ELLIPTIC CURVE PRIMALITY TESTS

by

Ali Rıza ÖZTEK

August 2006

ELLIPTIC CURVE PRIMALITY TESTS

by

Ali Rıza ÖZTEK

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 Şahin
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. Barış Kendirli
Supervisor

Examining Committee Members

Prof. Barış Kendirli _____

Assist. Prof. Tevfik Bilgin _____

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

Date
August 2006

ELLIPTIC CURVE PRIMALITY TESTS

Ali Rıza ÖZTEK

M. S. Thesis - Mathematics
August 2006

Supervisor: Prof. Dr. Barış KENDİRLİ

ABSTRACT

In this thesis, mainly primality tests are analyzed. Large integers have great importance especially in cryptography. Some deterministic and probabilistic primality tests will be examined in order to test primality of large integers. Recently, a lot of studies have been done on elliptic curves. One of the applications of elliptic curves is elliptic curve primality tests. Goldwasser and Kilian developed an algorithm which uses the group of rational points of elliptic curves over finite fields. Atkin and Morain extended the idea of Goldwasser and Kilian and used the elliptic curves with complex multiplication to obtain a more efficient algorithm.

Keywords: Finite Fields, Primality tests, Elliptic Curves, Cryptography.

ELİPTİK EĞRİ ASALLIK TESTLERİ

Ali Rıza ÖZTEK

Yüksek Lisans Tezi – Matematik
Ağustos 2006

Tez Yöneticisi: Prof. Dr. Barış Kendirli

ÖZ

Bu tezde asıl konu asallık testlerinin analizidir. Çok büyük tam sayıların özellikle kriptografideki çok önemli yeri vardır. Çok büyük tam sayıları test etmek için bazı gerçekçi ve olasılıksal asallık testleri incelenecek. Son yıllarda eliptik eğriler üzerine birçok çalışmalar yapılmaktadır. Eliptik eğrilerin uygulandığı alanlardan biri eliptik eğri asallık testleridir. Goldwasser ve Kilian sonlu cisimler üzerinde eliptik eğrilerin kullanıldığı asallık test algoritmaları geliştirmişlerdir. Atkin ve Morain bu testi geliştirerek kompleks sayılar üzerindeki eliptk eğrileri kullanarak daha güçlü bir algoritma geliştirmişlerdir.

Anahtar Kelimeler: Sonlu Cisimler, Asallık Testleri, Eliptik Eğriler, Kriptografi.

DEDICATION

This thesis is dedicated to my parents.

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 for their valuable suggestions and comments. I express my thanks and appreciation to my family for their understanding, motivation and patience. Lastly, but in no sense the least, I am thankful to all colleagues and friends who made my stay at the university a memorable and valuable experience.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF SYMBOLS AND ABBREVIATIONS

ABBREVIATION

EC	Elliptic Curve
ECPP	Elliptic Curve Primality Proving
GK	Goldwasser and Kilian
CM	Complex Multiplication

CHAPTER 1

INTRODUCTION

Positive integers greater than 1 can be classified as either a *prime number* or a *composite number*. If a positive integer greater than 1 has no positive factors other than 1 and itself is called a prime number. Prime numbers have great importance in abstract algebra. Many mathematicians tried to find mysterious properties of prime numbers for centuries. Prime numbers and their properties were first studied extensively by the Greek mathematicians especially by Eratosthenes and Euclid.

Primality tests are the tests to distinguish prime numbers from composite numbers. A technique known as the *sieve of Eratosthenes* represents a reasonable method for obtaining a complete list of primes less than or equal to n where n is a relatively small value. Nowadays, the importance of data security is increasing. We need big prime numbers to make codes to secure our data. These codes should not be easily broken. The time is very important while checking a large integer is prime or not. In the last decades, computer technology is developing very fast. Therefore data processing time is decreasing day by day. The Sieve of Eratosthenes is not good algorithm to find big primes. Fermat's Little Theorem is the basis for methods of checking whether numbers are prime which are still in use on today's computers. Using the extended ideas of Fermat's theorem, Sollovay and Strassen, and Miller and Rabin developed probabilistic primality tests.

An elliptic curve is a mathematical object which is defined over a field. Elliptic curves have become very popular subject in recent years. For example, Wiles used elliptic curves to prove Fermat's Last Theorem. Moreover, elliptic curves are being used in cryptography. In 1985, H. W. Lenstra introduced the usage of elliptic curves in factorization of integers. After that Goldwasser and Kilian developed an algorithm with the hope of finding a primality test with the help of groups of rational points of elliptic curves over finite fields. The major difficulty in the Elliptic curve primality proving

algorithm of Goldwasser & Kilian is to find the size of the group of rational points of elliptic curves by means of the theoretical algorithms due to Schoof. Although, some progress has been made in the direction of making Schoof's algorithm practical by Atkin, Atkin and Morain have found a better idea. They used elliptic curves with complex multiplication instead of using randomly chosen elliptic curves.

In this thesis, elementary number theory and some abstract algebra topic will be overviewed and then elliptic curves and some important primality tests will be explained.

CHAPTER 2

ELEMENTS OF NUMBER THEORY AND ABSTRACT ALGEBRA

2.1 DIVISIBILITY PROPERTIES OF INTEGERS

2.1.1 Prime and Composite Integers

An integer p which is greater than 1 is prime if it has only two positive factors 1 and itself. Otherwise, it is composite. Note that 1 is neither prime nor composite.

Example 2.1 29 is a prime number. Because the only positive factors of 29 are 1 and 29.

Every integer n greater than 1 can be expressed as a product of primes. It can be uniquely expressed in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i are primes and e_i are positive integers. This is called the *Fundamental Theorem of Arithmetic*.

Example 2.2 The positive integer 3500 can be factorized uniquely such that

$$3500 = 2^2.5^3.7$$

Theorem 2.1 There are infinitely many prime numbers.

Proof: Assume that there are finitely many prime numbers. Let these numbers be $p_1, p_2, p_3, \ldots, p_n$ and let p_n be the largest prime. Consider the integer

$$M = p_1.p_2.p_3 \ldots p_n + 1$$

So M is not divisible by any of the p_i. If M is not a prime number, it must have a prime factor. Hence, either M has prime factors which are greater than p_n or M is a prime

number itself. This contradicts with our assumption. Therefore there are infinitely many prime numbers.

Theorem 2.2. (Prime Number Theorem) Let π(x) denote the number of prime numbers less than or equal to x, then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Table 2.1 indicates the validity of the Prime Number Theorem.

Table 2.1 Prime Number Theorem

x	π(x)	x/lnx	π(x).lnx/x
100	25	22	1.151
1000	168	145	1.159
10000	1229	1086	1.132
100000	9592	8686	1.104
1000000	78498	72382	1.084
10000000	664579	620421	1.071
100000000	5761455	5428681	1.061

2.1.2 The Greatest Common Divisor

Let a, b be at least one of them nonzero integers and k is a positive integer. If $k|a$ and $k|b$, then k is called a *common divisor* of a and b. The largest positive integer g that divides the absolute values of each of two integers a and b is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by *(a, b)*.

$(a_1, a_2, \ldots, a_n)$ denotes the greatest common divisor of integers a_1, a_2, …, a_n, which are not all zero.

Example 2.3 The greatest common divisor of 18 and 45 is 9

(18, 45)= 9

Example 2.4 The greatest common divisor of 12, 20, 28 and 36 is 4.

$$(12, 20, 28, 36) = 4$$

If $(a, b) = 1$, then a, b are relatively prime.

If $(a_1, a_2, \ldots, a_n) = 1$, then a_1, a_2, …, a_n are relatively prime.

If $(a_i, a_j) = 1$ for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$ with $i \neq j$, then a_1, a_2, …, a_n are relatively prime in pairs.

Here are some properties of the greatest common divisor:

1. For integers a and b, there exist integers x and y such that $ax + by = (a, b)$.

   For integers a_1, a_2, …, a_n, there exist integers k_i such that

   $$(a_1, a_2, \ldots, a_n) = k_1a_1 + k_2a_2 + \cdots + k_na_n.$$

2. For any positive integer m, $(ma, mb) = m(a, b)$.

3. If $d \mid a$, $d \mid b$ and $d > 0$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$.

   If $(a, b) = g$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

4. If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$.

5. For any x, a and b, we have $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.

6. If $c \mid ab$ and $(b, c) = 1$, then $c \mid a$.

Theorem 2.3. If p is a prime number and $p|ab$, then $p|a$ or $p|b$.

