University of Belgrade

Faculty of Mathematics

Master thesis:

Finite fields and their applications

Student:

Sana Mohamad Abdulwanis Mohamad

Professor:

Žarko Mijajlović

Belgrade, 2013.

Acknowledgement

I would like to thank to all those who contributed to the successful completion of this thesis.

I particularly express gratitude to my supervisor professor Zarko for his advice, assistance and patience.

And I would like to thank my English teacher Dunja.

I am extremely grateful to my family and friends for their patience and support.

Dedication

I dedicate this work to my parents, who gave me the opportunity and necessary strength for accomplishing my studies and now my master thesis.

I dedicate this work to my husband Adel, and I am very grateful to him for his enormous support, patience and understanding during my studies.

Also, I dedicate this work to my lovely daughters Janat and Joumana.

Table of contents

Chapter I: RINGS AND FIELDS

Chapter II : IRREDUCIBLE POLYNOMIAL AND EXTENSION AS VECTOR SPACE

Chapter III : ELLIPTIC CURVE CRYPTOGRAPHY

Abstract

The aim of this thesis is to study the finite field and their application.

We introduced, as a background for this subject, the finite field and structure of finite field, and polynomials over an algebraic structure.

We also introduced the field extension as vector spaces.

We also studied some applications, such as for example Elliptic curve cryptography.

In this chapter, we studied group constructed using points on an Elliptic curve.

History of Finite fields

The origins of finite fields are from the 17^{th} and 18^{th} centuries. The first steps were done by:

- Fermat (1601-1665),
- Euler (1707-1783),
- Lagrange (1736-1813) and
- Legendre (1752-1833).

All of them for some special fields: F_p where p is a prime. We will see that there are other type of finite fields. The elements in this field can be seen as integers modulo p.
The theory of finite fields as we know it today was constructed at the end of the 18^{th} century and during 19^{th} century.
The main researchers of the area are

- Carl Friedrich Gauss (1777-1855), and
- Évariste Galois (1811-1832).

Gauss worked on problems in finite fields (possibly) around 1797-1798, at the time when was working on his famous Disquistiones Arithmeticae (1801). We will see his work related with the factorization of polynomials over finite fields. Unfortunately, Gauss never published his work. They became public only after his dead (1889).
The other giant, Galois, lived a very short life, but a very interesting one. His paper " Sur la theorie des nombres" marks the beginning of finite fields, or Galois fields; see, the complete works of Galois compiled by Liouville in 1846.
The next big step in the construction of finite fields was provided by Richard Dedekind on 1857.
He characterized the finite fields of order p^n as residue class rings
$F_p\,[x]/(f)$
Where f is an irreducible polynomial of degree n over F_p.
Also introduced the Mobius inversion formula in finite fields to study the number of irreducible polynomials of certain degree.
Finally, Eliakim H. Moore in 1893 proved that finite fields must have p^n elements, where p is a prime.

Chapter I - Rings and Fields

1.1 Rings and fields

One day our ancient shepherd settled down and became a farmer. He needed to figure out with his neighbors the areas of their lands. The shepherds – turned – farmers began to realize that it was no longer possible for them to use one basic operations for everything: they needed not only sum, but also product. The need for two operations over a set of objects started then.

1.1.1 Definition:

A ring R is a set together with two operations:

(addition) + and (multiplication), and has the following properties:

1. Under addition $(+)$, R is an abelian group, denote by 0 the additive identity (called the zero-element).
2. Under multiplication, R satisfies closure Axiom, Associativity axiom, and identity axiom, and identity axiom, denote by 1 the multiplicative identity (called the unity – element) $1 \neq 0$
3. $\forall\, a, b \in R; a \cdot b = b \cdot a$ (commutative Axiom)
4. $\forall\, a, b, c \in R; a \cdot (b + c) = a \cdot b + a \cdot c$ (Distribution Axiom)

1.1.2 Definition:

If the non-zero elements of ring forms a group under multiplication, then the ring is called a field.

The closure axiom for the multiplicative group

(i.e., the non-zero elements of a field implies that a field F can not contain a zero-divisor, that is, for any $a, b \in F, ab = 0$ implies either $a = 0$ or $b = 0$.

If the number of elements in F is finite, we call F a finite field and denote it F_n, where n is the number of elements in F.

1.1.1 Example:

1. A simple example of a field and more important is the finite field F_2, the elements of this field of order two are 0 and 1 and the operation tables have the following form:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

In this context, the elements (0)and (1)are called binary elements.

2. $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields under usual addition with natural elements 0 and 1 for multiplication.
3. For p being a prime number, Z_p a field under addition with natural elements 0 and 1 with multiplication modulo p.

Note that:
Z under integer addition and multiplication is not a field because any non zero element does not have a multiplicative inverse in Z, also for being a composite, Z_n is not a field too since we have seen that Z_n contains zero-divisors.

1.1.1 Theorem:
Every finite integral domain is a field.

Proof:
Let the elements of finite integral be a_1 , a_2 ...,a_n for (a) fixed nonzero element $a \in R$ consider the products:
$aa_1, aa_2, \ldots, aa_n$ these are distinct for if $aa_i = aa_j$
then $a(a_i - a_j) = 0$,
and since $a \neq 0$ we must have $a_i - a_j = 0$ or $a_i = a_j$ thus each element of R is the form aa_i,
(n) particular $e = aa_i$,
for some i with $1 \leq i \leq n$ where (e) is identity of R
since R commutative
we have also $a_i \; a = e$ and so a_i is the multiplicative inverse of a, thus the non zero elements of R form (a) commutative group and R is field.

1.1.3 Definition:
An algebraic structure is said to be finite if it contains a finite number of elements.
The number of elements is called the order of the structure.
A substructure of an algebraic structure A is non-empty subset S of A which is itself an algebraic structure under the operation (S) of A. If $S \neq A$ then S is called a proper substructure of A.
Let A be an algebraic structure and $B \subseteq A$ be a substructure of A. The quotient structure of A modulo B, denoted by A/B is the set of all cosets $a \circ B$ with oranging over A, with the operation $*$ defined by
$(a \circ B) * (b \circ B) = (a \circ b) \circ B$, and with the identity elements being $0 \circ B$ and $1 \circ B$.

1.2The structure of finite fields

1.2.1 Finite fields of prime numbers of elements

Finite field with the simplest structure are those of orders (i.e. the number of elements) as prime numbers. Yet, such fields have been the most widely used ones in cryptography.

1.2.4 Definition:
Prime field: A field that contains no proper subfield is called a prime field.
For example: $\mathbb{Q}$ is a prime field where R is not, since $\mathbb{Q}$ is a proper subfield of R, but $\mathbb{Q}$ is an infinite field.

