CHAPTER 2
MATHEMATICAL BACKGROUND

2.1. Introduction To Number Theory

Number theory, in a general sense, is the study of numbers and their properties, and studying the applications of number theory, particularly those directed towards computer science. So that, number theory has been used in many ways to devise algorithms for efficient computer arithmetic and for computer operations with large integers[6].

One of the most important applications of number theory to computer science is in the area of cryptography.

2.1.1. Prime Numbers

The positive integer 1 has just one positive divisor. Every other positive integer has at least two positive divisors, because it is divisible by 1 and by itself. Integers with exactly two positive divisors are of great importance in number theory; they are called primes [6,7].

Definition: A prime is a positive integer greater than 1 and its divisors are only one and itself.

Example: the integers 2, 3, 5,7,13 and 163 are primes

Definition: The integer which is not a prime, and which is not equal to 1, is called a ***composite***.

Example.2.1 the integers $4 = 2 * 2$, $8 = 4 * 2$, $33 = 3 * 11$ and $1001 = 7 * 11 * 13$ are composite.

the primes are the building blocks of the integers. Later, will show that every positive integer can be written uniquely as the product of primes.

$$a = p_1^{a1} p_2^{a2} \dots \dots \dots . p_t^{at} \qquad (2.1)$$

where $p_1 < p_2 < \dots\dots < p_t$ are prime numbers and each is a positive integer. This is known as the fundamental theorem of arithmetic.

2.1.2. The Fundamental Theorem of Arithmetic

Every positive integer can be written uniquely as a product of primes, with the prime factors in the product written in order of non - decreasing size [6].

Example.2.2 the factorizations of some positive integers are given by

$$240 = 2 * 2 * 2 * 2 * 3 * 5 = 2^4 * 3 * 5,\ 289 = 17 * 17 = 17^2,\ 1001 = 7 * 11 * 13$$

Note that, it is convenient to combine all the factors of a particular prime into a power of this prime, such as in the previous example. Factorizations of integers in which the factors of primes are combined to form powers are called ***prime-power factorizations.***

2.1.3. Greatest Common Divisors

If a and b are integers, that are not both zero, then the set of common divisors of a and b is a finite set of integers, always containing the integers $+1$ and -1. We are interested in the largest integer among the common divisors of the two integers [7,8].

Definition. The greatest common divisor of two integers a and b, that are not both zero, is the largest integer which divides both a and b.The greatest common divisor of a and b is written as (a, b).

Example.2.3 the common divisors of 24 and 84 are ± 1, ± 2, ± 3, ± 4, ± 6, and ± 12 . Then$(24,84) = 12$.

The pairs of integers sharing no common divisors greater than l. Such pairs of integers are called *relatively prime*.

Definition. The integers a and b are called *relatively prime* if a and b have greatest common divisor $(a, b) = 1$.

Example 2.4. Since (25,42) =1, 25 and 42 are relatively prime

2.1.4. The Chinese Remainder Theorem

The systems of congruences that involve only one variable, but different moduli. Such systems arose in ancient Chinese puzzles such as the following: Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7.

This puzzle leads to the following system of congruences :

$$x \equiv 1 (\text{mod } 3), \qquad x \equiv 2 (\text{mod } 5), \qquad x \equiv 3 (\text{mod } 7)$$

then a method for finding all solutions of systems of simultaneous congruences such as this. The theory behind the solution of systems of this type is provided by the following theorem, which derives its name from the ancient Chinese heritage of the problem [6,7].

The Chinese Remainder Theorem.

Let $m_1 m_2 \ldots\ldots m_r$ be pair wise relatively prime positive integers. Then the system of congruence

$$x \equiv a_1 \ (\text{mod } m_1)$$
$$x \equiv a_2 \ (\text{mod } m_2)$$
$$.$$
$$.$$
$$x \equiv a_r \ (\text{mod } m_r)$$

has a unique solution modulo $M = m_1 m_2 \ldots\ldots m_r$

illustrating the use of the Chinese remainder theorem by solving the system that arises from the ancient Chinese puzzle [6].