Proof: If $p|a$, then the theorem is proved. If $p \nmid a$, then $(p,a) = 1$. By property 6, it follows that $p|b$.

Theorem 2.4. If $p \mid a_1a_2 \cdots a_n$, then p divides at least one of the a_i.

2.1.3 Euclidean Algorithm

To find the greatest common divisor of large numbers is not easy. In such cases, we may apply the Euclidean Algorithm. This algorithm makes use of the following fact

If a, b are not both zero, then $(a, b) = (a - bm, b) = (a, b - an)$ for any positive integers m, n. In particular, if $a > b > 0$ and $a = bm + r$, then $(a, b) = (r, b)$.

Let $a > b > 0$ and

$$\begin{aligned} a &= bq + r_1 & 0 \le r_1 < b \\ b &= r_1 q_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2 \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1} \\ r_{n-1} &= r_n q_n \end{aligned}$$

Then $(a, b) = r_n$. We can also write $r_n = (a, b) = xa + by$ by eliminating r_{n-1}, …, r_2, r_1 from the above equations.

Example 2.5 Let a = 91 and b = 35. Then

$$91 = 2.35 + 21$$
$$35 = 1.21 + 14$$
$$21 = 1.14 + 7$$
$$14 = 2.7$$

Thus (91, 35) = 7. Moreover,

$$7 = 21 - 14$$
$$7 = 21 - (35 - 21) = 2.21 - 35$$
$$7 = 2(91 - 2.35) - 35 = 2.91 - 5.35$$
$$7 = 2.91 - 5.35$$

2.2 CONGRUENCES

If an integer k ($k \neq 0$) divides $a - b$, then a is congruent to b modulo m and we write

$$a \equiv b \pmod{m}.$$

If k does not divided $a - b$, then a is not congruent to b modulo m and we write

$$a \not\equiv b \pmod{m}.$$

Example 2.6

We say that $13 \equiv 19 \pmod 3$ because $3 \mid (19 - 13)$.

However, $28 \not\equiv 41 \pmod 3$ because $3 \nmid (41 - 28)$.

2.2.1 Basic Properties

We have the following properties:

1. $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ and $a - b \equiv 0 \pmod{m}$ are equivalent.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ax + by \equiv cx + dy \pmod{m}$.
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
5. If $a \equiv b \pmod{m}$ and $d \mid m$ $(d > 0)$, then $a \equiv b \pmod{d}$.
6. If f is a polynomial with integral coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.
7. $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \left(\mod \frac{m}{(a, m)} \right)$.

   In particular, if $(a, m) = 1$, then $x \equiv y \pmod{m}$.
8. $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, k$ if and only if

   $x \equiv y \pmod{[m_1, m_2, \ldots, m_k]}$.
9. If $x \equiv y \pmod{m}$, then $(x, m) = (y, m)$.

If $x \equiv y \pmod{m}$, then y is called a residue of x modulo m. A set $x_1, x_2, \ldots, x_m$ is called a *complete residue system modulo m* if for every integer y there is one and only one x_i such that $y \equiv x_i \pmod{m}$.

A *reduced residue system modulo m* is a set of integers r, such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m, is congruent modulo m to some member r_i of the set.

Let $(a, m) = 1$. Let $r_1, r_2, \ldots, r_n$ be a complete, or a reduced, residue system modulo m. then $ar_1, ar_2, \ldots, ar_n$ is a complete, or a reduced, residue system, respectively, modulo m.

Example 2.7 12, 37, 166, 999 form a complete residue system modulo 4.

2.2.2 Euler's ϕ-function

For a positive integer *n*, we define $\phi(n)$ to be the number of positive integers less than *n* that are relatively prime to *n*.

Example 2.8 $\phi(10) = 4$ since among the positive integers less than 10, there are 4 of them, namely, 1, 3, 7, 9, which are relatively prime to 10.

Facts:

1. If *p* is a prime number, then $\phi(p^k) = p^k - p^{k-1}$, where *k* is a positive integer.
2. If *a* and *b* are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.
3. If $p_1, p_2, \ldots, p_r$ are all the prime factors of *n*, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Example 2.9

1. $\phi(11^3) = 11^3 - 11^2 = 1210$.
2. Let $a = 8$, $b = 9$. Then *a* and *b* are relatively prime. Thus
   $\phi(72) = \phi(8\times 9) = \phi(8)\phi(9) = \phi(2^3)\phi(3^2) = (2^3 - 2^2)(3^2 - 3^1) = 24$.
3. Let $n = 60$. Then the prime factors of *n* are 2, 3, 5. Thus
   $\phi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$.

2.5 Fermat's Little Theorem

Theorem 2.5 If p is a prime number and *(a,p) = 1*, then $a^{p-1} \equiv 1 \pmod p$

Proof: Claim that the integers *0a, 1a, 2a,……,(p-1)a* are complete residue system modulo p. If *ia = ja mod p* then *p| (j – i)a*. Since *a* is not divisible by *p*, we would have

$p|\ (j - i)$. Since i and j both less than p, the only way this can happen is if $i = j$. We conclude that *1a, 2a,…….,(p-1)a* rearrangement of
1, 2, …..,p-1 when considered modulo p. The product of *1a, 2a,…….,(p-1)a* will be congruent to the product of the numbers in the second sequence.

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$$

Since $p \nmid (p-1)!$, we have $p|\ a^{p-1} - 1$. Therefore $a^{p-1} \equiv 1 \pmod p$

Corollary 2.1 Let p is a prime number and a is any integer, then $a^p = a \bmod p$

Proof: *Case 1*: $p|a$ □ both sides are zero.

Case 2: $p \nmid a$ □ $a^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem (since $(a,p) = 1$). If we multiply both sides by a, we get

$$a.a^{p-1} \equiv a.1 \pmod p \ \square\ a^p = a \pmod p.$$

Theorem 2.6 (Euler's Theorem) For any positive integer n such that $(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod n.$$

Example 2.10

Since 11 is prime and $(8, 11) = 1$, $8^{10} \equiv 1 \pmod{11}$.

Since $\phi(9) = \phi(3^2) = 3^2 - 3^1 = 6$ and $(8, 9) = 1$, $8^6 \equiv 1 \pmod 9$.

2.2.4 Chinese Remainder Theorem

Theorem 2.7 The *Chinese Remainder Theorem* states that if $m_1, m_2, \ldots, m_n$ are pairwise relatively prime integers, the following system of congruences has solution and the solution is unique modulo $m_1 m_2 \cdots m_n$.

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

To find a solution, let $M_j = \dfrac{m_1 m_2 \cdots m_n}{m_j}$. One solution is given by

$$x = M_1^{\phi(m_1)} b_1 + M_2^{\phi(m_2)} b_2 + \cdots + M_n^{\phi(m_n)} b_n$$

Example 2.11 The following system of congruences has solution.

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

The solution is given by

$$x = \left(\frac{2\times 3\times 5}{2}\right)^{\phi(2)} \times 1 + \left(\frac{2\times 3\times 5}{3}\right)^{\phi(3)} \times 2 + \left(\frac{2\times 3\times 5}{5}\right)^{\phi(5)} \times 3 = 6803$$

Since $6803 \equiv 23 \pmod{2\times 3\times 5}$, any number which is congruent to 23 modulo 30 is a solution to the system.

2.3 GROUP THEORY

In mathematics, a group is a set, together with a binary operation, such as multiplication or addition, satisfying certain axioms, detailed below. For example, the set of integers is a group under the operation of addition. The branch of mathematics which studies groups is called group theory.

The historical origin of group theory goes back to the works of Evariste Galois (1830), concerning the problem of when an algebraic equation is soluble by radicals. Previous to this work, groups were mainly studied concretely, in the form of permutations; some aspects of abelian group theory were known in the theory of quadratic forms.

