solution.

CHAPTER 6

ELLIPTIC CURVES

6.1 GENERAL INFORMATION

Elliptic curves have been extensively studied for over a hundred years, and there is a vast literature on the topic. Orginally pursued mainly for aesthetic reasons, elliptic curves have been recently become a tool in several important applied areas, including coding theory, pseudorandom bit generation; and number theory algorithms (Goldwasser and Kilian for primalitiy proving and Lenstra for integer factorization).

Over the last two or three decades,elliptic curves have been playing an increasingly important role both in number theory and in related fields such as Cryptography.For example in 1980's elliptic curves started being used in Cryptography and elliptic curve techniques were developed for factorization and primality testing.It became famous after the proof of Fermat's Last Theorem.(By Wiles)

In 1985, Koblitz and Miller independently proposed using the group of points on an elliptic curve defined over a finite field in discrete log cryptosystems.The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field(and also over systems based on the intractability of integer factorization) is the absence of a subexponential-time algorithm that could find discrete logs in these groups. Consequently, one can use an elliptic curve group that is smaller in size while maintaining the same level of security.The result is smaller key sizes, bandwidth savings, and faster implementations, features which are especially attractive foe security applicaitons where computational power and integrated circuit space is limited, such as smart cards, PC(personal computer) cards, and wireless devices.

Elliptic curves also appear in the so-called elliptic curve analogues of the RSA cryptosystem, as first proposed by Koyama. In these systems, one works in an elliptic curve defined over the ring Z_n, and the order of the elliptic curve group serves as the trapdoor. The security of these schemes is based on the difficulty of factoring n. They are called elliptic because these equations first arose in the calculation of the arc lenght of ellipses.

Definition6.1.1(Koblitz, 1994) Let K be a field of characteristic $\neq 2,3$, and let $x^3 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots. An *elliptic curve* over *K* is the set of points (*x,y*) with $x, y \in K$ which satisfy the equation

$$y^2 = x^3 + ax + b \qquad (1)$$

Together with a single element denoted ∞ and called the " point at infinity"

If *K* is a field of characteristic 2, then an *elliptic curve* over K is the set of points satisfying an equation of the type either

$$y^2 + cy = x^3 + ax + b \qquad (2)$$

or else

$$y^2 + xy = x^3 + ax^2 + b \qquad (3)$$

(here we do not care whether or not the cubic on the right has multiple roots) together with a "point at infinity" ∞.

If *K* is a field of characteristic 3, then an *elliptic curve* over K is the set of points satisfying the equation

$$y^2 = x^3 + ax^2 + bx + c \qquad (4)$$

Definition6.1.2(Koblitz, 1994) Let E be an elliptic curve over the real numbers and let P and Q be two points on E. We define the negative of P and the sum $P + Q$ according to the following rules:

1) If *P* is the point at infinity ∞, then we define $-P$ to be ∞ and $P + Q$ to be Q; that is, ∞ serves as the additive identity of the group of points. In what follows, we shall suppose that neither P nor Q is the point at infinity.

2) The negative $-P$ is the point with the same x-coordinate but negative the y-coordinate of P, i.e., $-(x,y)=(x,-y)$. It is obvious from (1) that $(x,-y)$ is on the curve whenever (x,y) is.

3) If P and Q have different x-coordinates, then it is not hard to see that the line $l=\overline{PQ}$ intersects the curve in exactly one more point R (unless that line is tangent to the curve at P,in which case we take $R=P$, or at Q , in which case we take $R=Q$). Then define $P+Q$ to be $-R$, i.e., the mirror image (with respect to the x-axis) of the third point of intersection.

4) If $Q=-P$ (i.e., Q has the same x-coordinate but minus the y-coordinate), then we define $P+Q=\infty$ (the point at infinity).

5) The final possibility is $P=Q$. Then let l be the tangent line to the curve at P , let R be the only other point of intersection of l with the curve , and define $P+Q=-R$.

Example6.1.1

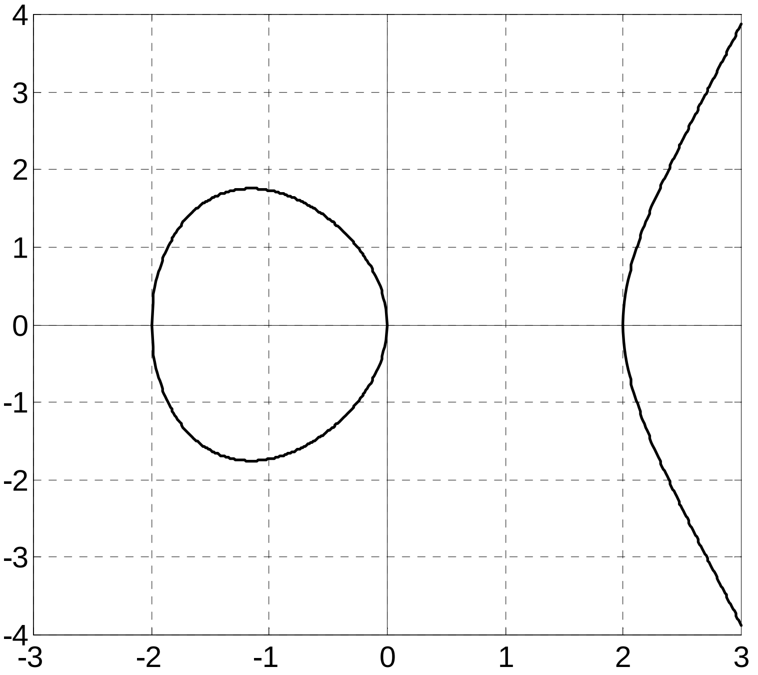


Figure 6.1 The elliptic curve $y^2=x(x^2-1)$

6.1.1 Adding Points *P* and *Q* – Geometric Approach.

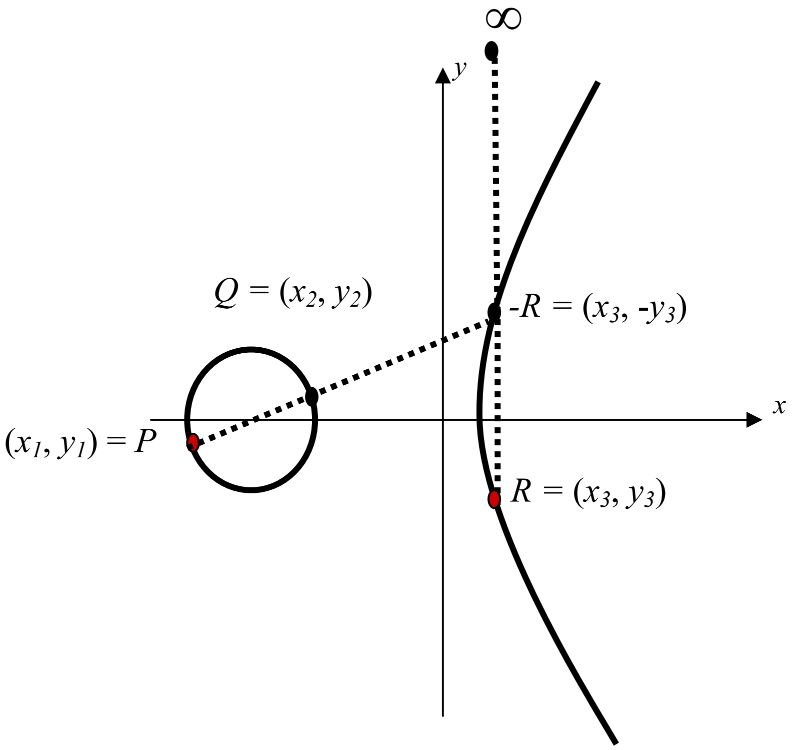


Figure 6.2 Chord-and-tangent rule $P + Q = R, P \neq Q$

To get the sum of two points on the curve follow the steps given below:

i) Draw a line that intersects distinct points P and Q

- The line will intersect a third point –R

ii) Draw a vertical line through point –R

- The line will intersect a fourth point R

iii) Point R is defined as the summation of points P and Q

- R = P + Q

6.1.2 Adding Points *P* and (–*P*) – Geometric Approach.

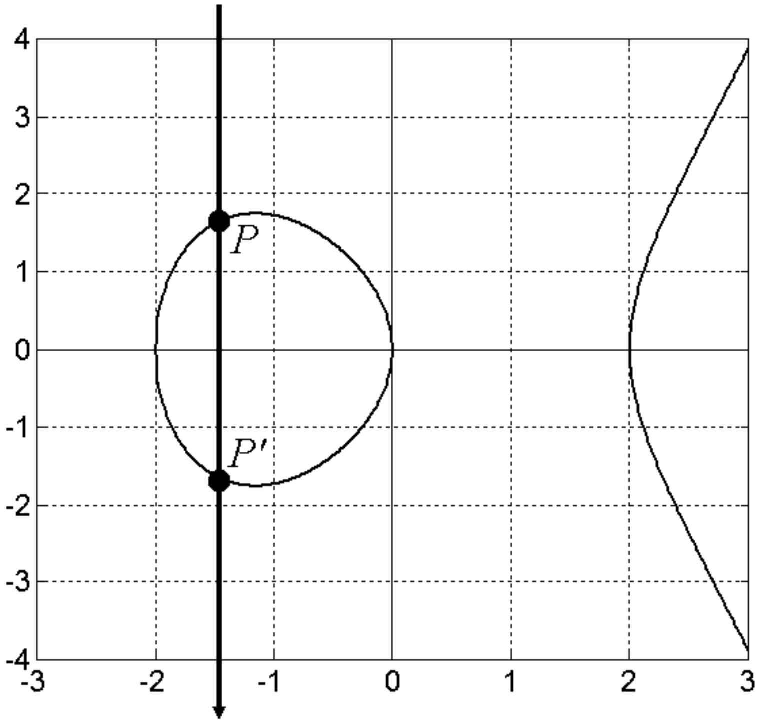


Figure 6.3 Sum of the points *P and* (-*P*)

To get the sum of the points *P* and (-*P*) follow the steps given below:

i) Draw a line that intersects points P and –P

- The line will not intersect a third point

ii) For this reason, elliptic curves include ∞, a point at infinity

- P + (-P) = ∞

- ∞ is the additive identity

6.1.3 Doubling the Point *P* – Geometric Approach

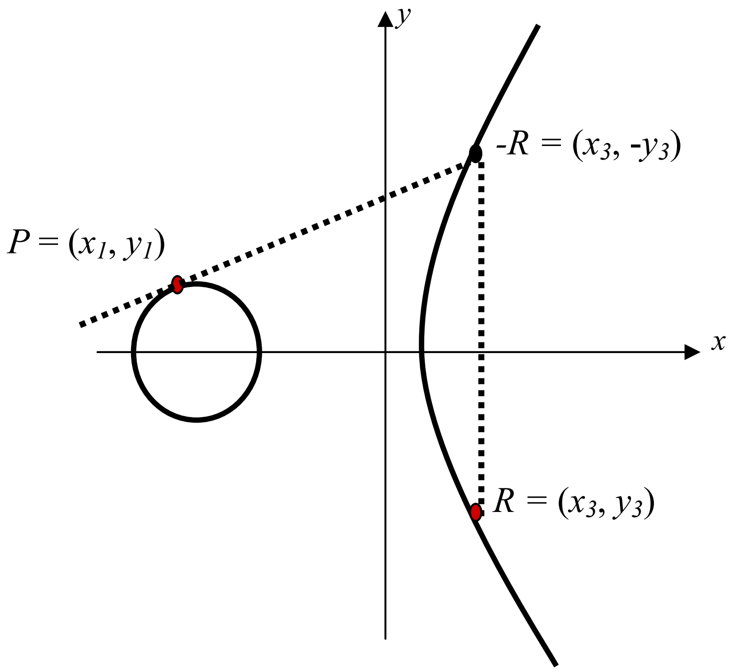


Figure 6.4 Point doubling $P + P = 2P = R$

i) Draw a line tangent to point P

- The line will intersect a second point -R

ii) Draw a vertical line through point –R

- The line will intersect a third point R

iii) Point R is defined as the summation of point P with itself

- R = 2·P

6.2 THE GROUP STRUCTURE OF ELLIPTIC CURVES

Let K be a field and let

$$E = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

where ∞ is an articial point added to the set of graph of equation which will play the role of zero element of the group.(Kendirli, 2006) The operation is defined as follows:

Case1. P and $Q \in E, P \neq Q, \quad P \neq \infty, \quad Q \neq \infty$ then

1) If $x_1 \neq x_2$, the line through $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ intersects the curve at a point $R' = (x_3, y_3)$ since

$$-((\frac{y_2 - y_1}{x_2 - x_1})(x - x_1) + y_1) + x^3 + ax + b = 0$$

has three roots, i.e.,

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

thus

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

$$y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_3 - x_1) + y_1$$

Define

$$P + Q = R \ ,$$

where $R = (x_3, -y_3)$ is the reflection of R' across the x-axis.

2) $x_1 = x_2 \Rightarrow y_2 = -y_1$. The line through $P = (x_1, y_1)$ and $Q = (x_1, -y_1)$ is a vertical line which intersects the curve at ∞, i.e.,

$$P + Q = \infty$$

Case 2. $P = Q = (x_1, y_1)$ then the slope of the tangent line at P can be calculated by implicit differentiation

$$2yy' = 3x^2 + a \Rightarrow m = \frac{3x_1^2 + a}{2y_1}$$

1) If $y_1 = 0$, then the line is vertical and intersects the curve at ∞, i.e.,

$$P + P = \infty$$

2) If $y_1 \neq 0$, then

$$-(m(x - x_1) + y_1)^2 + x^3 + ax + b = 0$$

has a double root at x_1 since the derivative of equation

$$-2(m(x - x_1) + y_1)m + 3x^2 + a = 0$$

has also x_1 as its root. Thus,

$$x_1 + x_1 + x_3 = m^2 \Rightarrow x_3 = m^2 - 2x_1$$

$$y_3 = m(x_3 - x_1) + y_1$$

Consequently ,

$$P + P = (m^2 - 2x_1, -(m(x_3 - x_1) + y_1))$$

Case 3. $Q = \infty$ then

1) If $P = (x_1, y_1) \neq \infty$, the line through P and Q is a vertical line which intersects the curve at

$$P' = (x_1, -y_1)$$

Whose reflection across the x-axis is P itself. Thus , $P + \infty = P$.

2)If $P = \infty$ then we define

$$\infty + \infty = \infty$$

Example6.2.1 $y^2 = x^3 - 4$ is an elliptic curve over $\mathbb{Q}$. If $P = (2,2)$ and $Q = (5,-11)$, then

$$x_3 = (\frac{-11-2}{5-2})^2 - 2 - 5 = \frac{106}{9}$$

$$y_3 = \frac{-13}{3}(\frac{106}{9} - 2) + 2 = \frac{-1090}{27}$$

Hence

$$P + Q = (\frac{106}{9}, \frac{1090}{27})$$

Theorem6.2.1 An elliptic curve is an Abelian group under the operation defined with the identity element ∞.

Note.(Point at infinity)(Koblitz, 1994) We have not yet said much about the "point at infinity" ∞. By definition, it is the identity of the group law. It is the "third point of intersection" of any vertical line with the curve; that is, such a line has points of intersection of the form $(x_1, y_1), (x_1, -y_1)$ and ∞. A more natural way to introduce the point ∞ is as follows.

By the *projective plane* we mean the set of equivalance classes of triples (x, y, z) (not all component zero) where two triples are said to be equivalent if they are a scalar multiple of one another, i.e., $(\lambda X, \lambda Y, \lambda Z) \sim (X, Y, Z)$. Such an equivalence class is called a *projectice point*.