Example 2.5. To solve the system

$$x = 1 \pmod 3$$

$$x = 2 \pmod 5$$

$$x = 3 \pmod 7$$

having $M = 3.5.7 = 105$, $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, and $M_3 = 105/7 = 15$. To determine y_1, solve $35y_1 \equiv 1 \pmod 3$, or equivalently, $2y_1 \equiv 1 \pmod 3$.This yields $y_1 \equiv 1 \pmod 3$. find $y_1$by solving $2ly_1 \equiv 1 \pmod 5$; this immediately gives $y_2 \equiv 1 \pmod 5$. Finally, find $y_3$by solving $15y_3 \equiv 1 \pmod 7$. This gives$y_3 \equiv 1 \pmod 7$. Hence,

$$x \equiv 1 * 35 * 2 + 2 * 21 * 1 + 3 * 15 * 1$$

$$\equiv 157 \equiv 52 \pmod{105}$$

2.1.5. Fermat's Little Theorem.

If p is prime and a is a positive integer with $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod p$.

Example 2.6 Let $p = 7$ and $a = 3$. Then, $1.3 = 3 \pmod 7$, $2.3 = 6 \pmod 7$, $3.3 = 2 \pmod 7$, $4.3 = 5 \pmod 7$, $5.3 = 1 \pmod 7$, and $6.3 = 4 \pmod 7$.

consequently,

$$(1.3)(2.3)(3.3)(4.3)(5.3)(6.3) \equiv 3.6.2.5.1.4 \pmod 7$$

so that $3^6.1.2.3.4.5.6 \equiv 3.6.2.5.1.4 \pmod 7$. Hence $3^6.6! \equiv 6! \pmod 7$ and therefore.

$$3^6 \equiv 1 \pmod 7$$

Theorem 2.1. If p is prime and a is a positive integer, then

$$a^p \equiv a \pmod p$$

If $p \mid a$, by Fermat's little theorem, know that $a^{p-1} \equiv 1 \pmod p$. Multiplying both sides of this congruence by a, find the $a^p \equiv a \pmod p$ [6].

If $p|a$, then $p|a^p$ as well , so that $a^p \equiv a \equiv 0 \pmod p$. this finishes the proof, since $a^p \equiv a \pmod p$ if $p \nmid a$ and if $p \mid a$.

2.1.6. Euler's Theorem.

If m is a positive integer and a is an intrger with $(a, m) = 1$, then

$$a^{\emptyset(m)} \equiv 1 \pmod{m}.$$

Example. Know that both the sets 1,3,5,7 and 3.1, 3.3, 3.5, 3.7 are reduced residue systems modulo residues modulo 8. Hence, the have the same least positive residues modulo 8. Therefore,

$$(3 * 1)(3 * 3)\ (3 * 5)\ (3 * 7) = \ 1 * 3 * 5 * 7\ (mod\ 8),$$

and

$$3^4 * 1 * 3 * 5 * 7 \equiv 1 * 3 * 5 * 7 (\mathrm{mod}\ 8)$$

since $(1 * 3 * 5 * 7, 8) \ = \ 1$, and conclude that

$$3^4 \equiv 3^{\emptyset(8)} \equiv 1 \pmod{8}$$

the idea was illustrated by this example used to prove Euler's theorem [6,8].