A great many of the objects investigated in mathematics turn out to be groups. These include familiar number systems, such as the integers, the rational numbers, the real numbers, and the complex numbers under addition, as well as the non-zero rationals, reals, and complex numbers, under multiplication. Another important example is given by non-singular matrices under multiplication, and more generally, invertible functions under composition. Group theory allows for the properties of these systems and many others to be investigated in a more general setting, and its results are widely applicable. Group theory is also a rich source of theorems in its own right.

Groups underlie many other algebraic structures such as fields and vector spaces. They are also important tools for studying symmetry in all its forms; the principle that the symmetries of any object form a group is foundational for much mathematics. For

these reasons, group theory is an important area in modern mathematics, and also one with many applications to mathematical physics (for example, in particle physics).

2.3.1 Basic Definitions

A group (G, *) is a nonempty set G together with a binary operation * : G × G → G, satisfying the group axioms. "a * b" represents the result of applying the operation * to the ordered pair (a, b) of elements of G. The group axioms are the following:

1. *Closure:* For all a and b in G, a * b belongs to G.
2. *Associativity:* For all a, b and c in G, (a * b) * c = a * (b * c).
3. *Identity element:* There is an element e in G such that for all a in G, e * a = a * e = a.
4. *Inverse element:* For all a in G, there is an element b in G such that a * b = b * a = e, where e is the identity element from the previous axiom.

The way that the definition above is phrased, this axiom is not necessary, since binary operations are already required to satisfy closure. When determining if * is a group operation, however, it is nonetheless necessary to verify that * satisfies closure; this is part of verifying that it is in fact a binary operation.

It should be noted that there is no requirement that the group operation be commutative, that is there may exist elements such that a * b ≠ b * a. A group G is said to be abelian (after the mathematician Niels Abel) (or commutative) if for every a, b in G, a * b = b * a. Groups lacking this property are called non-abelian.

The order of a group G, denoted by |G| or o(G), is the number of elements of the set G. A group is called finite if it has finitely many elements, that is if the set G is a finite set.

We often refer to the group (G, *) as simply "G", leaving the operation * unmentioned. But to be perfectly precise, different operations on the same set define different groups.

2.3.2 Notation for groups

Usually the operation, whatever it really is, is thought of as an analogue of multiplication, and the group operations are therefore written multiplicatively. That is:

- We write "a • b" or even "ab" for a * b and call it the product of a and b;

- We write "1" for the identity element and call it the unit element;
- We write "a^{-1}" for the inverse of a and call it the reciprocal of a.

However, sometimes the group operation is thought of as analogous to addition and written additively:

- We write "a + b" for a * b and call it the sum of a and b;
- We write "0" for the identity element and call it the zero element;
- We write "−a" for the inverse of a and call it the opposite of a.

Usually, only abelian groups are written additively, although abelian groups may also be written multiplicatively. When being noncommittal, one can use the notation (with "*") and terminology that was introduced in the definition, using the notation a^{-1} for the inverse of a.

If S is a subset of G and x an element of G, then, in multiplicative notation, xS is the set of all products {xs : s in S}; similarly the notation Sx = {sx : s in S}; and for two subsets S and T of G, we write ST for {st : s in S, t in T}. In additive notation, we write x + S, S + x, and S + T for the respective sets.

Example 2.12 An abelian group is the integers under addition.

For this example, let Z be the set of integers, {..., −4, −3, −2, −1, 0, 1, 2, 3, 4, ...}, and let the symbol "+" indicate the operation of addition. Then (Z,+) is a group (written additively).

Proof:

- If a and b are integers then a + b is an integer. (Closure; + really is a binary operation)
- If a, b, and c are integers, then (a + b) + c = a + (b + c). (Associativity)
- 0 is an integer and for any integer a, 0 + a = a + 0 = a. (Identity element)
- If a is an integer, then there is an integer b := −a, such that a + b = b + a = 0. (Inverse element)

This group is also abelian: a + b = b + a.

The integers with both addition and multiplication together form the more complicated algebraic structure of a ring. In fact, the elements of any ring form an abelian group under addition, called the additive group of the ring.

Example 2.13 The integers under multiplication is not a group.

On the other hand, if we consider the operation of multiplication, denoted by "•", then (Z,•) is not a group.

Proof:

- If a and b are integers then a • b is an integer. (Closure)
- If a, b, and c are integers, then (a • b) • c = a • (b • c). (Associativity)
- 1 is an integer and for any integer a, 1 • a = a • 1 = a. (Identity element)
- However, it is not true that whenever a is an integer, there is an integer b such that ab = ba = 1. For example, a = 2 is a integer, but the only solution to the equation ab = 1 in this case is b = 1/2. We cannot choose b = 1/2 because 1/2 is not an integer. (Inverse element fails)

Since not every element of (Z,•) has an inverse, (Z,•) is not a group. The most we can say is that it is a commutative monoid.

Example 2.14 An abelian group: the nonzero rational numbers under multiplication

Consider the set of rational numbers Q, that is the set of numbers a/b such that a and b are integers and b is nonzero, and the operation multiplication, denoted by "•". Since the rational number 0 does not have a multiplicative inverse, (Q,•), like (Z,•), is not a group.

However, if we instead use the set Q \ {0} instead of Q, that is include every rational number except zero, then (Q \ {0},•) does form an abelian group (written multiplicatively). The inverse of a/b is b/a, and the other group axioms are simple to check. We don't lose closure by removing zero, because the product of two nonzero rationals is never zero.

Just as the integers form a ring, so the rational numbers form the algebraic structure of a field. In fact, the nonzero elements of any given field form a group under multiplication, called the multiplicative group of the field.

2.3.3 Theorems

Theorem 2.8 A group has exactly one identity element.

Theorem 2.9 Every element has exactly one inverse.

Theorem 2.10 The inverse of a product is the product of the inverses in the opposite order: $(a * b)^{-1} = b^{-1} * a^{-1}$

.

2.4 RING THEORY

2.4.1 Ring Theory

In mathematics, a ring is an algebraic structure in which addition and multiplication are defined and have similar (but not identical) properties to those familiar from the integers. The branch of abstract algebra which studies rings is called ring theory.

Definition 2.1 A ring is a set R equipped with two binary operations + and •, called addition and multiplication, such that:

1. (R, +) is an abelian group with identity element 0:
   a. (a + b) + c = a + (b + c)
   b. a + b = b + a
   c. 0 + a = a + 0 = a
   d. □a □(−a) such that a + −a = −a + a = 0
2. (R, •) is a monoid with identity element 1:
   a. 1•a = a•1 = a
   b. (a•b)•c = a•(b•c)
3. Multiplication distributes over addition:
   a. a•(b + c) = (a•b) + (a•c)
   b. (a + b)•c = (a•c) + (b•c)

As with groups the symbol • is usually omitted. Also the standard order of operation rules are used, so that e.g. a+bc is an abbreviation for a+(b•c).

Although ring addition is commutative (i.e. a+b = b+a), note that the commutativity for multiplication (a•b = b•a) is not among the ring axioms listed above. Rings that also satisfy commutativity for multiplication (such as the ring of integers) are called commutative rings. Not all rings are commutative.

Also note that an element of a ring need not have a multiplicative inverse. An element a in a ring is called a unit if it is invertible with respect to multiplication, i.e., if there is an element b in the ring such that a•b = b•a = 1. If that is the case, then b is uniquely determined by a and we write $a^{-1} = b$. The set of all units in R forms a group under ring multiplication; this group is denoted by U(R).

Example 2.15 The ring of integers with the two operations of addition and multiplication. This is a commutative ring.

Example 2.16 The rational, real and complex numbers form rings (in fact, they are even fields). These are likewise commutative rings.

More generally, every field is a commutative ring. If n is a positive integer, then the set Z/nZ of integers modulo n forms a ring with n elements.The set of all continuous real-valued functions defined on the interval [a, b] forms a ring (even an associative algebra). The operations are addition and multiplication of functions. The set of all polynomials over some common coefficient ring forms a ring. For any ring R and any natural number n, the set of all square n-by-n matrices with entries from R, forms a ring with matrix addition and matrix multiplication as operations. For n=1, this matrix ring is just (isomorphic to) R itself. For n>2, this matrix ring is an example of a noncommutative ring (unless R is the trivial ring). The trivial ring {0} has only one element which serves both as additive and multiplicative identity.