If a projective point has nonzero Z, then there is one and only one triple in its equivalence class of the form $(x, y, 1)$: simply set $x = X/Z$, $y = Y/Z$. Thus the projectice plane can be identified with all points (x, y) of the ordinary plane plus the points for which $\mathrm{Z} = 0$. The latter points make up what is called the *line at infinity* roughly speaking, it can be visualized as the "horizon" on the plane. Any equation $F(x, y) = 0$ of a curve in the afine plane corresponds to an equation $\widetilde{F}(X, Y, Z) = 0$ satisfied by the corresponding projective points: simply replace $x \ by \ X/Z \ and \ y \ by \ Y/Z$ and multiply by a power of Z to clear denominators. For example, if we apply this procedure to the afine equation (1) of an elliptic curve, obtain its "projective equation" $Y^2Z = X^3 + aXZ^2 + bZ^3$. This latter equation is satisfied by all projective points (X,Y,Z) $with\ Z \neq 0$ for which the corresponding afine points (*x*,*y*), where $x = X/Z, y = Y/Z$, satisfy (1). In addition, what projective points (X,Y,Z) on the line at infinity satisfy the equation $\widetilde{F} = 0$? Setting $Z = 0$ in the equation leads to $0 = X^3$, i.e., $X = 0$. But the only equivalence class of triples (X,Y,Z) with both $X\ and\ Z$ zero is the class of $(0,1,0)$. This is the point we call ∞. It is the point on the intersection of the $y - axis$ with the line at infinity.

Definition6.2.1 The value $\Delta = 4a^3 + 27b^2$ is called the discriminant of the elliptic curve.

Corollary6.2.1 $4a^3 + 27b^2 \neq 0 \Leftrightarrow x^3 + ax + b = 0$ has three distinct roots.

After these now an elliptic curve can be expressed in the form below:

$$\{(x,y) \in F \times F : y^2 = x^3 + ax + b : 4a^3 + 27b^2 \neq 0\} \cup \{\infty\}$$

Example6.2.2 The curves defined by $y^2 = x^3$ and $y^2 = x^2(x+1)$ are not elliptic curves. Why.?

Because the polynomials on the right hand side have a multiple root. So from the perivous corollary, if the curve has multiple root then the discriminant is equal to 0, then the equation can not define an elliptic curve.

CHAPTER 7

ELLIPTIC CURVES OVER A FINITE FIELD

7.1 ELLIPTIC CURVES OVER A FINITE FIELD

Let F be a finite field and let E be an elliptic curve defined over F. Since there are only finitely many pairs (x, y) with $x, y \in F$, the group $E(F)$ is cyclic.

Example7.1.1 Let E be the curve $y^2 = x^3 + x + 1 \textit{ over } F_5$. To count points on E, we make a list of the possible values of x, then of $x^3 + x + 1 \pmod 5$, then of the square roots y of $x^3 + x + 1 \pmod 5$. This yields the points on E.

Table 7.1 Points of curve over F_5

x	$x^3 + x + 1$	y	*points*
0	1	± 1	$(0,1),(0,4)$
1	3	$-$	$-$
2	1	± 1	$(2,1),(2,4)$
3	1	± 1	$(3,1),(3,4)$
4	4	± 2	$(4,2),(4,3)$
∞		∞	∞

Therefore, $E(F_5)$ has order 9, i.e.,

$$E(F_5) = \{(0,1),(0,4),(2,1),(2,4),(3,1),(3,4),(4,2),(4,3)\} \cup \{\infty\}$$

We now show that this ia cyclic group. Take a random point as $P = (0,1)$. Let's calculate $2P$. Before, recall that;

$$P + Q = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \,,\ \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right)$$

$$P+P=((\frac{3x_1^2+a}{2y_1})^2-2x_1\ ,\ \frac{3x_1^2+a}{2y_1}(x_1-x_3)-y_1)$$

$P=(0,1)$ $\qquad$ $P+P=(0,1)+(0,1)=?$

$$P+P=((\frac{3.0^2+1}{2.1})^2-2.0\ ,\ (\frac{3.0^2+1}{2.1})(0-x_3)-1)$$

$$=(\frac{1}{4}-0\ ,\ \frac{1}{2}(0-\frac{1}{4})-1)$$

$$=(\frac{1}{4}\ ,\ -\frac{9}{8})=(4,2)$$

Now let's calculate $3P$;

$$3P=P+2P=(0,1)+(4,2)$$

$$=((\frac{2-1}{4-0})^2-0-4\ ,\ (\frac{2-1}{4-0})(0-x_3)-1)$$

$$=(\frac{1}{16}-4\ ,\ \frac{1}{4}(-\frac{1}{16}+4)-1)$$

$$=(-\frac{63}{16}\ ,\ -\frac{1}{64})$$

$$=(2,1)$$

Similarly, if you do the calculations you will get ;

$$4P=2P+2P=(3,1)$$

$$5P=3P+2P=(2,4)$$

$$6P=3P+3P=(4,3)$$

$$7P=P+6P=(0,4)$$

$$8P=P+7P=(3,4)$$

$$9P=P+8P=\infty$$

So order of $(0,1)$ is equal to 9. All 8 non-zero elements with ∞ form a cyclic group. $(0,1)$ is a generator of this group.

Table 7.2 Nonzero elements of the group over $y^2 = x^3 + x + 1 \bmod 5$

$P = (0,1)$	$5P = (2,4)$
$2P = (4,2)$	$6P = (4,3)$
$3P = (2,1)$	$7P = (0,4)$
$4P = (3,1)$	$8P = (3,4)$

Theorem7.1.1 Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0, then

$$E[n] \simeq Z_n \oplus Z_n$$

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

$$E[n] \simeq Z_{n'} \oplus Z_{n'} \quad \text{or} \quad Z_n \oplus Z_{n'}$$

Theorem7.1.2(Washington, 2003) Let E be an elliptic curve over the finite field F_q. Then

$$E(F_q) \simeq Z_n \qquad \text{or} \qquad Z_{n_1} \oplus Z_{n_2}$$

for some integer $n \geq 1$, for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

Proof. A basic result in number theory says that a finite Abelian group is isomorphic to a direct sum of cyclic groups

$$Z_{n_1} \oplus Z_{n_2} \oplus \dots\dots\dots \oplus Z_{n_r},$$

With $n_i \mid n_{i+1}$ for $i \geq 1$. Since, for each *i*, the group Z_{n_i} has n_1 elements of order dividing n_1, we find that $E(F_q)$ has n_1^r elements of order dividing n_1. By Theorem(7.1.2), there are at most n_1^2 such points (even if we allow coordinates in the algebraic closure of F_q). Therefore $r \leq 2$. This is the desired result.

7.1.1 Group Law of Elliptic Curves Over Finite Fields

Consider the set $E(F_p)$ over addition. We can see that;

$i)$ $\forall P,Q \in E(F_p)$, $if\ R \in E(F_p)$ $(Closure\ Property)$

$ii)$ $\forall P,Q,R \in E(F_p)$ then $P+(Q+R)=(P+Q)+R$ $(Associative\ Property)$

$iii)$ $\exists \infty \in E(F_p)$ $such\ that$ $\forall P \in E(F_p)$, $P+\infty=\infty+P=P$ $(Identity\ element)$

$iv)$ $\forall P \in E(F_p)$, $\exists\,(-P) \in E(F_p)$ $s.t$ $P+(-P)=(-P)=\infty$ $(Inverse\ element)$

$v)$ $\forall P,Q \in E(F_p)$, $P+Q=Q+P$ $(Commutative\ Property)$

Thus we see that $E(F_p)$ forms an *Abelian group* under addition.