Proof. Let$r_1 , r_2 , \dots\dots , r_{\emptyset(m)}$ denote the reduced residue system made up of the positive integers not exceeding m that are relatively prime to m. By Theorem 5.9, since $(a, m) = 1$, the set $ar_1 , ar_2 , \dots\dots , ar_{\emptyset(m)}$ is also a reduced residue system modulo m. Hence, the least positive residues of $ar_1 , ar_2 , \dots\dots , ar_{\emptyset(m)}$ must be the integers $r_1 , r_2 , \dots\dots , r_{\emptyset(m)}$ in some order. Consequently, if multiply together all terms in each of these reduced residue systems, then obtain

$$ar_1 , ar_2 , \dots\dots , ar_{\emptyset(m)} = r_1 , r_2 , \dots\dots , r_{\emptyset(m)} \ (\mathrm{mod}\ m)$$

thus,

$$a^{\emptyset(m)}\ r_1 , r_2 , \dots\dots , r_{\emptyset(m)} = \ r_1 , r_2 , \dots\dots , r_{\emptyset(m)} \ (\mathrm{mod}\ m)$$

since $(r_1 , r_2 , \dots\dots , r_{\emptyset(m)}, m) = 1$, then, can conclude that

$$a^{\emptyset(m)} \equiv 1 \pmod{m}$$

Can be used Euler's Theorem to find inverses modulo m. If a and m are relatively prime, know that

$$a . a^{\emptyset(m)-1} = a^{\emptyset(m)} \equiv 1 \pmod{m}$$

hence, $a^{\emptyset(m)-1}$ is an inverse of a modul.

Example 2.7 If know that $2^{\emptyset(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod{9}$ is an inverse of 2 modulo 9.

2.1.7. The Euler's Totient Function

The Euler's totient function $\emptyset(n)$ is defined as the number of totatives of n. Sometimes the Euler totient function is called Euler's phi function or simply the phi function [5]. It means that the Euler totient function gives a count of how many numbers in the set, $\{1,2,3,\ldots,n\}$ share no common factors with n that are greater than one. Will be soon get in to evaluating the totient [6].

To derive a formula for evaluating, $\emptyset(n)$ will apply the fundamental theorem of arithmetic which says that every natural number greater than one has a unique factorization in terms of prime numbers. I.e., $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, where p_m are the m distinct prime factor of n .

Example 2.8 $n = 30$, its prime factor representation is $2 \times 3 \times 5$ .Likewise for $n = 72$, find it factors into $8 \times 9 = 2^3.3^2$

Now, to find the value of the phi-function at prime.

Theorem 2.2. if n is prime. Then $\emptyset(n) = n - 1$. Conversely, if n is a positive integer with $\emptyset(n) = n - 1$, then n is prime.

To find the value of the phi-function at prime powers.

Theorem 2.3. Let n be a prime and a a positive integer. Then

$$\emptyset(n^a) = n^a - n^{a-1} = n^{a-1}(n-1)$$

Example 2.9 find that $\emptyset(5^3) = 5^3 - 5^2 = 100$, $\emptyset(2^{10}) = 2^{10} - 2^9 = 512$, and

$$\emptyset(11^2) = 11^2 - 11 = 110$$

To find a formula for $\emptyset(n)$, given the prime factorization of, must be shown that $\emptyset$ is multiplicative.

Theorem 2.4. Let m and n be relatively prime positive integers. Then

$$\emptyset(mn) = \emptyset(m)\emptyset(n)$$

Theorem 2.5. Let $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ be the prime-power factorization of the positive integer n. Then

$$\emptyset(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

2.2. Elliptic Curve Arithmetic

Definition: An *elliptic curve E over a field K* is defined by Weirstrass equation [9,10]