Theorem 2.11 From the axioms, one can immediately deduce that, for all elements a and b of a ring, we have

- 0a = a0 = 0
- (−1)a = −a
- (−a)b = a(−b) = −(ab)
- (ab)−1 = b−1 a−1 if both a and b are invertible

2.4.2 Constructing new rings from given ones

If a subset S of a ring R is itself a ring with the same operations (restricted to S), and the identity element 1 of R is contained in S, then S is called a subring of R.

The center of a ring R is the set of elements of R that commute with every element of R; that is, c lies in the center if cr=rc for every r in R. The center is a subring of R. We say that a subring S of R is central if it is a subring of the center of R.

The direct sum of two rings R and S is the cartesian product R×S together with the operations

$(r_1, s_1) + (r_2, s_2) = (r_1+r_2 , s_1+s_2)$ and

$(r_1, s_1)\ (r_2, s_2) = (r_1r_2 , s_1s_2)$

Given a ring R and an ideal I of R, the quotient ring (or factor ring) R/I is the set of cosets of I together with the operations

$(a+I) + (b+I) = (a+b) + I$ and

$(a+I)(b+I) = (ab) + I$.

Since any ring is both a left and right module over itself, it is possible to construct the tensor product of R over a ring S with another ring T to get another ring provided S is a central subring of R and T.

2.5 INTEGRAL DOMAIN

2.5.1 Integral Domain

In abstract algebra, an integral domain is a commutative ring with $0 \neq 1$ in which the product of any two non-zero elements is always non-zero; that is, there are no zero divisors. Integral domains are generalizations of the integers and provide a natural setting for studying divisibility.

Alternatively and equivalently, integral domains may be defined as commutative rings in which the zero ideal {0} is prime, or as the subrings of fields. Viewing the underlying commutative ring as a categorical construction, the previous criterion on zero divisors is equivalent to the condition that every nonzero morphism is a monomorphism (hence also an epimorphism).

The condition $0 \neq 1$ only serves to exclude the trivial ring {0} with a single element.

Example 2.17 The ring Z of all integers.

Example 2.18 Every field is an integral domain. Conversely, every Artinian integral domain is a field. In particular, the only finite integral domains are the finite fields.

Example 2.19 Rings of polynomials are integral domains if the coefficients come from an integral domain. For instance, the ring Z[X] of all polynomials in one variable with integer coefficients is an integral domain; so is the ring R[X,Y] of all polynomials in two variables with real coefficients.

Example 2.20 The set of all real numbers of the form a + b$\sqrt{2}$ with a and b integers is a subring of R and hence an integral domain. A similar example is given by the complex numbers of the form a + bi with a and b integers (the Gaussian integers).

Example 2.21 The p-adic integers.

Example 2.22 If U is a connected open subset of the complex number plane C, then the ring H(U) consisting of all holomorphic functions f : U → C is an integral domain. The same is true for rings of analytical functions on connected open subsets of analytical manifolds.

Example 2.23 If R is a commutative ring and P is an ideal in R, then the factor ring R/P is an integral domain if and only if P is a prime ideal.

2.5.2 Divisibility, prime and irreducible elements

If a and b are elements of the integral domain R, we say that a divides b or a is a divisor of b or b is a multiple of a if and only if there exists an element x in R such that ax = b.

If a divides b and b divides c, then a divides c. If a divides b, then a divides every multiple of b. If a divides two elements, then a also divides their sum and difference.

The elements which divide 1 are called the units of R; these are precisely the invertible elements in R. Units divide all other elements.

If a divides b and b divides a, then we say a and b are associated elements. a and b are associated if and only if there exists a unit u such that au = b.

If q is a non-unit, we say that q is an irreducible element if q cannot be written as a product of two non-units.

If p is a non-zero non-unit, we say that p is a prime element if, whenever p divides a product ab, then p divides a or b.

This generalizes the ordinary definition of prime number in the ring Z, except that it allows for negative prime elements. If p is a prime element, then the principal ideal (p) generated by p is a prime ideal. Every prime element is irreducible (here, for the first time, we need R to be an integral domain), but the converse is not true in all integral domains (it is true in unique factorization domains, however).

2.5.3 Field of fractions

If R is a given integral domain, the smallest field Quot(R) containing R as a subring is uniquely determined up to isomorphism and is called the field of fractions or quotient field of R. It consists of all fractions a/b with a and b in R and $b \neq 0$, modulo an appropriate equivalence relation. The field of fractions of the integers is the field of rational numbers. The field of fractions of a field is isomorphic to the field itself.

2.5.4 Characteristic and homomorphisms

The characteristic of every integral domain is either zero or a prime number.

If R is an integral domain with prime characteristic p, then f(x) = x p defines an injective ring homomorphism $f : R \rightarrow R$, the Frobenius homomorphism.

2.6 FIELDS

In abstract algebra, a field is an algebraic structure in which the operations of addition, subtraction, multiplication and division (except division by zero) may be performed, and the same rules hold which are familiar from the arithmetic of ordinary numbers.

2.6.1 Introduction to fields

Fields are important objects of study in algebra since they provide a useful generalization of many number systems, such as the rational numbers, real numbers, and complex numbers. In particular, the usual rules of associativity, commutativity and

distributivity hold. Fields also appear in many other areas of mathematics; see the examples below.

When abstract algebra was first being developed, the definition of a field usually did not include commutativity of multiplication, and what we today call a field would have been called either a commutative field or a rational domain. In contemporary usage, a field is always commutative. A structure which satisfies all the properties of a field except for commutativity, is today called a division ring or sometimes a skew field, but also non-commutative field is still widely used.

The concept of a field is of use, for example, in defining vectors and matrices, two structures in linear algebra whose components can be elements of an arbitrary field. Galois Theory studies the symmetry of equations by investigating the ways in which fields can be contained in each other.

Definition 2.2 A field is a commutative ring (F, +, *) such that 0 does not equal 1 and all elements of F except 0 have a multiplicative inverse.

This means that the following hold:

1. Closure of F under + and *
2. For all a, b belonging to F, both a + b and a * b belong to F (or more formally, + and * are binary operations on F).
3. Both + and * are associative
4. For all a, b, c in F, a + (b + c) = (a + b) + c and a * (b * c) = (a * b) * c.
5. Both + and * are commutative
6. For all a, b belonging to F, a + b = b + a and a * b = b * a.
7. The operation * is distributive over the operation +
8. For all a, b, c, belonging to F, a * (b + c) = (a * b) + (a * c).
9. Existence of an additive identity
10. There exists an element 0 in F, such that for all a belonging to F, a + 0 = a.
11. Existence of a multiplicative identity
12. There exists an element 1 in F different from 0, such that for all a belonging to F, a * 1 = a.
13. Existence of additive inverses
14. For every a belonging to F, there exists an element −a in F, such that a + (−a) = 0.

15. Existence of multiplicative inverses
16. For every $a \neq 0$ belonging to F, there exists an element a^{-1} in F, such that $a * a^{-1} = 1$.

The requirement $0 \neq 1$ ensures that the set which only contains a single element is not a field. Directly from the axioms, one may show that (F, +) and (F − {0}, *) are commutative groups (abelian groups) and that therefore (see elementary group theory) the additive inverse −a and the multiplicative inverse a−1 are uniquely determined by a. Furthermore, the multiplicative inverse of a product is equal to the product of the inverses:

$$(a*b)^{-1} = b^{-1} * a^{-1} = a^{-1} * b^{-1}$$

provided both a and b are non-zero. Other useful rules include

$$-a = (-1) * a$$

and more generally

$$-(a * b) = (-a) * b = a * (-b)$$

as well as

$$a * 0 = 0,$$

If the requirement of commutativity of the operation * is dropped, one distinguishes the above commutative fields from non-commutative fields, usually called division rings or skew field.

Example 2.24 The complex numbers C, under the usual operations of addition and multiplication. The field of complex numbers contains the following subfields (a subfield of a field F is a set containing 0 and 1, closed under the operations + and * of F and with its own operations defined by restriction):

Example 2.25 The rational numbers $Q = \{ a/b \mid a, b \text{ in } Z, b \neq 0 \}$ where Z is the set of integers. The rational number field contains no proper subfields.