1.2.1 Lemma:
If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.

Proof:
Clearly $a^q = a$ is satisfied for $a = 0$, the non-zero elements form a group of order $q - 1$ under multiplication using the fact that $a^{|G|} = 1_G$ for any element of finite group G, we have that all $0 \neq a \in F$ satisfy $a^{q-1} = 1$
i.e. $a^q = a$.

1.2.5 Definition: Homomorphism and Isomorphism

Let A, B be two algebraic structures. A mapping $f: A \longmapsto B$ is called a homomorphism of A in to B if f preserves operations of A. That is, if $\circ$ is an operation of A and $*$, an operation of B, then $\forall\, x, y \in A$, we have $f(x \circ y) = f(x) * f(y)$.
If F is a one-to-one homomorphism of A onto B, then f is called an isomorphism and we say that A and B are isomorphic.
If $f: A \longmapsto B$ is homomorphism and e is an identity element in A (either additive or multiplicative), then
$f(e) * f(e) = f(e \circ e) = f(e)$
so that $f(e)$ is the identity element in B, also for any $a \in A$
$f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e)$

1.2.6 Definition:

For a prime p, let F_p be the set $\{0,1, \ldots, p-1\}$ of integers, and let $\emptyset: {}^{Z}/_{p} \to F_p$ be the mapping defined by $\emptyset([a])=a$ for $a = 0,1, \ldots, p-1$, then F_p endowed with the field structure induced by $\emptyset$ is a finite field, called the Galois field of order p.

1.2.2 Example:

We have $\frac{z}{(5)}$ isomorphic to F_5={0,1,2,3,4} where the isomorphism is given by$[0] \to 0$, $[1] \to 1$, $[2] \to 2$,…$[4] \to 4$.

The operation tables are:

+	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	1

1.2.7 Definition of Prime subfield:

The prime subfield of a field F is the subfield of F generated by the multiplicative identity 1_f of F. It is isomorphic to either Q (if the field characteristic is 0) or the finite field $F_p = {}^{Z}/_{pZ}$ (if the field characteristic p).

1.2.8 Definition: Characteristic of a rings:

If R is an arbitrary ring and there exists a positive integer n such that $nr = 0$ for every $r \in R$, then the least such positive integer n is called the characteristic of R and R is said to have (positive) characteristic n.

If no such positive integer n exists, R is said to have the characteristic 0.

1.2.3 Example:

1. The rings Z, Q, R and C have characteristic zero
2. In the ring ${}^{Z}/_{4Z}$ the smallest positive integer n such that $n \cdot a = 0$ for all $a \in {}^{Z}/_{4Z}$ is 4. So characteristic of the ring ${}^{Z}/_{4Z}$ is 4 (even though $8 \cdot a = 0$ in $\frac{Z}{4Z}$, the characteristic is 4, not 8).

   In general, the characteristic of $\frac{z}{mz}$ is m.
3. F_2 and F_5 have characteristic (2) and (5) respectively.

1.2.2 Theorem:

Any $R \neq 0$ of positive characteristic having an identity and no zero divisors must have prime characteristic.

Proof:

Since R contains non zero elements, R has characteristic $n \geq 2$, if n were not prime.

We could write $n = k \cdot m$ with $k, m \in z, 1 < k, m < n$ then

$0 = ne = (km)e = (ke)(me)$, and this implies that either

$ke = 0$ or $me = 0$.

Since R has no zero divisors, it follows that either $kr = (ke)r = 0$ for all $r \in R$ or $mr = (me)r = 0$ for all $r \in R$ in contradiction to the definition of the characteristic (n).

1.2.1 Corollary: Evey finite field has prime characteristic.

Proof:

By theorem (1.2.2) it suffices to show that finite field has a positive characteristic, consider the multiples $e, 2e, 3e, \ldots$ of the identity, since F contains only finitely many distinct elements, there must exist integers k and m with $1 \leq k < m$ such that $ke = me$ or $(m - k)e = 0$, and so F has appositive characteristic.

(1.2 .2) Finite Fields Modulo irreducible polynomials:

The order of a finite prime field is equal characteristic of the field. However, this is not the general case for finite fields. A more general form of finite fields can be constructed using polynomials.

(1.2.2.1) Polynomials over an algebraic structure:

1.2.9 Definition: Polynomials over an algebraic structure:

Let A be a finite field with addition and multiplication.

A polynomial over A is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where n is a non-negative integer, the coefficients a_i, $0 \leq i \leq n$ are elements in A, and x is a symbol not belonging to A.

The coefficient a_n is called the leading coefficient and is not the zero-element in A for $n \neq 0$. The integer n is called the degree of $f(x)$ and is denoted by $n = \deg(f(x)) = \deg(f)$.

If the leading coefficient is a_0, then f is called a constant polynomial.

If the leading coefficient is $a_0 = 0$, then f is called the zero-polynomial and denoted by $f = 0$ we denote by $A[x]$ the set of all polynomials over algebraic structure A.

For $f, g \in A[x]$ with

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

and

$$g(x) = \sum_{i=0}^{m} b_i x^i$$

Over R are considered equal if and only if $a_i = b_i$ for $0 \leq i \leq n$.
We define the Sum of $f(x)$ and $g(x)$ by

1-

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)\, x^i$$

2-

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k \text{ where } c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq n \\ 0 \leq j \leq m}} a_i b_j$$

3- $$\deg(f + g) \leq \max(\deg(f), \deg(g)),$$

$$\deg(fg) \leq \deg(f) + \deg(g)$$

Now if A is a field, then because a field has no zero-divisors we will have

$c_{n+m} = a_n b_m \neq 0$ for $a_n \neq 0$ and $b_m \neq 0$. So if A is a field, then

$\deg(fg) = \deg(f) + \deg(g)$.

1.2.3 The Division Theorem for polynomials:

If f and g are polynomials over F and $g \neq 0$, then there exist over F unique polynomials q and r such that $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$.

Proof:

Let R denote the set of all polynomials over F which have the form $f - qg$ for some polynomial q over F.

If R contains 0, the polynomial with all coefficients zero, we set $r = 0 = f - qg$, and we are finished except for uniqueness.

Suppose then $0 \notin R$. Then the set

$S = \{n \in \overline{N}/n = \deg h, h \in R\}$

is nonempty since either $\deg f \in S$ or, when $f = 0, \deg g \in S$. Therefore, S has a smallest element m.

By definition of S we have $m = \deg r$ for some $r \in R$, and by definition of R we have $r = f - qg$ for some q. In other words,

$f = qg + r$, and it remains to show that $\deg r < \deg g$.

Clearly, there is an element $C \in F$ such that the polynomial S given by

$Sx = rx - Cx^{m-n}(gx) = fx - [(qx) + (Cx^{m-n})](gx)$

has degree $m - 1$ or less. However, $S \in R$ and this contradicts the minimality of m.