Theorem7.1.3(Hasse)(Washington, 2003) Let E be an elliptic curve over the finite field F_q. Then the order of $E(F_q)$ satisfies

$$|\ q+1-\#E(F_q)\ |\le 2\sqrt{q}$$

7.2 FINDING THE TYPE OF THE GROUP

Example7.2.1 Let's find the type of the group when

$$y^2=x^3+5x+7$$

over Z_7.

First, determine whether the discriminant is different from 0 or not. Recall that;

$$\Delta=4a^3+27b^2$$

$$\Delta=4\times a^3+27b^2=4\times 5^3+27\times 7^2\equiv 3(\mathrm{mod}\,7)$$

Now we can use Hasse Theorem in order to estimate the number of elements in $E(\mathrm{Z}_7)$.

$$|\ 7+1-\#E(\mathrm{Z}_7)\ |\le 2\sqrt{7}\approx 5.2915$$

$$|\ 8-\#E(\mathrm{Z}_7)\ |\le 5 \quad \Rightarrow 3\le \#E(F_7)\le 13$$

On the other hand,

$(0,0)\in E(\mathrm{Z}_7)$ since $0^3+5\times 0+7\equiv 0(\mathrm{mod}\,7)$. By Maple, we can obtain all multiples of (0,0) in the following way.

> *multsell*([0,0],2,5,7,7);

```
[[1,[0,0],[2,["infinity” , “infinity”9]]
```

Now,

$(2,2)\in E(F_7)$

since $2^3+2\times 5+7\equiv 4(\mathrm{mod}\,7)$. By Maple

```
> multsell([2,2],4,5,7,7);
[[1,[2,2],[2,[4,0],[3,[2,5],[4,[“infinity” , “infinity”]].
```

Another point

$(3,0)\in E(Z_7)$

since $0^3+5\times 0+7\equiv 0(\mathrm{mod}\,7)$. By Maple

```
>multsell([3,0],4,5,7,7);
[[1,[3,0],[2,[“infinity” , “infinity”]],
[[3,[3,0],[4,[“infinity” , “infinity”]]
```

Another point

$(4,0)\in E(Z_7)$

since $4^3+5\times 4+7\equiv 0(\mathrm{mod}\,7)$. By Maple

```
> multsell([4,0],2,5,7,7);
[[1,[4,0],[2,[“infinity” , “infinity”]]
```

$(6,1)\in E(Z_7)$

since $6^3+5\times 6+7\equiv 1(\mathrm{mod}\,7)$. By Maple

```
> multsell([6,1],4,5,7,7);
[[1,[6,1],[2,[4,0],[3,[6,6],[4,[“infinity” , “infinity”]]
```

We have found 8 different elements so the order of group is 8. But non of these elements is the generator of the whole group so this group is not cyclic. Moreover, there is an element of order 4. Therefore,

$$E(Z_7)\cong Z_2 * Z_4$$

Example7.2.2 Find the type of the group when $y^2 = x^3 + 5x + 7$ over Z_{13}

$4a^3 + 27b^2 = \Delta = 4 \times 5^3 + 27 \times 7^2 \equiv 3(\mathrm{mod}13)$

Now we can use Hasse Theorem in order to estimate the number of elements in $E(Z_{13})$.

$$\left| 13 + 1 - \# E(Z_{13}) \right| \le 2\sqrt{13} \approx 7.2111$$

$$\left| 13 + 1 - \# E(Z_{13}) \right| \le 7$$

$$7 \le \# E(Z_{13}) \le 21$$

When $x = 0$ then y does not exist. You can see this procedure in Maple as below:

```
>legendre (7,13);
                 -1
```

$x = 1$ then $y = 0$

$(1,0) \in E(Z_{13})$

since $1^3 + 5 \times 1 + 7 \equiv 0(\mathrm{mod}13)$

Using Maple to determine the order of the point,

```
> multsell([1,0],21,5,7,13);

[[1, [1, 0]], [2, ["infinity", "infinity"]], [3, [1, 0]],
[4, ["infinity", "infinity"]], [5, [1, 0]], [6, ["infinity", "infinity"]],
[7, [1, 0]], [8, ["infinity", "infinity"]], [9, [1, 0]],
[10, ["infinity", "infinity"]], [11, [1, 0]],
[12, ["infinity", "infinity"]], [13, [1, 0]],
[14, ["infinity", "infinity"]], [15, [1, 0]],
[16, ["infinity", "infinity"]], [17, [1, 0]],
[18, ["infinity", "infinity"]], [19, [1, 0]],
[20, ["infinity", "infinity"]], [21, [1, 0]]]
```

When x=2 then y=5

$(2,5) \in E(Z_{13})$ since $2^3+5 \times 2+7 \equiv 12(\mathrm{mod}13)$

```
> multsell([2,5],21,5,7,13);
```

```
[[1, [2, 5]], [2, [5, 12]], [3, [10, 11]], [4, [4, 0]], [5, [10, 2]],
[6, [5, 1]], [7, [2, 8]], [8, ["infinity", "infinity"]], [9, [2, 5]],
[10, [5, 12]], [11, [10, 11]], [12, [4, 0]], [13, [10, 2]], [14, [5, 1]],
[15, [2, 8]], [16, ["infinity", "infinity"]], [17, [2, 5]], [18, [5, 12]],
[19, [10, 11]], [20, [4, 0]], [21, [10, 2]]]
```

Here we have found at least 9 different elements so the order of (2,5) which is 8 must divide the order of the group.But by Hasse theorem we know that the order of group is at most 21.So the order of the group is must be 16. Therefore,

$$E(Z_{13}) \cong Z_2 * Z_8$$

But here there is a critical point to investigate , what is it.? The question is this , why especially, $E(Z_{13})$ isomorphic to $Z_2 * Z_8$. Why not $E(Z_{13})$ isomorphic to Z_{16} or $Z_4 * Z_4$ or $Z_2 * Z_2 * Z_2 * Z_2$. They also have 16 elements as $Z_2 * Z_8$. The answer for this question can be this ;

We have an element having the order 8, so in $Z_4 * Z_4$ and in $Z_2 * Z_2 * Z_2 * Z_2$ there is no an element of order 8 , by the way we can immediately omit them. Only Z_{16} is left. Z_{16} has an element of order 8 and also an element of order 2 , but here the group which is generated by the point (1,0) is not contained by the group which is generated by the point (2,5). Thus

$$E(Z_{13}) \cong Z_2 * Z_8$$

CHAPTER 8

ELLIPTIC CURVE CRYPTOSYSTEMS OVER A FINITE FIELD

8.1 THE BASIC SETUP

Nikita wants to send a message, often called the plaintext, to Michael. In order to keep the eavesdropper Eve from reading the message, she encrypts it to obtain the ciphertext. When Michael receives the ciphertext, he decrypts it and reads the message. In order to encrypt the message. Nikita uses an encryption key. Michael uses a decryption key to ecrypt the ciphertext. Clearly, the decryption key must be kept secret from Eve.

There are two basic types of encryption. In symmetric encryption, the encryption key and decryption key are the same, or one can be easily deduced from the other. Ğoğular symmetric encryption methods include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES, often referred to by its original name Rijndeal). In this case, Nikita and Michael need to have some way of establishing a key. For example. Michael could send a messenger to Nikita several days in advance. Then, when it is time to send the message, they both will have the key. Clearly is impractical in many situations.

The other type of encryption is public key encryption, or asymmetric encryption. In this case, Nikita and Michael do not need to have prior contact. Michael publishes a public encryption key, which Nikita uses. He also has a private decryption key that allows him to decrypt ciphertexts. Since everyone knows the encryption key, it should be infeasible to deduce the decryption key from the encryption key. The most famous public key system is known as RSA and is based on the difficulty of factoring integers into primes. Another wellknown system is due to EIGamal and is based on the difficulty of the discrete logarithm problem.

Generally, public key systems are slower than good symmetric systems. Therefore, it is common to use a public key system to establish a key that is then used in a symmetric system. The improvement in speed is important when massive amounts of data are being transmitted.