Example 2.26 An algebraic number field is a finite field extension of the rational numbers Q, that is, a field containing Q which has finite dimension as a vector space over Q. Such fields are very important in number theory.

Example 2.27 The field of algebraic numbers, the algebraic closure of Q.

Example 2.28 The real numbers R, under the usual operations of addition and multiplication. When the real numbers are given the usual ordering, they form a complete ordered field which is categorical — it is this structure that provides the foundation for most formal treatments of calculus.

Example 2.29 The real numbers contain several interesting subfields: the real algebraic numbers, the computable numbers, and the definable numbers.

2.6.2 Galois Field

If $q > 1$ is a power of a prime number, then there exists (up to isomorphism) exactly one finite field with q elements, usually denoted F_q, Z/qZ, or GF(q). Every other finite field is isomorphic to one of these fields. Such fields are often called a Galois field, whence the notation GF(q).

In particular, for a given prime number p, the set of integers modulo p is a finite field with p elements: $Fp = \{0, 1, ..., p - 1\}$ where the operations are defined by performing the operation in Z, dividing by p and taking the remainder; see modular arithmetic.

Taking p = 2, we obtain the smallest field, F_2, which has only two elements: 0 and 1. It can be defined by the two Cayley tables

Table 2.2 Cayley Tables

+	**0**	**1**
0	0	1
1	1	0

*	**0**	**1**
0	0	0
1	0	1

This field has important uses in computer science, especially in cryptography and coding theory.

The rational numbers can be extended to the fields of p-adic numbers for every prime number p. These fields are very important in both number theory and mathematical analysis.

Let E and F be two fields with E a subfield of F. Let x be an element of F not in E. Then E(x) is defined to be the smallest subfield of F containing E and x. We call E(x) a simple extension of E. For instance, Q(i) is the number field of complex numbers C consisting of all numbers of the form a + bi where both a and b are rational numbers. In fact, it can be shown that every number field is a simple extension of Q.

For a given field F, the set F(X) of rational functions in the variable X with coefficients in F is a field; this is defined as the set of quotients of polynomials with coefficients in F. This is the simplest example of a transcendental extension.

If F is a field, and p(X) is an irreducible polynomial in the polynomial ring F[X], then the quotient F[X]/<p(X)> is a field with a subfield isomorphic to F. For instance, R[X]/<X^2 + 1> is a field (in fact, it is isomorphic to the field of complex numbers). It can be shown that every simple algebraic extension of F is isomorphic to a field of this form.

- When F is a field, the set F((X)) of formal Laurent series over F is a field.
- If V is an algebraic variety over F, then the rational functions V → F form a field, the function field of V.
- If S is a Riemann surface, then the meromorphic functions S → C form a field.
- If I is an index set, U is an ultrafilter on I, and Fi is a field for every i in I, the ultraproduct of the Fi (using U) is a field.
- Hyperreal numbers and superreal numbers extend the real numbers with the addition of infinitesimal and infinite numbers.

There are also proper classes with field structure, which are some times called Fields.

- The surreal numbers form a Field containing the reals, and would be a field except for the fact that they are a proper class, not a set. The set of all surreal numbers with birthday smaller than some inaccessible cardinal number form a field.

Theorem 2.11 The set of non-zero elements of a field F (typically denoted by F^*) is an abelian group under multiplication. Every finite subgroup of F^* is cyclic.

Theorem 2.12 The characteristic of any field is zero or a prime number. (The characteristic is defined as follows: the smallest positive integer n such that n•1 = 0, or zero if no such n exists; here n•1 stands for n summands 1 + 1 + 1 + ... + 1.

Theorem 2.13 The number of elements of any finite field is a prime power.

Theorem 2.14 As a ring, a field has no ideals except {0} and itself.

Theorem 2.15 For every field F, there exists a unique field G (up to isomorphism) which contains F, is algebraic over F, and is algebraically closed. G is called the algebraic closure of F.

2.7 FINITE FIELDS

A field having finitely many elements is called finite field.

Theorem 2.16 If F is a finite field then $|F| = p^k$ for some prime p.

Proof: Since F is finite we know that F has finite characteristic p. Consider the set $S = \{1_F, 2.1_F, ..., p.1_F = 0\}$, it can be easily seen that $(S,+)$ is an additive cyclic group generated by 1_F and also $(S,+,.)$ is a finite subfield of F. Now, let $\phi : Z_p \to S$ be a homomorphism such that $\phi(1) = 1_F$. This gives us an isomorphism between Z_p and S. Thus we can see F as a vector space over Z_p. $|F| = p^k$.

2.7.1 Existence of Multiplicative Generators of a Finite Field

A finite field F_q contains q elements and F_q^* contains q-1 non-zero elements ($F - \{0\}$). By the definition of a field, they form an abelian group with respect to multiplication. This means that the product of two non-zero elements is non-zero. Since the associative law and the commutative laws hold, there exists an identity element and every non-zero element has an inverse. It is a general fact about 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 general proof of this in the case of our group F_q^*.

Theorem 2.17 The order of any $a \in F_q$* divides q-1**.**

Proof: Let *d* be the smallest power of a which equals 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 b*S* 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. Since each coset contains exactly *d* elements and the union of all the cosets exhausts F_q*, means that F_q* is a disjoint union of d-element sets; hence $d \mid q-1$.

2.7.2 Generator of a finite field

A generator *g* of a finite field F_q is an element of order q-1.

Theorem 2.18 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 are a total of $\phi(q-1)$ different generators of F_q^*.

Proof: Suppose $a \in F_q^*$ has order *d*, i.e., $a^d = 1$ and no lower power of a gives 1. By the above theorem *d* divides q-1. Since a^d is the smallest power which equals 1, it follows that the elements $a, a^2, ..., a^d = 1$ are distinct. We claim that the elements of order *d* are precisely the $\phi(d)$ values a^j for which $g.c.d(j, d) = 1$. First since *d* distinct powers of a all satisfy the equation $x^d = 1$, these are all 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 $d \mid d', j \mid d'$ are integers, we can write $\left(a^j\right)^{(d/d')} = \left(a^d\right)^{(j/d')} = 1$.

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 $a^m \neq 1$. Thus, a^j is of order *d* if and only if $g.c.d(j, d) = 1$.

The above theorem says that the non-zero elements of any field form a *cyclic group*, i.e., they are all powers of a single element. This means that if there is any element *a* of order *d*, then there are exactly $\phi(d)$ elements of order *d*. So for every $d \mid q-1$ there are only two possibilities: no element has order *d*, or exactly $\phi(d)$ elements have order *d*.

Corollary 2. For every prime p, there exists an integer *g* such that the powers of *g* exhaust all non-zero residue classes modulo p.

Example 2.30 For numbers 1 to 18 all residues mod 19 can be obtained by taking powers of 2. Namely, the successive powers of 2 reduced mod 19 are: 2,4,,8,16, 13,7,14,9,18,17,15,11,3,6,12,5,10,1.

In many situations when working with finite fields, such as F_p for some prime p, it is useful to find a generator. What if a number $g \in F_p^*$ is chosen at random? What is the probability that it will be a generator? In other words, what proportion of all the non-zero elements consist of generators? According to the above theorem, the proportion is $\phi(p-1)/p-1$. But by our formula for it is equal to the $\prod\left(1-\frac{1}{l}\right)$, where the product is over all prime *l* dividing p-1. Thus the odds of getting a generator by a random guess depend heavily on the factorization of p-1.

2.7.2 Existence and Uniqueness of Finite Fields with Prime Power Number of Elements

In this section we prove both existence and uniqueness by showing that a finite field of $q = p^f$ elements is the spitting field of the polynomial $X^q - X$. The following theorem says that for every prime power q there is one and only one finite field with q elements.

Theorem 2.19 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_p of the polynomial $X^q - X$ is a field of q elements.