It must be that $\deg r < \deg g$

Suppose q' and r' are polynomials satisfying the same conditions as q and r

Then $f = qg + r = q'g + r'$ implies

$(q - q')g = r' - r$

If $q - q' \neq 0$, then taking degrees on both sides of this last equation we must have

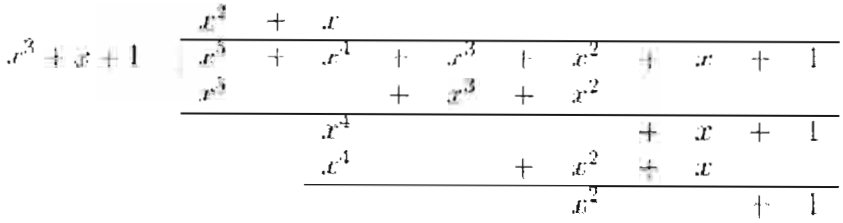
$\deg(q - q') + \deg g = max\{\deg r', \deg r\}$.

This implies that either $deg \leq \deg r'$ or $\deg g \leq \deg r$, both of which are wrong.

Thus, we must have $q = q'$ and, consequently, $r = r'$. This proves uniqueness.

1.2.4 Example:

Consider $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1 \in F_2[x]$, $g(x) = x^3 + x + 1 \in F_2[x]$ we can compute the polynomials $q, r \in F_2[x]$ with $f = qg + r$ by using long division.



Thus $q(x) = x^2 + x$ and $(x) = x^2 + 1$, and obviously $\deg(r) < \deg(g)$.

1.2.5 Example:

Let $f(x) = x^3 - 2$ and $g(x) = 2x^2 - 3$ with
$f, g \in F_5[x]$, or equivalently, $f(x) = x^3 + 3$, $g(x) = 2x^2 + 2$.

We have
$x^3 + 3 = 3x(2x^2 + 2) + (4x + 3)$,

thus
$q(x) = 3x$ and $r(x) = 4x + 3$

1.2.2 Corollary (The Remainder Theorem)

If f is a polynomial over the field F and α is an element of F, then there is a unique polynomial q over f such that.

$fx = (x - \alpha)(qx) + (f\alpha)$

Proof:

Applying the division theorem with g given by $gx = x - \alpha$, we have

$fx = (x - \alpha)(qx) + (rx)$

where $r = 0$ or $\deg r < \deg g = 1$. Thus, rx is a constant, and taking $x = \alpha$ shows that $rx = f\alpha$.

1.2.1 Proposition:

A polynomial of degree n over the field F has at most n roots in F.

Proof:

The proof is by induction on n. To start the induction, we note that a polynomial of degree 0 is a (non zero) constant and has no roots.

Now suppose the proposition is true for polynomials of degree less than n.

Let f be a polynomial of degree n.

If f has no root in F, then we are finished.

If f has a root $\alpha \in F$, then $fx = (x - \alpha)(qx)$ for some polynomials q over F of degree $n - 1$.

Then q has at most $n - 1$ roots in F, it clearly follows that f can have at most n roots since a root of f is either α or a root of q.

A polynomial of degree n over the field F which has all n roots in F is said to split over F. Clearly, a polynomial f of degree n splits over F if and only if it can be factored as

$$fx = C(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ are the roots of f.

1.2.2 Lemma:

Let F be a finite field containing a subfield k with q elements, then F has q^m elements, where $m = [F: k]$

Proof:

F is a vector space over k,and since F is finite,it is finite-dimensional as a vector space over k .

If $[F: k] = m$, then F has a basis over k consisting of m elements, say $b_1, \dots, b_m$.

Thus every element of F can be uniquely represented in the form

$a_1 b_1 + \cdots + a_m b_m$ (where $a_1, \dots, a_m \in k$) since each a_i can have q values, F must have exactly q^m elements.

1.2.4 Theorem: (Subfield Structure)

Let F be a finite field with p^n elements, then every subfield of F has p^m elements for some integer m dividing n.

Conversely, for any integer m dividing n there is a unique subfield of F of order p^m.

Proof:

A subfield K of the finite field F_{p^n} must have p^m, distinct elements for some positive integer m with $m \leq n$, by Lemma (1.2.2) p^n must be a power of p^m, so m must divide n.

On the other hand, assume that m divides n, then polynomial $x^{p^{m-1}} - 1$ divides

$x^{p^{n-1}} - 1$ and thus $x^{p^n} - x$ it follows that each root of $x^{p^m} - x$ is also a root of $x^{p^n} - x$.

Hence the field F_{p^n} must contain a splitting field of the polynomial $x^{p^m} - x$ over F_p and this splitting field must have exactly p^m distinct elements, if the subfield was not unique, that is, if there were two such fields contained in F_{p^n}, then their union would contain more than p^m roots of the polynomial $x^{p^m} - x$ in F_{p^n}, which is impossible.

1.2.5 Theorem: ((Existence and uniqueness of finite fields))

For every prime p and every positive integer (n), there exists afinite field with p^n elements, any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over F_p.

Proof:

(EXISTENCE) for $q = p^n$ consider $x^q - x$ in $F_p[x]$, and let F bits splitting field over F_p since its derivative is $qx^{q-1} - 1 = -1$ in $F_p[x]$ it can have no common root with $x^q - x$ and so, $x^q - x$ has q distinct roots in F, let $S = \{a \in F : a^q - a = 0\}$ then S is a subfield of since.

1- S contains O
2- $a, b \in S$ implies that $(a - b)^q = a^q - b^q = a - b$, so $a - b \in S$

3- For $a, b \in S$ and $b \neq 0$ we have $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, so $ab^{-1} \in S$

On the other hand $x^q - x$ must splitting S since S contains all its roots, *ie.* its splitting field F is a subfield of S.

Thus $F = S$ and, since S has q elements, F is afinite field with $q = p^n$ elements (uniqueness) let F be afinite field with $q = p^n$ elements, then F has characteristic p , and so contains F_p as asubfield, so F is asplitting field of $x^q - x$, the result now follows from theorem (existence and uniqueness of splitting field) say:

1. If k is a field and F any polynomial positive degree in $k[x]$, then there exists a splitting field of F over k
2. Any two splitting fields of F over k are isomorphic under an isomorphism which keeps the elements of k fixed and maps roots of F into each other.

Chapter II - Irreducible polynomial and extension as vector space

2.1 Irreducible polynomial and extension as vector space

2.1.10 Definition: Irreducible polynomial

Let A be a finite field. A polynomial $f \in A[x]$ is said to be irreducible over A or irreducible in $A[x]$, or prime in $A[x]$ if f has a positive degree and $f = gh$ with $g, h \in A[x]$ implies that either g or h is a constant polynomial).