$$E : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.2)$$

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

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$$

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1 a_3$$

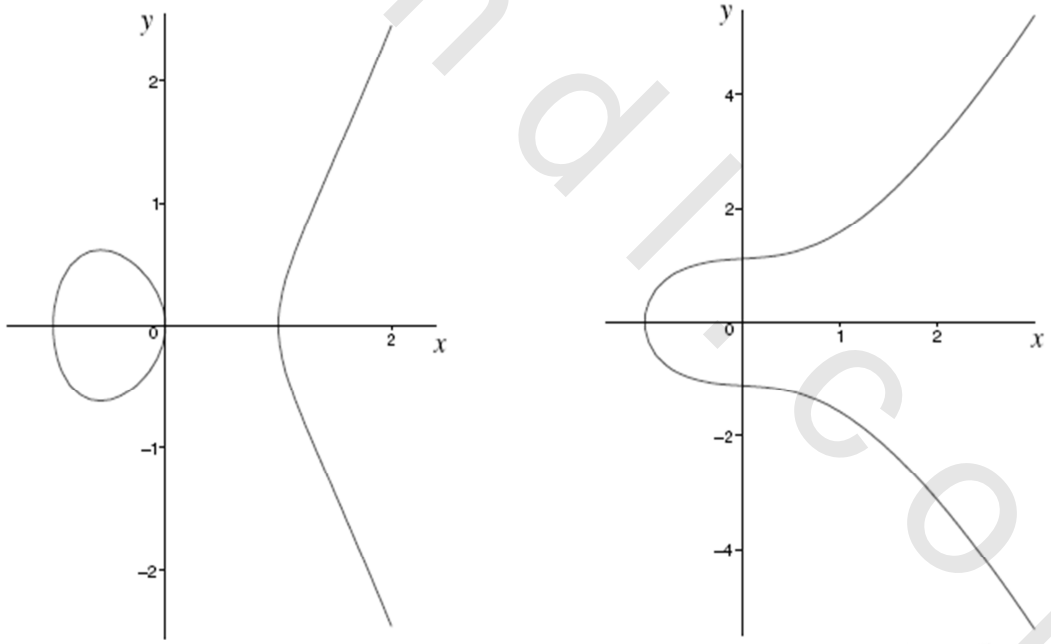
$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_2^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

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

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6 = 0\} \cup \{\infty\}$$

where ∞ is the *point at infinity*.



(a) $E_1 : y^2 = x^3 - x$ (b) $E_2 : y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$

Figure 2.1. Elliptic curves over $\mathbb{R}$

2.2.1. Simplified Weierstrass Equations

Definition: Two elliptic curves E_1 and E_2 defined over K and given by the Weierstrass equations [9]

$$E_1 : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6$$

$$E_2 : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6$$

are said to be *isomorphic over* K if there exist $u, r, s, t \in K, u \neq 0$, such that the change of variables

$$(x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t)$$

transforms equation E_1 into equation E_2. The transformation is called an *admissible change of variables*.

A Weierstrass equation

$$E : y^2 + a_1xy + a_3 y = x^3 + a_2x^2 + a_4x + a_6 \qquad (2.3)$$

defined over K can be simplified considerably by applying admissible changes of variables.

Consider separately the cases where the underlying field K has characteristic different from 2 and 3, or has characteristic equal to 2 or 3.

1. If the characteristic of K is not equal to 2 or 3, then the admissible change of variables

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right)$$

transforms E to the curve

$$y^2 = x^3 + ax + b$$

where $a, b \in K$. The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$.

2. If the characteristic of K is 2, then there are two cases to consider. If $a_1 = 0$, then the admissible change of variables

$$(x, y) \rightarrow \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)$$

transforms E to the curve

$$y^2 + xy = x^3 + ax^2 + b$$

where $a, b \in K$. Such a curve is said to be *non-supersingular* and has discriminant $\Delta = b$ If $a_1 = 0$, then the admissible change of variables

$$(x, y) \rightarrow (x + a_2, y)$$

transforms E to the curve

$$y^2 + cy = x^3 + ax + b$$

where $a, b, c \in K$. Such a curve is said to be *supersingular* and has discriminant $\Delta = c^4$