Theorem 2.20 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_p 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 divides q-1, it follows that 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 satisfies the later equation. Thus all q elements of are roots of the degree –q polynomial $X^q - X$. Since this polynomial can not 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_p 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 $qX^{q^{-1}} - 1 = -1$ hence, the polynomial $X^q - X$ has no common roots with its derivative, and therefore no multiple roots. Thus F must contain at least the q distinct roots of $X^q - X$. But the set of q roots is a field. This is true because if a and b are 2 roots then $(ab)^q = a^q b^q = ab$ i.e., the product is also a root. By the fact that $(a+b)^p = a^p + p_{C_1} a^{p-1} b + \ldots + b^p = a^p + b^p$ (All other terms vanishes due to the presence of p as a fact).

This implies $(a+b)^q = a^q + b^q = a + b$. So, *a*+*b* is a root.

In this theorem we showed that raising to the p-th power preserves addition and multiplication.

Theorem 2.21 Let F_q be the finite field of $q = p^f$ elements, and let σ be the map that sends every element to its p-th power: $\sigma(a) = a^p$. Then σ is an automorphism of the field F_q (a 1-to-1 map of the field to itself which preserves addition and multiplication). The elements of F_q which are kept fixed by σ are precisely the elements of the prime field F_p. The *f*-th power(and no lower power) of the map σ is the identity map.

Example 2.31 (Construction of a field with 9 elements)

To construct F_9 (Field with 9 elements) we take any monic quadratic polynomial in $F_3[X]$ which has no roots in F_3. By trying all possible choices of coefficients and testing whether the elements $0, \pm 1 \in F_3$ are roots, we find that there are three monic irreducible quadratics: $X^2 + 1, X^2 \pm X - 1$. If, for example we take α to a root of $X^2 + 1$, then the elements of F_9 are all combinations of $a + bi$, where *a* and *b* are 0, 1 or -1. Hence $F_9 = \{a + bi : a, b \in F_3\}$. Addition and multiplication in F_9 is defined as

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2); (a_1 + a_2) \in F_3, (b_1 + b_2) \in F_3$$

$$(a_1 + ib_1).(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_2b_1 + a_1b_2); (a_1a_2 + b_1b_2) \in F_3, (a_2b_1 + a_1b_2) \in F_3$$

which makes F_9 as a field.

One can verify that $1 + i$ is the generator of the cyclic group F_9^*.

2.7.3 Euclidean Algorithm for polynomials

Let us consider polynomials with real coefficients. We define gcd(*f*, *g*) in essentially the same was as for integers, namely as a polynomial of greatest degree which divides both *f* and *g*. The polynomial *gcd*(*f*, *g*) defined in this way is not unique, since we can get another polynomial of the same degree by multiplying by any nonzero constant. However, we can make it unique by requiring that the gcd polynomial be monic. The following example shows the procedure for finding gcd of polynomials- namely Euclidean algorithm for polynomials – which is completely analogous to the Euclidean algorithm to the integers.

Example 2.32 Let $f(X) = X^4 + X^3 + X^2 + 1$ and $g(X) = X^3 + 1 \in F_2[X]$.

Find gcd (*f*,*g*) using Euclidean algorithm for polynomials.

Solution: Polynomial division gives us the sequence of equalities on the left below, which lead to the conclusion that $g.c.d(f,g) = X + 1$. We can express gcd as $u(X)f(X) + v(X)g(X)$. It is easy to see that $X + 1$ can be expressed as a linear combination of *f* and *g*. So we have

$f = (X+1)g + \left(X^2 + X\right)$

$g = (X+1)\left(X^2 + X\right) + (X+1)$

$X + 1 = g + \left(X \ \ +1\right)\left(X^2 + X\right)$

$= g + (X+1)\left(f + (X+1)g\right)$

$= (X+1)f + \left(X^2\right)g$

2.7.4 Quadratic Residue

Suppose p is an odd prime and x is an integer, $1 \le x \le p-1$. x is defined to be a quadratic residue modulo p if the congruence $y^2 = x \pmod p$ has a solution $y \in Z_p$. x is defined to be a quadratic non-residue modulo p if $x \not\equiv 0 \pmod p$ and x is not a quadratic modulo p.

Example 2.33 Let p = 13 in Z_p, quadratic residues are 1, 3, 4, 9, 10 and 12 and quadratic non-residues are 2,5,6,7,8,11

(since $1^2 \equiv 1 \bmod 13, 2^2 \equiv 4 \bmod 13, 3^2 \equiv 9 \bmod 13, \ldots$)

2.7.5 Legendre Symbol

Legendre symbol $\left(\frac{a}{p}\right)$ for any integer $a \ge 0$ and p an odd prime is defined as

$$\left(\frac{a}{p}\right)=\begin{cases}0 \quad if\ a\equiv 0 \bmod p\\ 1 \quad if\ \ a\, is\, quadratic\, residue \bmod ulo\ p\\ -1\ if\ \ a\, is\, a\, quadratic\, non-residue \bmod ulo\ p\end{cases}$$

Theorem 2.22. If p is odd prime then $\left(\frac{a}{p}\right)=a^{(p-1)/2} \bmod p$.

Proof: Case (i) $a\equiv 0 \bmod p$.

By definition $\left(\frac{a}{p}\right)\equiv 0$ and $a^{(p-1)/2}=(0)^{(p-1)/2} \bmod p$

$$\equiv 0 \bmod p\,.$$

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

Case (ii) If $a\not\equiv 0 \bmod p$, if 'a' is quadratic residue of modulo p, then there exists a x such that $x^2\equiv a \bmod p$. Then $a^{(p-1)/2}\equiv\left(x^2\right)^{(p-1)/2} \bmod p=x^{p-1} \bmod p\equiv 1 \bmod p$

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

To see the converse, if $a^{(p-1)/2}\equiv 1 \bmod p$ we show that $\left(\frac{a}{p}\right)=1$. Let b be any primitive element then there exists 'i' such that $b^i=a \bmod p$. For this b, we have $a^{(p-1)/2}\equiv b^{i(p-1)/2} \bmod p\equiv 1 \bmod p.$ since b is primitive $(p-1)\,|\left(i\left(p-1\right)/2\right)$. This implies that $2\,|\,i$.

This gives us $a\equiv\left(b^{i/2}\right)^2 \bmod p$ i.e., 'a' is a quadratic residue modulo p and $\left(\frac{a}{p}\right)=1$ by definition.

2.7. 6 Jacobi Symbol:

Suppose *n* is an odd positive integer and the prime factorization of *n* is $p_1^{e_1}...p_k^{e_k}$.

Let $a \geq 0$ be an integer. The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be $\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i}$.

Example 2.23

To compute Jacobi symbol $\left(\frac{1979}{13923}\right)$ look at prime factorization of 13923 as $3^2 \times 7 \times 13 \times 7$. By definition of Jacobi symbol

$$\left(\frac{1979}{13923}\right) = \left(\frac{1979}{3}\right)^2\left(\frac{1979}{7}\right)\left(\frac{1979}{13}\right)\left(\frac{1979}{17}\right)$$

$$= \left(\frac{2}{3}\right)^2\left(\frac{5}{7}\right)\left(\frac{3}{13}\right)\left(\frac{7}{17}\right)$$

$$= (-1)^2(-1)(1)(-1) = 1$$

Observe that quadratic residues modulo p when

$p = 3 \, are \, \{1\}$

$p = 7 \, are \, \{1, 2, 4\}$

$p = 13 \, are \, \{1, 3, 4, 9, 10, 12\}$

$p = 17 \, are \, \{1, 2, 4, 8, 9, 13, 15, 16\}$

CHAPTER 3

PRIMALITY TESTS

The process of proving whether a given integer is prime or not is called primality test. There are two different types of primality testing algorithms.

1. Probabilistic primality tests: Probabilistic primality testing is a process that proves a number has a high probability of being prime. For example, Fermat primality tests, Solovay and Strassen Primaility test, Miller and Rabin primality test.

2. Deterministic primality tests: Deterministic primality testing is a process that proves a number is definitely prime. For example, Sieve of Eratosthenes, N-1 primality tests, Elliptic Curve Primality tests.

3.1 PROBABALISTIC PRIMALITY TESTS

An integer that passes a probabilistic primality test, it may be prime. If it passes a lot of primality tests, it is very likely to be a prime. On the other hand, if it fails any single primality test, then it is definitely composite. It is generally recommended to use probabilistic primality testing, which is much quicker than actually proving a number is prime. One can use a probabilistic test that determines whether a number is prime with arbitrarily small probability of error, say, less than 2^{-100}.