8.1.1 Representation of a message in an elliptic curve

$$y^2 = x^3 + Ax + B$$

over a finite field F_{p^n}. Again, if we use an *N-letter* alphabet with $k-blocks$ such that

$$N^k < \frac{p^n - 1}{100}$$

then a $k-block$ is represented as an integer

$$\overline{P} = b_{k-1}N^{k-1} + b_{k-2}N^{k-2} + ... + b_1 N + b_0$$

in $\mathrm{Z}_{N^k} = \{0,1,2,...,N^k - 1\}$. Let

$$\overline{x_j} = \overline{P}.100 + j \qquad \text{for } 0 \le j < 100$$

Let $\overline{x_j} \equiv \overline{\overline{x_j}}(\mathrm{mod}\, p^n)$ and

$$\overline{\overline{x_j}} = b_{0,j} + b_{1,j}.p + b_{2,j}.p^2 + ... + b_{n-1,j}.p^{n-1}$$

So let

$$x_j = b_{0,j}.\alpha_0 + b_{1,j}.\alpha_1 + b_{2,j}.\alpha_2 + ... + b_{n-1,j}.\alpha_{n-1}$$

where

$$\{\alpha_0, \alpha_1, \alpha_2, ..., \alpha_{n-1}\}$$

İs a fixed vector space basis of F_{p^n} over $F_p = \mathrm{Z}_p$. For $j = 0,1,2,...,99$ compute

$$t_j = x_j^3 + Ax_j + B$$

in F_{p^n}. If we find a y_0 in F_{p^n} such that

$$y_0^2 = t_0$$

We take $P = (x_0, y_0)$. If not we look at y_1 for s_1 , i.e.,

$$y_1^2 = s_1$$

It is easy to see that there is only about a $\frac{1}{2^{100}}$ probability that this method will fail to produce a point P whose $x-coordinate$ corresponds to an integer between $m.100 + m.100 + 99$.

8.2 THE MASSEY-OMURA CRYPTOSYSTEM(For Elliptic Curves)

Nikita wants to sends a message to Michael over public channels. They have not yet established a private key. One way to do this is the following. Nikita puts her message in a box and puts her lock on it. She sends the box to Michael. Michael puts his lock on it and sends it back to Nikita. Nikita then takes her lock off and sends the box back to Michael. Michael then removes his lock, opens the box, and reads the message.

This procedure can be implemented mathematically as follows.

1. Nikita and Michael agree on an elliptic curve E over a finite field F_q such that the discrete log problem is hard in $E(F_q)$. Let $N = \# E(F_q)$.

2. Nikita represents her message as a point $M \in E(F_q)$. (We`ll discuss how to do this below)

3. Nikita chooses a secret integer m_A with $\gcd(m_a, N) = 1$, computes

$$M_1 = m_A M \text{ ,}$$

and sends M_1 to Michael.

4. Michael chooses a secret integer m_B with $\gcd(m_B, N) = 1$, computes

$$M_2 = m_B M_1 \text{,}$$

and sends M_2 to Nikita.

5. Nikita computes $m_A^{-1} \in Z_N$. She computes

$$M_3 = m_A^{-1} M_2$$

and sends M_3 to Michael.

6.Michael computes $m_B^{-1} \in Z_N$. He computes

$$M_4 = m_B^{-1} M_3 .$$

Then $M_4 = M$ is the message.

Let`s show that M_4 is the original message M. Formally, we have

$$M_4 = m_B^{-1} m_A^{-1} m_B m_A M = M\ ,$$

but we need to justify the fact that m_A^{-1}, which is an integer representing the inverse of m_A mod N, and m_A cancel each other. We have $m_A^{-1} m_A \equiv 1 (\text{mod}\ N)$, so $m_A^{-1} m_A = 1 + kN$ for some k. The group $E(F_q)$ has order N, so Lagrange`s theorem implies that $N\ R = \infty$ for any $R \in E(F_q)$. Therefore,

$$m_A^{-1} m_A R = (1 + kN)R = Rk\infty = R\ .$$

Applying this to $R = m_B M$, we find that

$$M_3 = m_A^{-1} m_B m_A M = m_B M\ .$$

Similarly, m_B^{-1} and m_B cancel, so

$$M_4 = m_B^{-1} M_3 = m_B^{-1} m_B M = M\ .$$

The eavesdropper Eve knows $E(F_q)$ and the points $m_A M, m_B m_A M$, and $m_B M$. Let $a = m_A^{-1}, b = m_B^{-1}, P = m_A m_B M$. Then we see that Eve knows P, bP, aP and wants to find abP. This is the Diffie-Hellman problem.

The above procedure works in any finite group. It seems that the method is rarely used in practice.

It remains to show to represent a message as a point on an elliptic curve. We use a method proposed by Koblitz. Suppose E is an elliptic curve given by $y^2 = x^3 + Ax + B$ over F_p. The case of an arbitrary finite field F_q is similar. Let m be a message, expressed as a number $0 \le m < p/100$. Let $x_j = 100_m + j$ for $0 \le j < 100$. For $j = 0,1,2,.....99$, compute $s_j = x_j^3 + Ax_j + B$. If $s_j^{(p-1)/2} \equiv 1\ (\text{mod}\ p)$, then s_j is a squre mod p, in which case we do not need to try any more values of j. When $p \equiv 3\ (\text{mod}\ 4)$, a squre root of s_j is then given by $y_j \equiv s_j^{(p+1)/4}\ (\text{mod}\ p)$. When $p \equiv 1\ (\text{mod} 4)$, a square root of s_j can also be computed, but the procedure is more complicated (see [19]). We obtain a point (x_j, y_j) on E. To recover m from (x_j, y_j), simply compute $[x_j/100]$ (= the greatest integer less than or equal to $x_{j/100)}$. Since

s_j is essentially a random element of F_p^x, which is cyclic of even order, the probability is approximately 1/2 that s_j is a square. So the probability of not being able to find a point for m after trying 100 values is around 2^{-100}.

Example8.2.1 Consider the elliptic curve E defined by

$$y^2 = x^3 + x + 1$$

over finite field F. We prepare the table below

i	b^i
1	$\alpha+2$
2	$\alpha^2+\alpha+1$
3	α^2+1
4	$\alpha+1$
5	α^2+2
6	2α
7	$2\alpha^2+\alpha$
8	$\alpha^2+2\alpha+1$
9	$2\alpha^2+2\alpha+1$
10	$2\alpha^2+2\alpha$
11	$2\alpha^2+\alpha+1$
12	α^2
13	2
14	$2\alpha+1$
15	$2\alpha^2+2\alpha+2$
16	$2\alpha^2+2$
17	$2\alpha+2$
18	$2\alpha^2+1$
19	α
20	$\alpha^2+2\alpha$
21	$2\alpha^2+\alpha+2$
22	$\alpha^2+\alpha+2$
23	$\alpha^2+\alpha$
24	$\alpha^2+2\alpha+2$
25	$2\alpha^2$
26	1