3. If the characteristic of K is 3, then there are two cases to consider. If $a_1^2 \neq -a_2$ then the admissible change of variables

$$(x, y) \rightarrow (x + \frac{d_4}{d_2}, y + a_1 x + a_1 \frac{d_4}{d_2} + a_3)$$

where $d_2 = a_1^2 + a_2$ and $d_4 = a_4 - a_1 a_3$, transforms E to the curve

$$y^2 = x^3 + ax^2 + b$$

where $a, b \in K$. Such a curve is said to be *non-supersingular* and has discriminant $\Delta = -a^3 b$. If $a_1^2 = -a_2$, then the admissible change of variables

$$(x, y) \rightarrow (x, y + a_1 x + a_3)$$

transforms E to the curve

$$y^2 = x^3 + ax + b$$

where $a, b \in K$. Such a curve is said to be *supersingular* and has discriminant $\Delta = -a^3$

2.2.2. Abelian Groups

An abelian group $(G,*)$ consists of a set G with a binary operation $*: G \times G \rightarrow G$ satisfying the following properties:

- ***Associativity*:** $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
- ***Existence of an identity*:** There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
- ***Existence of inverses:*** For each a ∈ G, there exists an element $b \in G$, called the inverse of a, such that $a * b = b * a = e$.
- ***Commutativity*:** $a * b = b * a$ for all $a, b \in G$.

the group operation is usually called addition (+) or multiplication (·). In the first instance, the group is called an *additive* group, the (additive) identity element is usually denoted by 0, and the (additive) inverse of a is denoted by $-a$. In the second instance, the group is called a *multiplicative* group, the (multiplicative) identity element is usually denoted by 1, and the (multiplicative) inverse of *a* is denoted by $a - 1$. The group is *finite* if G is a finite set, in which case the number of elements in G is called the *order* of G [11,12].

2.2.3. Group Law

Let p be a prime number, and let F_p denote the field of integers modulo p. An elliptic curve E over F_p is defined by an equation of the form

$$y^2 = x^3 + ax + b \quad (2.4)$$

where $a, b \in F_p$ satisfy $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$. A pair (x, y), where $x, y \in F_p$, is a point on the curve if (x, y) satisfies the equation (2.4). The point at infinity, denoted by ∞, is also said to be on the curve. The set of all the points on E is denoted by $E(F_p)$ [9,13]

for example, if E is an elliptic curve over F_7 with defining equation

$$y^2 = x^3 + 2x + 4$$

then the points on E are

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

Point Addition

Point addition is the addition of two points J and K on an elliptic curve to obtain another point L on the same elliptic curve [13,14].