3.1.1 Fermat Primality test

Definition 3.1 (Pseudoprime) Let n be an odd composite positive integer. We say that it is pseudoprime to the base a if

$$a^{n-1} \equiv 1 \pmod{n} \text{ and } \gcd(a,n)=1.$$

Example 3.1

$3^{90} \equiv 1 \pmod{91}$

91 is a pseudoprime to the base 3.

$2^{90} \neq 1 \pmod{91}$. 91 is not a pseudoprime to the base 2.

Definition 3.2 A composite integer *n* is a *Carmichael number* if and only if

$a^n \equiv a \pmod{n}$ for every integer *a* such that gcd(a,n)=1.

A Carmichael number is therefore a pseudoprime to any base.

Example 3.2 The first few Carmichael numbers are 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, ….

Theorem 3.1 Carmichael must be product of at least three distinct primes.

Theorem 3.2. There are infinitely many Carmichael Numbers.

To test primality of n, we pick an $a \in [1, n-1]$. If $a^{n-1} \equiv 1 \pmod{n}$, n may be prime. Otherwise n is composite. This test fails if n is a Carmichael number.

If the Fermat test says that a number n is composite, then the number n is definitely a composite number. If n is a prime number, the Fermat test will always say that n is prime.

3.1.2 Solovay and Strassen Primality test

Definition 3.3 A composite integer n is called an Euler pseudoprime to the base a if

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

where $\left(\frac{a}{n}\right)$ is Jacobi symbol

Example 3.3 1105 is an Euler Pseudoprime to the base 2

$$2^{552} \equiv 1 \pmod{1105}$$

Let n be a positive integer. We select k integers $a_1, a_2, \ldots, a_k$ less than n at random. We perform Euler pseudoprime test on n for each of these bases. If any these tests fails

then n is composite. If n is composite, the probability that passes all k tests is less than $1/2^k$

3.1.3 Miller and Rabin Primality test

Definition 3.3 A composite integer n is called a strong pseudoprime to the base a if $a^s \equiv 1 \pmod n$ or $a^{s.2^j} \equiv -1 \pmod n$ for $0 \le j \le r-1$ $n-1=2^r.s$ where s is an odd integer.

Example 3.4

n=15790321

n-1=15790320=24.986885

$2^{986895} \equiv 128 \pmod{15790321}$

$2^{2.986895} \equiv 16384 \pmod{15790321}$

$2^{4.986885} \equiv -1 \pmod{15790321} \Rightarrow$15790321 is a strong pseudoprime to the base 2.

Let n be a positive integer. We select k integers $a_1,a_2,\ldots,a_k$ less than n at random. We perform strong pseudoprime test on n for each of these bases. If any of these tests fails then n is composite. If n is composite, the probability that passes all k tests is less than $1/4^k$**.** Therefore this test is stronger than Solovay and Strassen Primality test.

3.2 DETERMINISTIC PRIMALITY TESTS

3.2.1 Trial Division

To check if a small integer is prime, we just divide that integer by all the primes less than or equal to its square root.

Theorem 3.3 For any prime $p \le \sqrt{n}$ such that $p \nmid n \Rightarrow$ n is prime.

Example 3.5

n=101

Let's find all primes $p \le \sqrt{101} \cong 10{,}05$

$2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$, $7 \nmid 101$.

Therefore 101 is prime.

3.2.2 Sieve of Eratosthenes

Eratosthenes is a Greek mathematician who found an efficient method to determine small primes. We write down all integers from 1 to n. Calculate square root of n. Firstly, we cross out 1. Then we cross out all composite numbers which are multiples of primes less than square root of n. The remaining numbers are prime numbers.

3.2.3 N-1 Primality tests

N-1primality testing algorithms are based on the converse of Fermat's Little Theorem. If we can find factors of N-1, we can test the primality of N.

Example 3.6 (Lucas) Let *a* and *n* be two positive integers and gcd(a,n)=1, if $a^{n-1} \equiv 1 \pmod n$ but $a^{\frac{n-1}{d}} \neq 1 \pmod n$ for each divisor of d > 1 of n-1,then *n* is prime number.

Example 3.7 (Pocklington) Let n be a positive integer. Suppose that there is a prime q dividing n-1 which is greater than √n-1. If there exists an integer a such that

i) $a^n-1 \equiv 1 \pmod n$

ii) $\gcd(a^{(n-1)/q}-1,n)=1$

then n is prime.

3.2.4 Elliptic Curve Primality tests

The elliptic curve primality test is an analog of Pocklington based on the group $(Z/nZ)^*$. In Chapter 5, it will be presented in details.

CHAPTER 4

ELLIPTIC CURVES

Elliptic curves have many applications such as cryptography, factorization of integers and primality testing. In this chapter basic definitions and facts about elliptic curves over different fields will be presented.

Definition 4.1 Let K be a field of characteristic is not 2 or 3. An *elliptic curve* is the set of solutions $(x, y) \in \mathrm{K}$ of an equation of the form

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

where $4a^3 + 27b^2 \neq 0$, together with a *point at infinity* denoted by *O*.

If K is a field of characteristic 2, then an *elliptic curve* is the set of solutions $(x, y) \in \mathrm{K}$ of an equation of the form

$$y^2 + \mathrm{cy} = x^3 + ax + b$$

or else

$$y^2 + \mathrm{xy} = x^3 + ax + b$$

where $4a^3 + 27b^2 \neq 0$, together with a *point at infinity O*.

If K is a field of characteristic 3, then an *elliptic curve* is the set of solutions $(x, y) \in \mathrm{K}$ of an equation of the form

$$y^2 = x^3 + ax^2 + bx + c$$

(where the cubic on the right has no multiple roots), together with a *point at infinity O*.

There is a natural addition operation under which the points of an elliptic curve form an Abelian group. The point at the infinity is the identity element of this group.

4.1 ELLIPTIC CURVES OVER R

Definition 4.2 Let E be an elliptic curve over the real numbers, and let P and Q be two points on E. We define,

1. The negative of a point P = (x,y) is its reflection in the x-axis: the point -P is (x,-y). Notice that for each point P on an elliptic curve, the point -P is also on the curve.

2. Let P ≠ -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R. (Figure 4.1)

3. Let Q = -P. The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and -P cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity *O*. By definition, P + (-P) = *O*. As a result of this equation, P + *O* = P in the elliptic curve group . *O* is called the additive identity of the elliptic curve group; all elliptic curves have an additive identity.

4. To add a point P to itself, a tangent line to the curve is drawn at the point P. If y-coordinate of P is not 0, then the tangent line intersects the elliptic curve at exactly one other point, -R. -R is reflected in the x-axis to R. This operation is called doubling the point P; the law for doubling a point on an elliptic curve group is defined by
P + P = 2P = R.
If a point P is such that y-coordinate of P is 0, then the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point. By definition, 2P = *O* for such a point P. If one wanted to find 3P in this situation, one can add 2P + P. This becomes P + O = P Thus 3P = P. 4P = O, 5P = P, 6P = O, 7P = P, etc.