A polynomial is said to be reducible over A if it is not irreducible over A.

2.1.6 Example:

For quadratic polynomial $f(x) = x^2 - 2x + 2$

(1) Discuss its reducibility over the usual infinite fields

(2) Investigate its reducibility over finite fields F_p for any odd prime number p

(3) Factor $f(x)$ over F_p for $p < 10$

using the rooting formula in elementary algebra, we can compute the two roots of $f(x) = 0$ as

$\alpha = 1 + \sqrt{-1}, \beta = 1 - \sqrt{-1}$

Solution:

(1) Since $\sqrt{-1}$ is not in $\mathbb{R}$, $f(x)$ is irreducible over $\mathbb{R}$

(Hence is irreducible over Z and Q).

But because $\sqrt{-1} = i \in C$ therefore $f(x)$ is reducible over $\mathbb{C}$

$f(x) = (x - 1 - i)(x - 1 + i)$

(2) A number x is a square modulo p if and only if there exists $y(mod\ p)$ satisfying $y^2 \equiv x(mod\ p)$, "by Fermat's little theorem" we know that all $x(mod\ p)$ satisfies $x^{p-1} \equiv 1(mod\ p)$. For p being an odd prime, Fermat's little theorem is equivalent to.

(*) $x^{(p-1)/2} \equiv \pm 1(mod\ p)$

For all x with $0 < x < p$ (where -1 denotes $p - 1$).

If x is square modulo p, then "Equation *" becomes

$x^{(p-1)/2} \equiv (y^2)^{(p-1)/2} \equiv y^{(p-1)} \equiv 1(mod\ p)$.

Therefore, we know that "Equation *" provides a criterion for testing whether x is a square modulo an odd prime p: x is a square (respectively, non-square) modulo p if the test yields 1 (respectively, -1)

to this end we know that for any odd prime $p, f(x)$ is reducible over $F_p \Leftrightarrow (-1)^{(p-1)/2} \equiv (mod\ p)$, and is irreducible $\Leftrightarrow (-1)^{(p-1)/2} \equiv 1$. In other words, $f(x)$ is reducible (or irreducible) over F_p if $p \equiv 1(mod\ 4)$ or $p \equiv 3\ (mod\ 4)$.

(3) For $p = 2, f(x) = x^2 - 2x + 2 = x^2 - 0x + 0 = x^2$ and is reducible over F_2, the only odd prime less then 10 and congruent to 1 modulo 4 is 5, since we can completely factor $f(x)$ over F_5,

$$f(x) = (x - 1 - \sqrt{-1})(x - 1 + \sqrt{-1}) = (x - 1 - 2)(x - 1 + 2)$$
$$= (x + 2)(x + 1)$$

(2.2) Field construction using irreducible polynomial:

2.2.11 Definition: Set $A[x]$ modulo a polynomial

Let A be a finite field and let $f, g, q, r \in A[x]$ with $g \neq 0$ satisfy the division expression(1,2,3) we say r is the remainder of f divided by g and denote $r \equiv f(mod\ g)$. The set of the remainders of all polynomials in $A[x]$ modulo g is called the polynomials in $A[x]$ modulo g, and is denoted by $A[x]_g$.

2.2.6 Theorem:

Let F be a field and f be a non-zero polynomial in $F[x]$. Then $F[x]_f$ is a ring and is a field if and only if f is irreducible over F.

Proof:

First: $F[x]_f$ is obviously a ring under addition and multiplication modulo f defined by (1.2.9) with the zero-element and unity-element the same as those of F.

Secondly: Let $F[x]_f$ be a field. Suppose $f = gh$ for g, h being non-constant polynomials in $F[x]$.

Then because $0 < \deg(g) < \deg(f)$ and $0 < \deg(h) < \deg(f)$,

g and h are non-zero polynomials in $F[x]_f$ whereas f is the zero polynomial in $F[x]_f$.

This violets the closure Axiom for the multiplicative group of $F[x]_f$.

So $F[x]_f$ can not be a field. This contradicts the assumption that $F[x]_f$ is a field.

Finally: Let f be irreducible over F,

since $F[x]_f$ is a ring, it suffices for us to show that any non-zero element in $F[x]_f$ has a multiplicative inverse in $F[x]_f$.

Let r be a non-zero polynomial in $F[x]_f$ with $\gcd(f, r) = c$ because $\deg(r) < \deg(f)$ and f is irreducible, c must be a constant polynomial.

Writing $r = cs$, we have $c \in F$ and $s \in F[x]_f$ with $\gcd(f, s) = 1$.
Analogous to the integer case, we can use the extended Euclid algorithm for polynomials to compute $s^{-}(mod\ f) \in F[x]_f$.
Also since $c \in F$, there exists $c^{-1} - F$.
Thus we obtain $r^{-1} = c^{-1}s^{-1} \in F[x]_f$.

2.2.2 Proposition:
A polynomial f, irreducible over the field F, has a root in F if and only if $\deg f = 1$.

Proof:
If $\deg f = 1$, then
$fx = c_0 + c_1 x$
and f has $-c_0|c_1$ as root in F.
On the other hand, if f has a root $\alpha \in F$,
then $fx = (x - \alpha)(qx)$ for some polynomial q over F.
Since f is irreducible,
it must be that $\deg q = 0$ and consequently $\deg f = 1$.

2.2.7 Theorem:
Let F be a field of p elements, and f be a degree $-n$ irreducible polynomial over F, then the number of elements in the field $F[x]_f$ is p^n.

Proof:
From definition (1.2.9) we know $F[x]_f$ is the set of all polynomials in $F[x]$ of degrees less than $\deg(f) = n$ with the coefficients ranging through F of p elements, there are exactly p^n such polynomials in $F[x]_f$.

2.2.3 Corollary:

The only irreducible polynomials over the field of complex numbers $\mathbb{C}$ are those of degree 1.

As an example we note that the polynomials $x^2 + 1$ over the field of rational number $\mathbb{Q}$ is irreducible, but considered as a polynomial over $\mathbb{C}$ it is reducible

$x^2 + 1 = (x - i)(x + i)$.

2.2.12 Definition:

Let $K \subset L$ be a field and $\alpha \in L$ be algebraic over K.
Let $K[x]$ be the ring of polynomial functions over K.

Then the unique irreducible, monic polynomial $f \in K[x]$ such that $f(\alpha) = 0$ is called the minimal of α over K.