i. Geometrical explanation

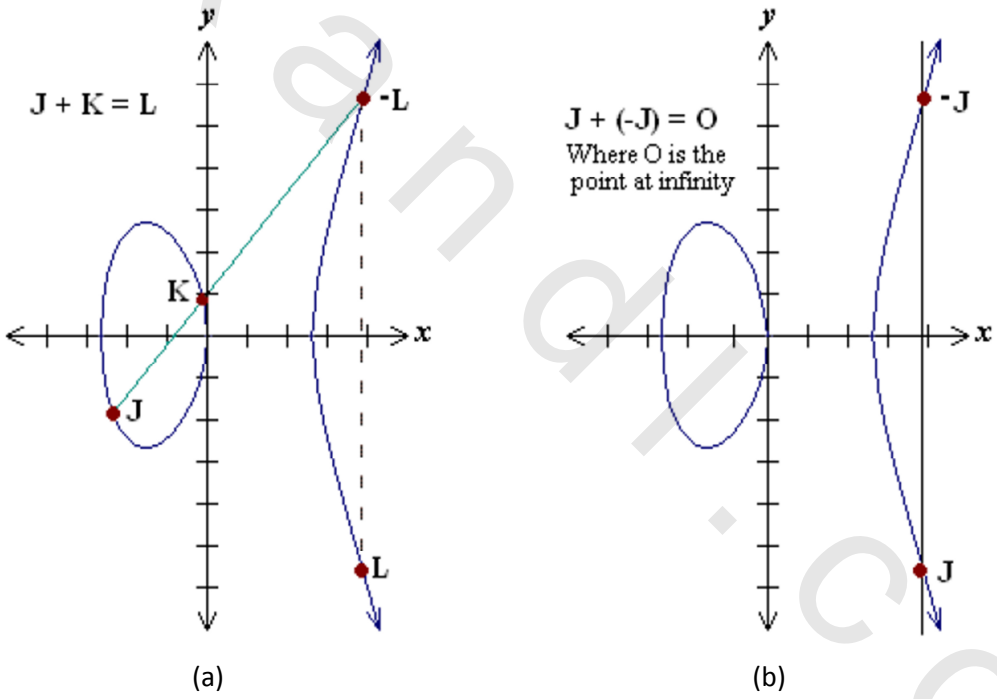


Figure 2.2. Points Addition over Elliptic Curve

Consider two points J = (x_1, y_1) and K = (x_2, y_2) on an elliptic curve as shown in figure (a). If J ≠ ±K then a line drawn through the points J and K will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of addition of points J and K. If J = –K the line through this point intersect at a point at infinity O. Hence J+ (–J) = O. This is shown in figure (b). O is the additive identity of the elliptic curve group. Recall that, a negative of a point is the reflection of that point with respect to x-axis.

ii. Analytical explanation

Let L= J+K where L= (x_3, y_3) and J $\neq \pm$K

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

Point Doubling

Point doubling is the addition of a point J on the elliptic curve to itself to obtain another point L on the same elliptic curve [13,14].

i. Geometrical explanation

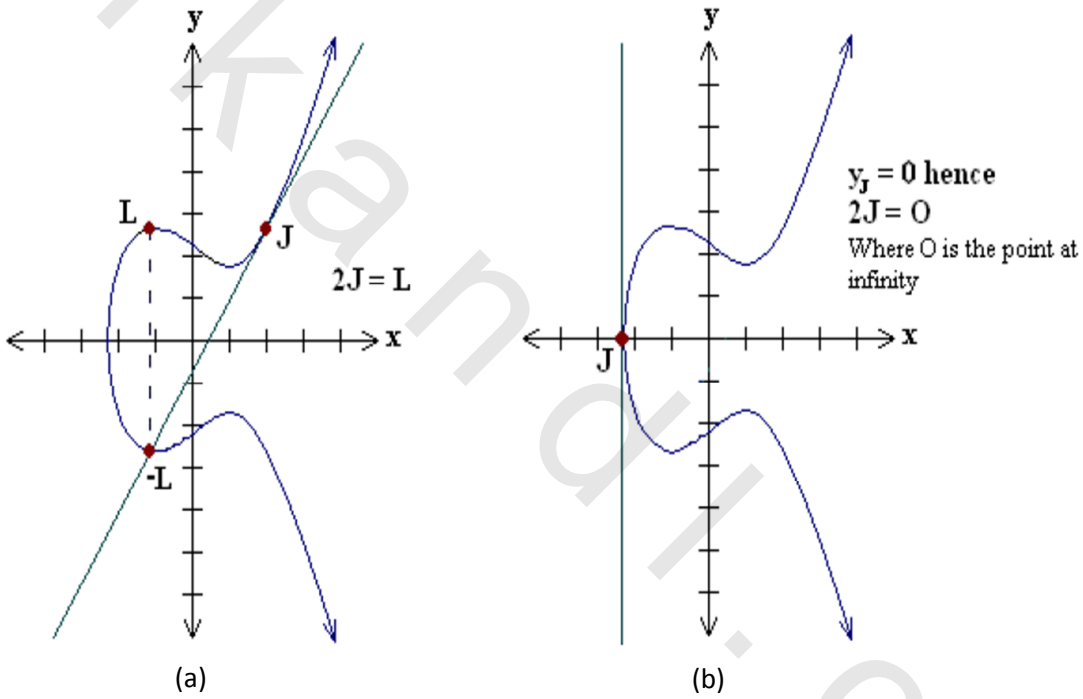


Figure 2.3. Points Doubling over Elliptic Curve

To double a point J to get L, i.e. to find L = 2J, consider a point J on an elliptic curve as shown in figure (a). If y coordinate of the point J is not zero then the tangent line at J will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of doubling the point J.