we prepare the following table

x	$y=\pm\sqrt{x^3+x+1}$	(x,y)
0	±1	(0,1),(0,2)
1	0	(1,0)
2	*None*	*none*
α	*None*	*none*
$1+\alpha$	$\pm(2\alpha^2+\alpha+1)$	$(1+\alpha,2\alpha^2+\alpha+1),(1+\alpha,\alpha^2+2\alpha+2)$
$\alpha+2$	$\pm(\alpha+2)$	$(\alpha+2,\alpha+2),(\alpha+2,2\alpha+1)$
2α	*None*	*none*
$2\alpha+1$	*None*	*none*
$2\alpha+2$	$\pm(\alpha^2+2)$	$(2\alpha+2,\alpha^2+2),(2\alpha+2,2\alpha^2+1)$
α^2	$\pm(2\alpha^2+\alpha)$	$(\alpha^2,2\alpha^2+\alpha),(\alpha^2,\alpha^2+2\alpha)$
α^2+1	$\pm(\alpha^2+1)$	$(\alpha^2+1,\alpha^2+1),(\alpha^2+1,2\alpha^2+2)$
α^2+2	*None*	*none*
$\alpha^2+\alpha$	$\pm\alpha$	$(\alpha^2+\alpha,\alpha),(\alpha^2+\alpha,\alpha)$
$\alpha^2+\alpha+1$	*None*	*none*
$\alpha^2+\alpha+2$	*None*	*none*
$\alpha^2+2\alpha$	*None*	*none*
$\alpha^2+2\alpha+1$	*None*	*none*
$\alpha^2+2\alpha+2$	*None*	*none*
$2\alpha^2$	$\pm(\alpha^2+\alpha+1)$	$(2\alpha^2,\alpha^2+\alpha+1),(2\alpha^2,2\alpha^2+2\alpha+2)$
$2\alpha^2+1$	*None*	*none*
$2\alpha^2+2$	*None*	*none*
$2\alpha^2+\alpha$	$\pm(2\alpha^2+2\alpha)$	$(2\alpha^2+\alpha,2\alpha^2+2\alpha),(2\alpha^2+\alpha,\alpha^2+\alpha)$
$2\alpha^2+\alpha+1$	$\pm(\alpha^2)$	$(2\alpha^2+\alpha+1,\alpha^2),(2\alpha^2+\alpha+1,2\alpha^2)$
$2\alpha^2+\alpha+2$	$\pm(\alpha+1)$	$(2\alpha^2+\alpha+2,\alpha+1),(2\alpha^2+\alpha+2,\alpha+1)$
$2\alpha^2+2\alpha$	$\pm(\alpha^2+2\alpha+1)$	$(2\alpha^2+2\alpha,\alpha^2+2\alpha+1),(2\alpha^2+2\alpha,2\alpha^2+\alpha+2)$
$2\alpha^2+2\alpha+1$	$\pm(2\alpha^2+2\alpha+1,2\alpha^2+2\alpha+1)$	$(2\alpha^2+2\alpha+1,\alpha^2+\alpha+2)$
$2\alpha^2+2\alpha+2$	*None*	*none*

since

$$b^{13} = 2$$

2 doesn't have a square root, since

$$(\alpha+2)^3+(\alpha+2)+1=\alpha^2+\alpha+1=b^2$$

its square root is $b = \alpha + 2, \ldots$

Now, the number of elements in $E(F_{3^3})$ is $N = 28$. Suppose that Alice chooses $e_A = 5$ it is correct since $\gcd(28,5) = 1$. Its arithmetic inverse $d_A = 17$ .Alice sends plaintext

"*go*"

to Bob as

$$5((2 + 2\alpha), (\alpha^2 + 2)), 5((2 + \alpha + 2\alpha^2), (\alpha + 1))$$

$$(1 + \alpha, 2\alpha^2 + 1), (\alpha^2 + 2\alpha + 1, 2\alpha + 2)$$

since

$$g \to 6 \to \overline{x_0} = 600 \equiv 6(\mathrm{mod}\, 27) \to \overline{\overline{x_0}} = 6 = 0.1 + 2.3 \to x_0 = 2\alpha \to$$

$$s_0 = (2\alpha)^3 + 2\alpha + 1 = 2\alpha^2 + 2\alpha + 2 = b^{15}$$

which doesn`t have a square root. So,

$$\overline{x_1} = 601 \equiv 7(\mathrm{mod}\, 27) \to \overline{\overline{x_1}} = 7 = 1.1 + 2.3 \to x_1 = 1 + 2\alpha$$

$$s_1 = (1 + 2\alpha)^3 + (1 + 2\alpha) + 1 = 2\alpha^2 + 2\alpha + 1 = b^9$$

which doesn`t have a square root. Next,

$$\overline{x_2} = 602 \equiv 8(\mathrm{mod}\, 27) \to \overline{\overline{x_2}} = 8 = 2.1 + 2.3 \to x_2 = 2 + 2\alpha$$

$$s_2 = (2 + 2\alpha)^3 + (2 + 2\alpha) + 1 = 2\alpha^2 + 2\alpha = b^{10} \Rightarrow y_2 = b^5 = \alpha^2 + 2.$$

Thus, "g" will be represented by

$$(2 + 2\alpha, \alpha^2 + 2)$$

on the elliptic curve E. Now let`s look at "*o*" :

$$o \to 14 \to \overline{x_0} = 1400 \equiv 23(\mathrm{mod}\, 27) \to \overline{x_0} = 23 = 2.1 + 1.3 + 2.3^2 \to$$

$$x_0 = 2 + \alpha + 2\alpha^2. \to s_0 = x_0^3 + x_0 + 1 = \alpha^2 + 2\alpha + 1 = b^8 \Rightarrow y_0 = b^4 = \alpha + 1.$$

Thus "*o*" will be represented by

$$(2 + \alpha + 2\alpha^2, \alpha + 1).$$

So, “go” is represented by

$$(2 + 2\alpha ,\alpha ^2 + 2),\ (2\alpha ^2 + \alpha + 2,\alpha + 1).$$

Now, Alice will compute

$$5(2 + 2\alpha,\alpha^2 + 2), 5(2\alpha^2 + \alpha + 2,\alpha + 1).$$

$$5\,(2 + 2\alpha,\alpha^2 + 2) = 5(b^{17},b^5):$$

$$(2 + 2\alpha,\alpha^2 + 2)\ +\ (2 + 2\alpha,\alpha^2 + 2)$$

Since

$$m = \frac{3(2 + 2\alpha)^2 + 1}{2(\alpha^2 + 2)} = \frac{1}{2\alpha^2 + 1} = \frac{1}{b^{18}} = b^8 = \alpha^2 + 2\alpha + 1$$

the sum is

$$(b^{16} - 2b^{17}, b^8(b^{17} - b^{16} + 2b^{17}) - b^5) = (b^{16}(1 + b), - b^{24} - b^5).$$

So,

$$(b^{17}, b^5) + (b^{17}, b^{5)} = (b^{16}b^{19}, b^{21}) = (b^9, b^{21}).$$

$$(b^9\ ,b^{21}) + (b^9,b^{21}) = (b^2,b^{19})$$

Since the slope

$$m = \frac{1}{2.b^{21}} = \frac{1}{b^{13}b^{21}} = \frac{1}{b^8} = b^{18}$$

and

$$x_3 = m^2 - 2x_1 = b^{36} - 2b^9\ = b^{10}\ + b^9\ = b^9\ (1 +) = b^9b^{19}\ = b^2,$$

$y_3 = m(x_1 - x_3) - y_1\ = b^{18}(b^9\ - b^2) - b^{21}\ = b - b^{20}(1 + b) = b - b^{20+19}\ = b - b^{13}\ = \alpha = b^{19}.$

So, it remains to calculate

$$(b^{17},b^5) + (b^2,b^9).$$

The slope

$$m = \frac{b^9\ - b^5}{b^2\ b^{17}} = \frac{2\alpha^2 + 2\alpha + 1 - \alpha^2 - 2}{\alpha^2 + \alpha + 1 - 2\alpha - 2} = \frac{\alpha^2 + 2\alpha + 2}{\alpha^2 + 2\alpha + 2} = 1.$$

$$x_3 = m^2 - x_1 - x_2\ = 1 - b^{17} - b^2\ = 1 - 2\alpha - 2 - \alpha^2 - \alpha - 1 = 2\alpha^2 + 1 = b^{18}$$

$$y_3 = b^{17} - b^{18} - b^5\ = 2\alpha + 2 = b^{17}.$$

So, the ciphertext for "g" is

$$(2\alpha^2 + 1 = b^{18}, 2\alpha + 2 = b^{17}).$$

Now, let`s look at

$$"o" = (2\alpha^2 + \alpha + 2 = b^{21}, \alpha + 1 = b^4):$$

$$m = \frac{1}{2.(\alpha + 1)} = \frac{1}{2\alpha + 2} = \frac{1}{b^{17}} = b^9.$$