2.2.3 Proposition:

If f is a minimal polynomial for α over F, then

1. f is irreducible over F
2. f divides any polynomials over F having α as a root

Proof:
Suppose f is irreducible, say $f = gh$.
Then we have $f\alpha = (g\alpha)(h\alpha) = 0$, which imply $g\alpha = 0$ or $h\alpha = 0$.
Both g and h have degree less than f, contradicting the definition of f as a minimal polynomial for α. Thus, f is irreducible.
Suppose α is a root of a polynomial g over f. By the division theorem we can write $g = qf + r$. Then we have $g\alpha = (q\alpha)(f\alpha) + r\alpha = 0$ which implies $r\alpha = 0$. If $r \neq 0$, then $\deg r < \deg f$. But then r is a polynomial of degree less than f with α as a root, contradicting the minimality of f. Thus, $r = 0$ and.$f|g$
2.2.7 Example:
1- The element $\sqrt[3]{3} \in R$ is algebraic over Q since it is a root of $x^3 - 3 \in Q[x]$, since $x^3 - 3$ is irreducible over Q, it is the minimal polynomial of $\sqrt[3]{3}$ over Q, and hence $\sqrt[3]{3}$ has degree 3 over Q.
2- The element $i = \sqrt{-1} \in C$ is algebraic over the subfield R or C, since it is the a root of the polynomial $x^2 + 1 \in R[x]$,since $x^2 + 1$ is irreducible over R, it is the minimal polynomial of i over R, and hence i has degree 2 over R

2.3 Field extension as vector space

Let L be an extension field of k, an important observation is that L may be viewed as a vector spaces over k, the elements of L are the "vectors" and elements of k are the "scalars" we briefly recall the main properties of a vector space.

2.3.13 Definition:

A vector space V over F is non empty set of elements "called vectors" up on which two operations are defined

1- Addition: There is some rule which produces, from any two elements in V, another elements in V (denote this operation by +)

2- Scalar multiplication: There is some rule which produces from an element of F (ascalar) and an element in V another element in V. These elements and operations obey the vector Axiom

- $x + y = y + x$ for all $x, y \in V$
- $(x + y) + z = x + (y + z)$ for all $x, y, z \in V$
- There exists an element $0 \in V$ such that $x + 0 = x$ for all $x \in V$
- For every $x \in V$ there exists an element $(-x)$ such that $x + (-x) = 0$
- $\lambda(x + y) = \lambda x + \lambda y$ for all $x, y \in V$ and all scalars $\lambda \in F$
- $(\lambda+\mu)x = \lambda x + \mu x$ for all $x = V$ and all scalars $\lambda,\mu \in F$
- $(\lambda\mu)x = \lambda(\mu x)$ forall $x \in V$ and all scalars $\lambda,\mu \in F$
- $1x = x$ for all $x \in V$

2.3.14 Definition:

1- A basis of a vector space Vover F is defined as a subset $\{v_1, v_2, \ldots v_n\}$ of vectors in V that are linearly independent and span V, if $v_1, v_2, \ldots, v_n$ is a list of vectors in V, then these vectors form a basis if and only if every $v \in V$can be uniquely written as

$v = a_1 v_1 + \cdots + a_n v_n$

2- A vector space will have many different bases, but there are always the same number of basis vector in each. The number of basis vectors in any basis is called the dimension of V over F.

3- Suppose V has dimension n over F, then any sequence of more than (n) vectors in V is linearly dependent.

2.3.4 Propositions:

A linearly independent spanning set is a basis.

Proof:

Suppose that B is a linearly independent spanning set for E over F.

If B is not a basis, then some proper subset S of B also spans E over F.

Choose $\beta \in B - S$. Since S spans E over F, there are elements $\delta_1, \delta_2, \ldots, \delta_m \in S$ and coefficient $C_1, C_2, \ldots, C_m \in F$ such that

$\beta = C_1\delta_1 + C_2\delta_2 + \cdots + C_m\delta_m$

However, this implies that the set $\{\beta, \delta_1, \delta_2, \ldots \delta_m\}$, which is a finite subset of B, is linearly dependent over F.

This contradicts the linear independence of B. Thus, B must be a basis.

2.3.5 Propositions:

If B is a basis for E over F, then every of E may be written uniquely as a linear combination of elements of B with coefficients in F.

Proof:

We have only to prove uniqueness since B spans E over F.

Suppose that $\beta \in E$ can be written in two ways as a linear combination of elements of B,

Say

$\beta = C_1\beta_1 + C_2\beta_2 + \cdots + C_n\beta_n,$

$\beta = d_1\beta_1 + d_2\beta_2 + \cdots d_n\beta_n,$

where we assume without loss of generality that the same elements $\beta_1, \beta_2, \ldots, \beta_n$ of B are involved in the linear combinations.

Now subtracting the two expressions above, we have

$(C_1 - d_1)\beta_1 + (C_2 - d_2)\beta_2 + \cdots + (C_n - d_n)\beta_n = 0$

linear independence of the set $\{\beta_1, \beta_2, \ldots, \beta_n\}$ implies that $C_i = d_i$ for $i = 1,2, \ldots, n$ uniqueness is proved.

2.3.8 Example:

The vectors $(2,2,5)$, $(3,3,12)$ and $(5,5,-1)$ are linearly dependent elements of the real vector space R^3 , since $7(2,2,2) - 3(3,3,12) - (5,5,-1) = (0,0,0)$.

(Thus if $V_1 = (2,2,5), V_2 = (3,3,12)$ and $V_3 = (5,5,-1)$, then the equation

$C_1V_1 + C_2V_2 + C_3V_3 = 0$ is satisfied with $C_1 = 7$, $C_2 = -3$ and $C_3 = -1$.

2.3.9 Example:

Let $p_j(x) = x^j$ for $j = 0,1,2,\dots,n$ where n is some positive integer. Then the polynomials $p_0(x), p_1(x), p_2(x), \dots, p_n(x)$ are the linearly independent elements of the vectors space consisting of all polynomials with real coefficients.

Indeed if $c_0, c_1, \dots, c_n$ are real numbers and if

$c_0p_0(x) + c_1p_1(x) + c_2p_2(x) + \cdots + c_np_n(x) = 0$

then $c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ is the zero polynomial, and

therefore $c_j = 0$ for $j = 0,1,2,\dots,n$.

2.3.3 Lemma: Let V be a vector space over a field k, let c be an element of k and let v be an element of v. Suppose that cv = 0 then either c=0 or v=0.

Proof:

Suppose that cv=0 and c≠ 0. We must show that v=0.

Now there exists an element c^{-1} of k satisffying $c^{-1}c=1$,

since any non-zero element of a field has a multiplicative inverse, then it follows from the vector space axioms

$v=1v=(c^{-1}c)v=c^{-1}(cv)=c^{-1}0=0$, as required.

2.3.15 Definition:

Let L be an extension field of k, if L is finite dimensional as vector space over k, the dimension of the vector space L over k is called the degree of L over k and it is written $[L:k]$.