If y coordinate of the point J is zero then the tangent at this point intersects at a point at infinity O. Hence 2J = O when y_J = 0. This is shown in figure (b).

ii. Analytical explanation

Consider point J= (x_J, y_J), where $y_J \neq 0$, let L=2J

$$x_L = \left(\frac{3x_J^2+a}{2y_J}\right)^2 - 2x_J \qquad y_L = \left(\frac{3x_J^2+a}{2y_J}\right) \times (x_J - x_L) - y_J$$

2.2.4. Finite Fields

The EC operations defined above are on real numbers. Operations over the real numbers are slow and inaccurate due to round-off error. Cryptographic operations need to be faster and accurate. To make operations on EC accurate and more efficient, the curve cryptography is defined over two finite fields [9,10].

- Prime field F_p
- Binary field F_2^m

the field is chosen with finitely large number of points suited for cryptographic operations.

EC on Prime Field F_p

The equation of the elliptic curve on a prime field $F_p$is

$$y^2 \ (mod\ p) = x^3 + ax + b\ (mod\ p)$$

where $4a^3 + 27b^2\ mod\ p \neq 0$. Here the elements of the finite field are integers between 0 and $p - 1$. All the operations such as addition, substation, division, multiplication involves integers between 0 and p – 1. The prime number p is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure. SEC specifies curves with p ranging between 112-521 bits.

EC on Binary field F_2^m

The equation of the elliptic curve on a binary field F_2^m is

$$y^2 + xy = x^3 + ax^2 + b$$

where b ≠ 0. Here the elements of the finite field are integers of length at most m bits. These numbers can be considered as a binary polynomial of degree $m - 1$. In binary polynomial the coefficients can only be 0 or 1. All the operation such as addition, substation, division, multiplication involves polynomials of degree $m - 1$ or lesser. The m is chosen such that there is finitely large number of points on the elliptic curve to make the cryptosystem secure. Securities & Exchange Commission (SEC) specifies curves with m ranging between 113-571 bits.

2.2.5. EC Domain Parameters

A part from the curve parameters a and b, there are other parameters that must be agreed by both parties involved in secured and trusted communication using Elliptic Curve Cryptography (ECC), these are domain parameters. The domain parameters for prime

fields and binary fields are described below. The generation of domain parameters is out of scope of this paper. There are several standard domain parameters defined by SEC, Standards for Efficient Cryptography, produced in 2000 [18,19]. Generally the protocols implementing the ECC specify the domain parameters to be used [11,12,13,14].

Domain parameters for EC over field F_p

The domain parameters for EC over F_P are p, a, b, G, n and h. p is the prime number defined for finite field F_P . a and b are the parameters defining the curve $y^2\ (mod\ p) = x^3 + ax + b\ (mod\ p)$. G is the generator point (x_G, y_G), a point on the EC chosen for cryptographic operations. n is the order of the EC. The scalar for point multiplication is chosen as a number between 0 and $n - 1$. h is the cofactor where $h = \#E(F_P)/n.\#E(F_P)$ is the number of points on an EC.

Domain parameters for EC over field F_2^m

The domain parameters for EC over F_2^m are $m, f(x), a, b, G, n$ and $h.m$ is an integer defined for finite field F_2^m . The elements of the finite field F_2^m are integers of length at most m bits. $f(x)$ is the irreducible polynomial of degree m used for EC operations. a and b are the parameters defining the curve $y^2 + xy = x^3 + ax^2 + b$. G is the generator point (x_G, y_G), a point on the EC chosen for cryptographic operations. n is the order of the EC. The scalar for point multiplication is chosen as a number between 0 and $n - 1$. h is the cofactor where $h = \#E(F_2^m)/n.\#E(F_2^m)$ is the number of points on an EC.