Thus,

$$x_3 = m^2 - 2x_1 = b^{18} - 2b^{21} = b^{18} - b^{13+21} = b^{18} - b^8 = \alpha^2 + \alpha = b^{23}$$

and

$$y^3 = m(x_1 - x_3) - y_1 = b^9(b^{21} - b^{23}) - b^4 = b^4 - b^6 - b^4 = -2\alpha = \alpha = b^{19}.$$

Therefore,

$$(2\alpha^2 + \alpha + 2 = b^{21}.\alpha + 1 = b^4) + (2\alpha^2 + \alpha + 2 = b^{21}, \alpha + 1 = b^4) = (b^{23}, b^{19}).$$

Now.

$$(b^{23}, b^{19}) + (b^{23}, b^{19}):$$

since

$$m = \frac{1}{2b^{19}} = \frac{1}{b^{32}} = \frac{1}{b^6} = b^{20},$$

we have

$$x_3 = m^2 - 2x_1 = b^{40} - 2b^{23} = b^{14} - b^{10} = \alpha^2 + 1 = b^3$$

and

$$y_3 = m(x_1 - x_3) - y_1 = b^{20}(b^{23} - b^3) - b^{19} = b^{17} - b^{23} - b^{19} = 2\alpha^2 + 2 = b^{16}.$$

Let`s look at

$$(2\alpha^2 + \alpha + 2 = b^{21}, \alpha + 1 = b^4) + (b^3, b^{16}):$$

The slope

$$m = \frac{b^{16} - b^4}{b^3 - b^{21}} = \frac{b^9}{b^{15}} = b^{20}.$$

$$x_3 = m^2 - x_1 - x_2 = b^{40} - b^{21} - b^3 = b^{14} - b^{21} - b^3 = \alpha + 1 = b^4,$$

$$y_3 = m(x_1 - x_3) - y_1 = b^{20}(b^{21} - b^4) - b^4 = b^{15} - b^{24} - b^4 = \alpha^2 + 2\alpha + 2 = b^{24}.$$

So, the ciphertext for "o" is

$$5(2\alpha^2+\alpha+2=b^{21},\alpha+1=b^4)=(\alpha+1=b^4,\alpha^2+2\alpha+2=b^{24}).$$

Consequently Bob receives cipherteext

$$(2\alpha^2+1=b^{18},2\alpha+2=b^{17}),(\alpha+1=b^4,\alpha^2+2\alpha+2=b^{24}).$$

Then Bob calculates in the same way the expression

$$3(b^{18},b^{17}),3(b^4,b^{24})$$

and send it to Alice. She then calculates

$$17(3(b^{18},b^{17})),17(3(b^4,b^{24}))$$

and sends it to Bob. Then Bob can see the orginal plaintext by calculating

$$19(17(3(b^{18},b^{17}))),19(17(3(b^4,b^{24}))).$$

8.3 THE ELGAMAL CRYPTOSYSTEM(For Elliptic Curves)

Nikita wants to send a message to Michael. First, Michael establishes his public key as follows. He chooses an elliptic curve E over a finite field F_q such that the discrete log problem is hard for $E(F_q)$. He also chooses a point P on E (usually, it is arranged that the order of P is a large prime). He chooses a secret integer s and computes $B=sP$. The elliptic curve E, the finite field F_q, and the points P and B are Michael`s public key. They are made public. Michael`s private key is the integer s.

To send a message to Michael, Nikita does the following:

1. Downloads Michael`s public key.
2. Expresses her message as a point $M \in E(F_q)$.
3. chooses a secret random integer k and computes $M_1 = kP$.
4. Computes $M_2 = M + kB$.
5. sends M_1, M_2 to Michael.

Michael decrypts by calculating

$$M = M_2 - sM_1.$$

This decryption works because

$$M_2 - sM_1 = (M+kB) - s(kP) = M + k(sP) - skP = M.$$

The eavesdropper Eve knows Michael`s public information and the points M_1 and M_2. If she can calculate discrete logs, she can use P and B to find s, which she can then use to decrypt the message as $M_2 - sM_1$. Also, she could use P and M_1 to find k. Then she can calculate $M = M_2 - kB$. If she cannot calculate discrete logs, there does not appear to be a way to find M.

It is important for Nikita to use a different random k each time she sends a message to Nikita. Suppose Nikita uses the same k for both M and M'. Eve recognizes this because then $M_1 = M_1'$. She she then computes $M_2' - M_2 = M' - M$. Suppose M is a sales announcement that is made public a day later. Then Eve finds out M, sos he calculates $M' = M - M_2 + M_2'$. Therefore, knowledge of one plaintext M allows Eve to deduce another plaintext M' in this case.

Example8.3.1 Consider the Example(8.2.1). Let

$$O = (\alpha, \alpha^2 + \alpha).$$

Suppose that Bob chooses $a = 4$ .Then $4O$ is public key. Let`s calculate it:

$$(\alpha, \alpha^2 + \alpha) + (\alpha, \alpha^2 + \alpha) = (0, \alpha^2 + \alpha + 1 = b^2)$$

since $$m = \frac{1}{2(\alpha^2 + \alpha)} = \frac{1}{b^{13} b^{23}} = \frac{1}{b^{10}} = b^{16},$$

$$x_3 = b^{32} - 2\alpha = b^6 - 2\alpha = 0$$

$$y_3 = b^{16}(\alpha - 0) - \alpha^2 - \alpha = b^{16} b^{19} - \alpha^2 - \alpha = \alpha^2 + \alpha + 1 = b^2.$$

Moreover,

$$(0, b^2) + (0, b^2) = (b^{22}, 2)$$

since $$m = \frac{1}{2b^2} = \frac{1}{b^{15}} = b^{11},$$

$$x_3 = b^{22} - 2.0 = \alpha^2 + \alpha + 2 = b^{22}$$

$$y_3 = b^{11}(0 - b^{22}) - b^2 = \alpha^2 + \alpha - \alpha^2 - \alpha - 1 = 2.$$

Therefore

$$4O = (b^{22}, 2).$$

Suppose that Alice chooses $k = 2$.

$$2O = (0, b^2)$$

to Bob as

$$((0,b^2),(P+(4O+4O)))=((0,b^2),(b^{14},b^8)).$$

Since $m=\frac{1}{2.2}=\frac{1}{1}=1,$

$$x_3 1-2.b^{22}=1-b^9=\alpha^2+\alpha=b^{23}$$

$$y_3=1(b^{22}-b^{23})-2=0,$$

$$4O+4O=(\alpha^2+\alpha=b^{23},0).$$

Now, we need to calculate

$$(P+(4O+4O))=(2+2\alpha=b^{17},\alpha^2+2=b^5)+(b^{23},0)$$

since "g" is represented by

$$(2+2\alpha=b^{17},\alpha^2+2=b^5).$$

$$m=\frac{0-b^5}{b^{23}-b^{17}}=\frac{b^{18}}{b^8}=b^{10}\Rightarrow$$

$$x_3=b^{20}-b^{17}-b^{23}=2\alpha+1=b^{14},$$

$$y_3=b^{10}(b^{17}-b^{14})-b^5=\alpha^2+2\alpha+1=b^8.$$

Now, we calculate similiarly for "o":

$$(P+(4O+4O))=(2+\alpha+2\alpha^2=b^{21},\alpha+1=b^4)+(b^{23},0):$$

The slope $m=\frac{0-b^4}{b^{23}-b^{21}}=\frac{b^{17}}{b^{18}}=b^{25}$. Thus,

$$x_3=b^{50}-b^{21}-b^{23}=0,$$

$$y_3=b^{25}(b^{21}-0)-b^4=\alpha^2+\alpha+2=b^{22}$$

Thus, Bob receives ciphertext as

$$((0,b^2),(b^{14},b^8)),((0,b^2),(0,b^{22})).$$

8.4 THE DIFFIE-HELLMAN KEY EXCHANGE SYSTEM

Nikita and Michael want to agree on a common key that they can us efor exchanging data via a symmetric encryption scheme such as DES(Data Encryption Standard) or AES(Advanced Encryption Standard). For example, Nikita and Michael could be banks that want to transmit financial data. It is impractical and time-consuming to use a courier to deliver the key. Moreover, we assume that Nikita and Michael have had no prior contact and therefore the only communication channels between them are public. One way to eatablish a secret key is the following method, due to Diffie and Hellman (actually, they used multiplicative groups of finite fields).