2.3.8 Theorem:

If L is a finite extension of k and M is a finite extension of L, then M is a finite extension of k with $[M:k]=[M:L][L:k]$

Proof:

Let $[M:L]=m$, $[L:k]=n$

Let $\{\alpha_{1,\dots,}\alpha_m\}$ be a basis of M over L, and let $\{\beta_{1,\dots,}\beta_n\}$ be a basis of L over k.

We shall use them to form a basis of M over k of appropriate cardinality. Every $\alpha \in M$ can be expressed as a linear combination $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_m\alpha_m$ for some $\gamma_{1,\dots,}\gamma_m \in L$, writing each γ_i as a linear combination of the β_j is we get

$$\alpha = \sum_{i=1}^{m} \gamma_i\,\alpha_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} r_{ij}\,\beta_j)\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\,\beta_j\alpha_i$$

with coefficients $r_{ij} \in k$, we claim that the mn elements $\beta_j \alpha_i$ form a basis of M over k, clearly they span M; it suffices to show that they are linearly independent over k.

$$\sum_{i=1}^{m} \sum_{j=1}^{n} S_{ij} \beta_j \alpha_i = 0$$

where the coefficients $S_{ij} \in k$ then

$$\sum_{i=1}^{m} (\sum_{j=1}^{n} S_{ij} \beta_j) \alpha_i = 0$$

and since the α_i are linearly independent over L we must have

$$\sum_{j=1}^{n} S_{ij} \beta_j = 0$$

for $1 \leq i \leq m$, now, since the β_j are linearly independent over k, it follows that all δ_{ij} are 0, as required.

2.3.9 Theorem:

Every finite extension of k is algebraic over k.

Proof:

Let L be a finite extension of k, and let $[L:k] = m$ for $\alpha \in L$. The $m+1$ elements $1, \alpha, \ldots, \alpha^m$ must be linearly dependent over k.

i, e must satisfy $a_0 + a_1 \alpha + \cdots + a_m \alpha^m = 0$ for some $a_i \in k$ (not all zero), thus α is algebraic over k.

Chapter III - Elliptic curve cryptography

A class of groups which are very important to modern cryptography is those constructed by point on elliptic curves. Miller and Koblitz originally suggest to use elliptic curve groups for realizing public – key cryptography.

(3.1) Group constructed using points on an Elliptic Curve

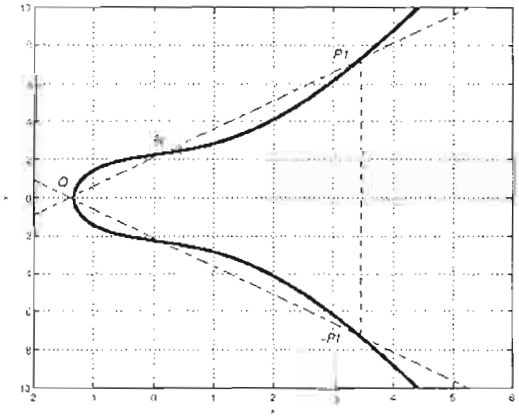
3.16 Definition of Elliptic curves

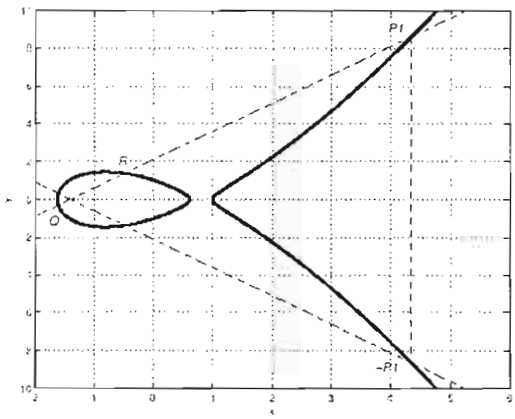
An elliptic curve is defined by an equation of the form:

$y^2+axy+by = x^3+cx^2+dx + e$

where $a, b, c, d, and\ e$ are real numbers. A special addition operation is defined over elliptic curves, and this with the inclusion of a point O, called point at infinity.

Figure (1) shows the elliptic curves $y^2=x^3+2x+5$ and $y^2=x^3-2x+1$





3.1 Elliptic curves over Galois Fields

An elliptic group over the Galois Field $E_p(a, b)$ is obtained by computing $x^3+ax + b$ mod p for $0 \leq x < p$. The constants a and b are non negative integers that the prime number p and must satisfy the condition:

$4a^3+27b^2 \not\equiv 0\ (mod\ p)$

for each value of x, one needs to determine whether or not it is a quadratic residue.

If it is the case, then there are two values in the elliptic group. If not, then the point is not in the elliptic group $E_p(a, b)$.

3.2 The group operation

3.2.17 Definition:

Elliptic curve group operation ("tangent and chord method")

Let p, Q ∈E, I be the line containing p and Q (tangent line to E if p=Q), and R, the third point of intersection of I with E. Let I' be the line connecting R and O.
Then $p''+''$Q is the point such that I' intersects E at R, O and $p''+''$Q
Notice that

$$\Delta = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{3}\right)^2 = \frac{4a^3 + 27b^2}{4 \times 27}$$

is the discriminant of the cubic polynomial

$$f(x) = x^3 + ax + b.$$

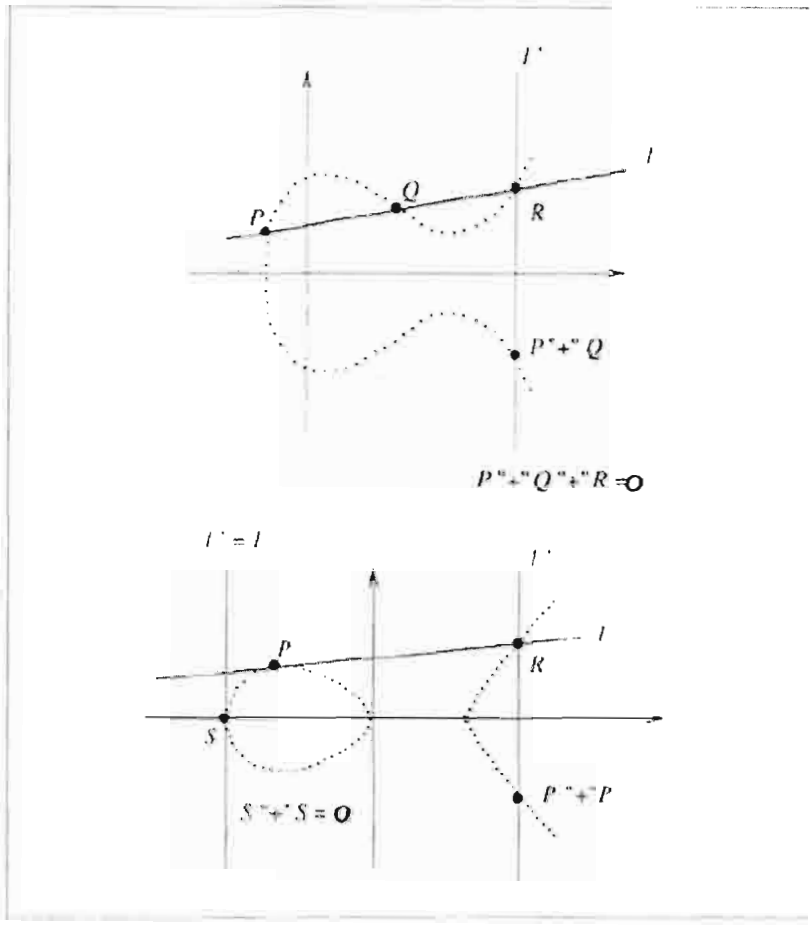
If $\delta = 0$ then $f(x) = 0$ has at least a double zero × (root which makes $f(x) = 0$) and clearly $(x, 0)$ is on E.