1. Nikita and Michael agree on an elliptic curve E over a finite field F_q such that the discrete logarithm problem is hard in $E(F_q)$. They also agree on a point $p \in E(F_g)$ such that the subgroup generated by P has large order (usually, the curve and point are chosen so that the order is a large prime).

2. Nikita chooses a secret integer a, computes

$$P_a = aP,$$

and sends P_a to Michael.

3. Michael chooses a secret integer b, computes

$$P_b = bP,$$

and sends P_b to Nikita.

4. Nikita computes

$$aP_b = abP\ .$$

5. Michael computes

$$bP_a = baP\ .$$

6. Nikita and Michael use some publicly agreed on method to extract a key from abP. For example, they could use the the last 256 bits of the x-coordinate of abP as the key. Or they could evaluate a hash function at the x-coordinate.

Example8.4.1 Consider the elliptic curve E defined by

$$y^2 = x^3 + x + 1$$

over finite field F_{3^3}. Assume that

$$O = (\alpha, \alpha^2 + \alpha)$$

as in the previous example. Let the key of Alice be $a = 2$, and the key of Bob be $b = 4$. Then

$$abO = 8O = (\alpha + \alpha^2 = b^{23}\ , 0)$$

which was calculated in the previous example(Example 8.3.1). Therefore we can take the enciphering transformation as

$$C \equiv P + 1(\mathrm{mod}\, N)$$

where the message units are single letters in the $29-letter\ alphabet$ with $A-Z$ corresponding to 27 , $? = 28$. Therefore, Alice sends plaintext

Addition of infinity is essentially **the projective completion** of the afine curve as a ciphertext

$$beejujpo.pg.jogjojuz.jt.fttfoujbmmz.uif.qspk$$

$$fdujwf.dpnqmfujpo.ps.uif.bggjof.dvswf$$

to Bob.

CHAPTER 9

CONCLUSIONS

As a branch of mathematics, abstract algebra shares an important topic with number theory which is called finite fields.

Finite fields have many applications in many branches of mathematics especially in number theory. In this thesis, we studied elliptic curves over a finite field with cryptographic applications. We see that defining an elliptic curve over a finite field offers us more security. Namely, let's define an elliptic curve over Z_p (where p is a prime number). When you choose p as a large prime then it means that the ciphertext becomes so hard to crack.

On the other hand, when we compare elliptic curve cryptosystem with the others such as RSA, Diffie – Hellman Key Exchange and ElGamal cryptosystem, we have some practical advantages of elliptic curve cryptosystem as mentioned below.

i) Faster then the other systems

ii) Low power consumption

iii) Low memory usage

iv) Low CPU utilization

For example, it is estimated that a key size of 4096 bits for RSA gives the same level of security as 313 bits in an elliptic curve system. This means that implementations of elliptic curve cryptosystems require smaller chip size, less power consumption.

As a consequence, the study of elliptic curves includes much beautiful and deep number theory. Until recently this study was almost exclusively the province of pure mathematicians. Now elliptic curves can claim their place as one of the important subjects in the study of cryptography. Not only are they useful theoretically but are already having great practical impact.

REFERENCES

Anderson, J. A., *Number Theory with Applications*, Prentice Hall, New Jersey, 1997.

Balkanay, E. and G. Ağargün, *Soyut Cebir II*, Yıldız Teknik Üniversitesi Basım-Yayın Merkezi, İstanbul, 2002.

Bozkurt, D., *Soyut Cebire Giriş*, Selçuk Üniversitesi Basımevi, Konya, 2001.

Burton, D. M., *Elementary Number Theory*, McGrawHill, Boston, 2002.

Cassels, J.W.S., *Lectures on Elliptic Curves*, Cambridge University Press, New York, 1995.

Çallıalp, F., *Sayılar Teorisi*, Marmara Üniversitesi, İstanbul, 1999.

Çallıalp, F., *Soyut Cebir*, İstanbul Teknik Üniversitesi, İstanbul, 2001.

Dummit, D. S. and R. M. Foote, *Abstract Algebra*, Prentice – Hall, New Jersey, 1999.

Enge, A., *Elliptic Curves and Their Applications to Cryptography An Introduction*, Kluwer Academic Publishers, Boston, 1999

Fraleigh, J. B., *A First Course in Abstract Algebra*, Addison Wesley, New York, 2003.

Gallian, J. A., *Contemporary Abstract Algebra*, D.C.Heath, Massachusetts, 1994.

Hardy, G. H. and E. M. Wright, *An Introduction to The Theory of Numbers*, Clarendon Pres, New York, 1979.

Herstein, I. N., *Abstract Algebra*, Prentice – Hall, New Jersey, 1996.

Hungerford, T. W., *Abstract Algebra*, Saunders College Pub., Philadelphia, 1990.

Husemöller, D., *Elliptic Curves*, Springer – Verlag, New York, 2004.

Ireland, K. F., *A Classical Introduction to Modern Number Theory*, Springer – Verlag, New York 1990.

Janusz, G. J., *Algebraic Number Fields*, American Mathematical Society, 1996.

Jones, G. A. and J.M. Jones, *Elementary Number Theory*, Springer, New York, 1999.

Judson, T. W., *Abstract Algebra: Theory and Applications*, Pws Pub. Boston, 1994.

Kato, K., *Number Theory 1*, American Mathematical Society, Rhode Island, 1999.

Kendirli, B., *Number Theory with Cryptographic Applications*, Fatih University, Istanbul, 2005.

Knapp, A. W., *Elliptic Curves*, New Jersey, Princeton University Press, 1992.

Koblitz, N., *Introduction To Elliptic Curves and Modular Forms*, Springer – Verlag, New York, 1993.

Koblitz, N., *A Course in Number Theory and Cryptography*, Springer – Verlag, New York, 1994.

Lang, S., *Algebra*, Addison – Wesley, Massachusetts, 1993.

Lang, S., *Algebraic Number Theory*, Springer – Verlag, New York, 1994.

Lidl, R. and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Pres, 1994.

Mollin, R. A., *Algebraic Number Theory*, Chapman & Hall/CRC, Boca Raton, 1999.

Mollin, R. A., *An Introduction to Cryptography*, Chapman&Hall, Boca Raton, 2001.

Mollin, R. A., *Fundamental Number Theory with Applications*, CRC Pres, Boca Raton, 1998.

Niven, I. and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.

Rose, H. E., *A Course in Number Theory*, Clarendon Press, Oxford, 1995.

Rosen, K. H., *Elementary Number Theory and its Applications*, Addison-Wesley, Massachusetts, 2000.

Rotman, J. J., *A First Course in Abstract Algebra*, Prentice – Hall, New Jersey, 2000.

Saracino, D., *Abstract Algebra A First Course*, Addison – Wesley, Massachusetts,1980.

Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer -Verlag, New York, 1986.

Silverman, J. H. and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

Silverman, J. H., *A Friendly Introduction to Number Theory*, Prentice Hall, New Jersey, 1997.

Stinson, D.R., *Cryptography: Theory and Practice*, Crc Press, Boca Raton, 1995.

Washington, L. C., *Elliptic Curves Number Theory and Cryptography*, Chapman & Hall/CRC, Boca Raton, 2003.