For $F(x, y) = y^2 - x^3 - ax - b = 0$ this point satisfies

$$\frac{\partial F}{\partial y} = 2y \Big|_{y=0} = \frac{\partial F}{\partial x} \Big|_{x=X} = 0$$

That is, $(x, 0)$ is a singular point at which there is no definition for real tangent value. With the tangent – and chord operation failing at the singular point $(x, 0)$, E can not be a group.

Fig(2) illustrates the tangent – and- chord operation.
The top curve is the case of $\Delta < 0$ (the cubic polynomial has only one real root) and the lower, $\Delta > 0$. We have intentionally plotted the curves as dotted lines to indicate $E(F_p)$ being a discrete points are called F_p - rational points.



Now let us show that $(E,"+")$ does form a group under the tangent – and – chord operation.

First, for any p=(X,Y)∈E , let us apply definition $(*)$ to a special case of Q being O (since we have included O in E). Line ℓ intersecting p and O is

$\ell: x = X.$

Since p∈E means $f(x) = x^3 + ax + b \bmod p$ being a quadratic residue in F_p, therefore -Y is the other solution to $y^2 = f(x)$ (i.e, the other square root of $f(x)$ modulo pThat is, ℓ also intersects point $R = (x, -y) \in E$.

Clearly, because $\ell' = \ell$, it intersect the same three points on E as ℓ does. By definition $(*)$ we obtain

P=P″+″O

For any p∈E. Moreover, for all $(x, y) \in E$, we have also derived

$(x, y)" + (x, -y) = O$

By denoting $(x, -y) = -"(x, y)$, we see that point O behaves exactly as the identity element under the operation " + ".

Therefore we have obtained Identity Axiom and Inverse Axiom $(E," + ")$.

A special case of this special case is $y_1 = -y_2 = 0$.

This is the case of $p = " - "p$ (point S on the lower curve in Fig 5.1). At this doubly special point we have $p = " + "p = 0$. That is, p is an order -2 element.
We have mentioned this special element earlier: it is a solution of $y^2 = f(x) \equiv 0 \pmod{p}$. Such special points only exist when $f(x)$ has zeros in F_p
i.e. , when $f(x)$ is reducible over F_p.
Now let us consider the general case of ℓ being a non-vertical line.

The formula for ℓ is

Equation (1)
$\ell: y - y_1 = \lambda(x - x_1)$ where

Equation (2)

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & if\ x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & if\ x_1 = x_2\ and\ y_1 = y_2 \neq 0 \end{cases}$$

since ℓ will meet $R = (x_3, y_3)$ on the curve, we can use formulae
$E: y^2 = x^3 + ax + b\ (mod\ p)$ and $\ell: y - y_1 = \lambda(x - x_1)$ to find the point R.
The X part of the point R is a solution of
$\ell \cap E: [\lambda(x - x_1) + y_1]^2 - (x^3 + ax + b) = 0$
Notice that $\ell \cap E$ is a cubic polynomial which has solutions x_1, x_2, x_3. We can also write it as
$\ell \cap E: C(x - x_1)(x - x_2)(x - x_3) = 0$
where C is some consonant $\ell \cap E$ (the coefficient of x^3 and x^2) we obtain $C = -1$ and
$x_3 = \lambda^2 - x_1 - x_2$
Finally, by definition $(*)$ and the fact that $p" + "Q = " - "R$, we obtain the coordinates of the point $p" + "Q$ as
Equation:
$x_3 = \lambda^2 - x_1 - x_2$
$y_3 = \lambda(x_1 - x_3) - y_1$
Where λ is defined in "Equation 2" we notice that because line ℓ intersect p, Q and R, R must be on the curve, and consequently, $p" + "Q = " - "R$ must also be on the curve.
Thus, we have obtained closure Axiom for $(E, " + ")$ is indeed a group. Moreover, it is clearly an abelian group.

3.2.10 Example:

The equation $E: y^2 = x^3 + 6x + 4$ over F_7 defines an elliptic curve group since $4 \times 6^3 + 27 \times 4^2 \equiv 0 \ (mod\ 7)$.

The following points are on $E(F_7)$

$E(F_7) = \{O, (0,2), (0,5), (1,2), (1,5), (3,0), (4,1), (4,1), (4,6), (6,2), (6,5)\}$.

some applications of the addition law are

$(3,0)" + "(3,0) = O$, $(3,0)" + "(4,1) = (1,2)$ and $(1,2)" + "(1,2) = (0,2)$.

3.2.11 Examples: (Construction of an elliptic group)

Let the prime number $p = 23$ and let the constants $a = 1$ and $b = 1$, we first verify that:

$4a^3 + 27b^2 mod\ p = 4 \times 1^3 + 27 \times 1^2\ mod\ 23$

$4a^3 + 27b^2 mod\ p = 4 + 27\ mod\ 23$

$4a^3 + 27b^2 mod\ p = 8 \neq 0$

we then determine the quadratic residues Q_{23} from the reduced set of residues

$Z_{23} = \{1,2,3, \ldots, 21,22\}$

$x^2\ mod\ p$	$(p-x)^2\ mod\ p$	=
$1^2\ mod\ 23$	$22^2\ mod\ 23$	1
$2^2\ mod\ 23$	$21^2\ mod\ 23$	4
$3^2\ mod\ 23$	$20^2\ mod\ 23$	9
$4^2\ mod\ 23$	$19^2\ mod\ 23$	16
$5^2\ mod\ 23$	$18^2\ mod\ 23$	2
$6^2\ mod\ 23$	$17^2\ mod\ 23$	13
$7^2\ mod\ 23$	$16^2\ mod\ 23$	3
$8^2\ mod\ 23$	$15^2\ mod\ 23$	18
$9^2\ mod\ 23$	$14^2\ mod\ 23$	12
$10^2\ mod\ 23$	$13^2\ mod\ 23$	8
$11^2\ mod\ 23$	$12^2\ mod\ 23$	6

Therefore, the set of $\frac{p-1}{2} = 11$ quadric residues $Q_{23} = \{1,2,3,4,6,8,9,12,13,16,18\}$

Now, for $a \leq x < p$, compute $y^2 = x^3 + x + 1\ mod\ 23$ and determine y^2 is in the set of quadratic residues Q_{23}:

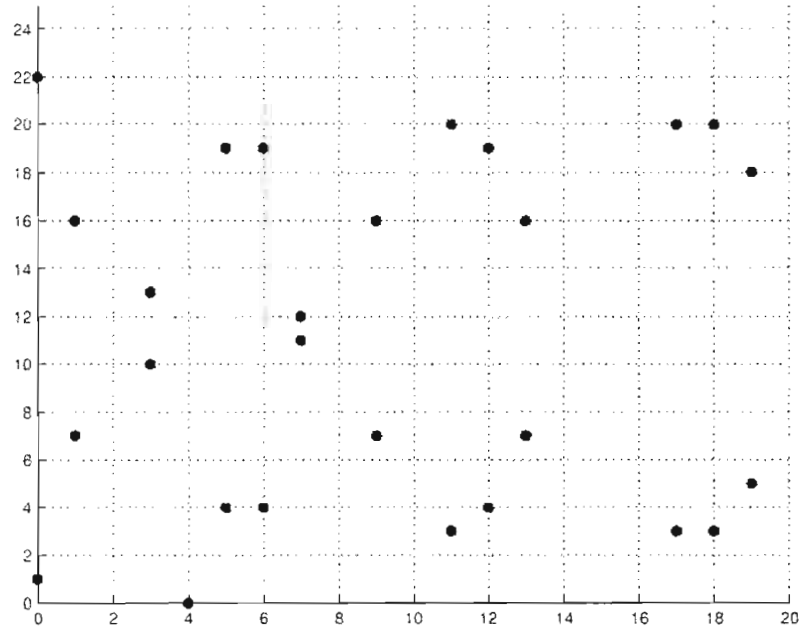
x	0	1	2	3	4	5	6	7	8	9	10	11
y^2	1	3	11	8	0	16	16	6	15	3	22	9
$y^2 \in Q_{23}?$	yes	yes	no	yes	no	yes	yes	yes	no	yes	no	yes
y_1	1	7		10	0	4	4	11		7		3
y_2	22	16		13	0	19	19	12		16		20

x	12	13	14	15	16	17	18	19	20	21	22
y^2	16	3	22	10	19	9	9	2	17	14	22
$y^2 \in Q_{23}?$	yes	yes	no	no	no	yes	yes	yes	no	no	no
y_1	4	7				3	3	5			
y_2	19	16				20	20	18			

The elliptic group $E_p(a, b,) = E_{23}(1,1)$ thus include the points

$$E_{23}(1,1) = \left\{ \begin{matrix} (0,1)(0,22)(1,7)(1,16)(3,10)(3,13)(4,0) \\ (5,4)(5,19)(6,4)(6,19)(7,11)(7,12)(9,7) \\ (9,16)\ (11,3)(11,20)(12,4)(12,19)(13,7)(13,16) \\ (17,3)(17,20)(18,3)(18,20)(19,5)(19,18) \end{matrix} \right\}$$

Figure (3) shows a Scatterplot of the elliptic group $E_p(a, b) = E_{23}(1,1)$



3.2.1 Addition and multiplication operations over elliptic groups

Let the points $P = (x_1, y_1)$ and $Q(x_2, y_2)$ be in the elliptic group $E_p(a, b)$, and O be the point at infinity, the rules for addition over the elliptic group $E_p(a, b)$ are:

1. $P + O = O + P = P$
2. if $x_2 = x_1$ and $y_2 = -y_1$, that is $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (x_1, -y_1) = -P$, then $P + Q = O$
3. if $Q \neq -P$, then their sum $P + Q = (x_3, y_3)$ is given by

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

where

$$\lambda \triangleq \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ p \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & if\ p = Q \end{cases}$$

3.2.12 Example (Multiplication over on elliptic curve group):

The multiplication over an elliptic curve group $E_p(a, b)$ is the equivalent operation of the modular exponentiation in RSA.

Let $P = (3,10) \in E_{23}(1,1)$. Then $2P = (x_3, y_3)$ is equal to:

$2P = P + P = (x_1, y_1) + (x_1, y_1)$ since $P = Q$ and $x_2 = x_1$, the values of λ, x_3 and y_3 are given by:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p = \frac{3x(3)^2 + 1}{2x10} \bmod 23 = \frac{5}{20} \bmod 23 = 4^{-1} \bmod 23 = 6$$

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p = 6^2 - 3 - 3 \bmod 23 = 30 \bmod 23 = 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p = 6 \times (3 - 7) - 10 \bmod 23 = -34 \bmod 23 = 12$$

Therefore $2P = (x_3, y_3) = (7,12)$

The multiplication kp is obtained by repeating the elliptic curve addition operation k times by following the same additive rules.

k	$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ (if $p \neq Q$) or $\lambda = \frac{3x_1^2 + a}{2y_1}$ (if $p = Q$)	x_3 $\lambda^2 - x_1 - x_2$ mod 23	y_3 $\lambda(x_1 - x_3) - y_1$ mod 23	kp (x_3, y_3)
1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)
4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,6)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)
26	12	7	11	(7,11)
27	6	3	13	(3,13)

References

1. Wenbo Mao Hewlett- Packard company , Modern cryptography: Theory and practice, 2003.;
2. Clark Allan, Elements of Abstract Algebra, Purdue University;
3. Sudan Madhu and Yuen Henry, Algebra and Computation *(MIT 6.S897),* lecture (3);
4. Panario Daniel, A mini course in finite fields and applications, Carlton University, 2006.;
5. Wilkins D.R, Mathematics course 111:Algebra I part IV:Vector spaces, Academic year 1996/7;
6. Prof.: Dr Jean-Yves Chouinard, Notes on Elliptic curve cryptography, 2002.;
7. Chapter 3: Finite Field.

Internet

- (3.) www.people.csail.mit.edu
- (6.) www.site.uottawa.ca
- (7.) www.groups.mcs.st-and.ac.uk

Figures:

- Figure (1) - Prof.: Dr Jean-Yves Chouinard, Notes on Elliptic curve cryptography, 2002., page 1;
- Figure (2) - Wenbo Mao Hewlett- Packard company , Modern cryptography: Theory and practice, 2003., page 198;
- Figure (3) - Prof.: Dr Jean-Yves Chouinard, Notes on Elliptic curve cryptography, 2002., page 3;