Let $P = (x_1,y_1)$, $Q = (x_2,y_2)$ and $R = (x_3,y_3)$, where P + Q = R and Q ≠ P , then

$$P + Q = R = (x_3, y_3) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \ , \ \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right)$$

If Q = P, then

$$P + P = R = (x_3, y_3) = ((\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 , \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1)$$

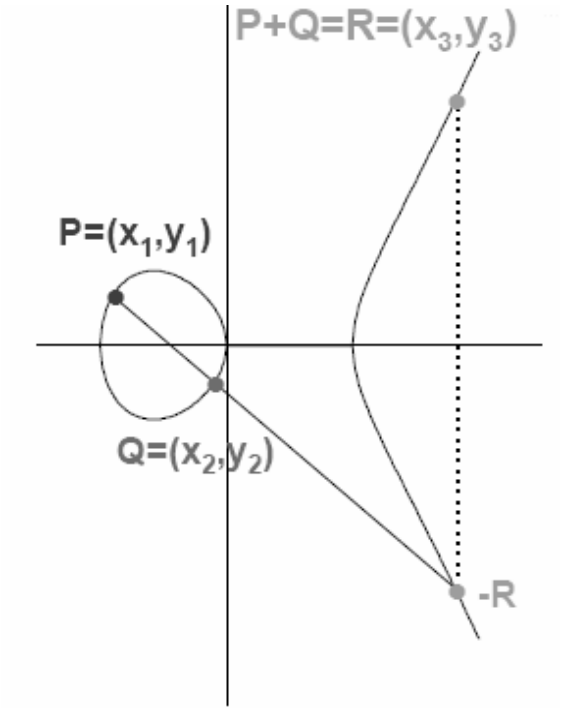

Figure 4.1: An elliptic Curve over R

Example 4.1 Let $y^2 = x^3 + 3x$ and P = (1,2), Q = (3,6), then

$$P + Q = R = (x_3, y_3) = ((\frac{6-2}{3-1})^2 - 1 - 3 , (\frac{6-2}{3-1})(1-0) - 2) = (0,0)$$

$$P + P = R = (x_3, y_3) = ((\frac{3.1+3}{2.2})^2 - 2.1 , \frac{3.1+3}{2.2}(1 - \frac{1}{4}) - 2) = (\frac{1}{4}, -\frac{7}{8})$$

4.2 ELLIPTIC CURVES OVER FINITE FIELDS

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.

Theorem 4.1 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

$$E[n] \simeq \mathrm{Z}_n \oplus \mathrm{Z}_n$$

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

$$E[n] \simeq \mathrm{Z}_{n'} \oplus \mathrm{Z}_{n'} \quad \text{or} \quad \mathrm{Z}_n \oplus \mathrm{Z}_{n'}$$

Theorem 4.2 Let E be an elliptic curve over the finite field F_q. Then

$$E(F_q) \simeq \mathrm{Z}_n \qquad \text{or} \qquad \mathrm{Z}_{n_1} \oplus \mathrm{Z}_{n_2}$$

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

$$\mathrm{Z}_{n_1} \oplus \mathrm{Z}_{n_2} \oplus \ldots\ldots\ldots \oplus \mathrm{Z}_{n_r},$$

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, 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.

4.2.1 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) $\exists \infty \in \mathrm{E}(\mathrm{F_p})$ such that $\forall \mathrm{P} \in \mathrm{E}(\mathrm{F_p})$, $\mathrm{P} + \infty = \infty + \mathrm{P} = \mathrm{P}$ (*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.

Theorem 4.3(Hasse) Let E be an elliptic curve over the finite field F_q. Then the order of $E(F_q)$ satisfies

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

Example 4.2 $y^2=x^3+5x+7$ over Z_5

$4a^3+27b^2=4.\ 5^3+27.\ 7^2=1823 \equiv 3 \neq 0 \pmod 5$

By Hasse Theorem

$$|5+1-E(Z_5)| \le 2\sqrt{5} = 4.4721$$

$$-4 \le 6-E(Z_5) \le 4$$

$$-10 \le -E(Z_5) \le -2$$

$$2 \le E(Z_5) \le 10$$

Let x = 0

$y^2 \equiv 0^3+5.0+7 \equiv 2 \pmod 5$ But $(\frac{2}{5}) = -1$

Let x=1

$y^2 \equiv 1^3+5.1+7 \equiv 3 \pmod 5$ But $(\frac{3}{5}) = -1$

Let x = 2

$y^2 \equiv 2^3+5.2+7 \equiv 0 \pmod 5$ y = 0

$(2,0) \in E(Z_5)$

We use Maple to calculate multiples of (2,0). We know that the number of elements can not exceed 10 by Hasse theorem.

multsell([2,0],10,5,7,5);

[[1, [2, 0]], [2, ["infinity", "infinity"]], [3, [2, 0]], [4, ["infinity", "infinity"]], [5, [2, 0]], [6, ["infinity", "infinity"]], [7, [2, 0]], [8, ["infinity", "infinity"]], [9, [2, 0]], [10, ["infinity", "infinity"]]]

The order of (2,0) is 2.

Let x = 3

$y^2 \equiv 3^3+5.3+7 \equiv 4 \pmod 5$ y = 2

We use Maple to calculate multiples of (3,2). We know that the number of elements can not exceed 10 by Hasse theorem.

multsell([3,2],10,5,7,5)

[[1, [3, 2]], [2, [3, 3]], [3, ["infinity", "infinity"]], [4, [3, 2]], [5, [3, 3]], [6, ["infinity", "infinity"]], [7, [3, 2]], [8, [3, 3]], [9, ["infinity", "infinity"]], [10, [3, 2]]]

The order of (3,2) is 3.

We know that the order of an element must divide the order of the group. The lcm(2,3)=6. So the order of group can be 6 or multiples of 6. We know that the number of elements can not exceed 10 by Hasse theorem. Hence the order of this group must be 6.

$E(Z_5) \cong Z_2 \times Z_3 = Z_6$

4.3 ELLIPTIC CURVES OVER C

4.3.1 Lattices and Elliptic Curves

If we take K=C, we see that there are relationships between Elliptic curves over C and lattices.

Let ω_1, ω_2 be complex numbers that are linearly independent over R. Then

$$L=Z\omega_1+Z\omega_2=\{n_1\omega_1+n_2\omega_2 \mid n_1,n_2 \in Z\}$$

is called lattice. The main reason we are interested in lattices is that C/L is a torus, and we want to show that a torus gives us an elliptic curve. The set

$$F=\{a_1\omega_1+a_2\omega_2 \mid 0 \le a_i<1, \quad i=1,2\}$$

is called a fundamental parallelogram for L. A different choice of basis ω_1, ω_2 for L will of course give a different fundamental parallelogram. Since it will occur several times, we get

$$\omega_3=\omega_1+\omega_2$$

A function on C/L can be regarded as a function f on C such that $f(z+\omega)=f(z)$ for all $z \in Z$ and all $\omega \in L$. We are only interested in meromorphic functions, so we define a doubly periodic function to be a meromorphic function $f:C \to C \cup O$ such that

$f(z+\omega)=f(z)$ for all $z \in C$ and all $\omega \in L$. Equivalently,

$$f(z+\omega_i)=f(z) \quad i=1,2$$

The numbers $\omega \in L$ are called the periods of f. If f is a meromorphic function and $\omega \in C$, then we can write

$$f(z)=a_r(z-w)^r+a_{r+1}(z-w)^{r+1}+.....$$

with $a_r \neq 0$. The integer r can be either positive, negative, or zero. Define the order and the residue of f at ω to be

$$r = ord_w f$$

$$a_{-1}=Res_w f$$

4.3.2 Weierstrass Function

The series defined by

$$\frac{1}{z^2} + \sum_{l \in L,\, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) \qquad (1)$$

is normally convergent on every compact included in C\L The sum of this series is called the Weierstrass function associated with the lattice L. It is denoted by $\wp_L(z)$

Properties 4.1

1.The sum defining $\wp(z)$ converges absolutely and uniformly on compact sets not containing elements of L.

2.$\wp(z)$ is meromorphic in C and has a double pole at each $\omega \in L$.

3.$\wp(-z)=\wp(z)$ for all $z \in C$

4.$\wp(z+\omega)=\wp(z)$ for all $\omega \in L$

5.The set of doubly periodic functions for L is $C(\wp,\wp')$. In other words every doubly periodic function is a rational function of $\wp$ and its derivative $\wp$.If we differentiate $\wp(z)$ term by term we get

$$\wp'_L(z) = -2 \sum_{l \in L} \frac{1}{(z-l)^3}.$$

4.3.3 Elliptic Curves in Weierstrass Form

The Laurent series for $\wp(z)$ about z=0 is given by

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}\, z^{2k}$$

For each nonzero $\omega \in L$, we expand the term corresponding to l in the definition (1) of $\wp(z)$.

We do this by differentiating the geometric series $\frac{1}{1-x} = 1 + x + x^2 + x^3 \ldots$ then substituting z/w for x we get

$$\frac{1}{(1-z/\omega)^2} = 1 + 2\frac{z}{\omega} + 3\frac{z^2}{\omega^2} + 4\frac{z^3}{\omega^3} + \ldots$$

If we subtract 1 from both sides, divide both sides by ω^2,and then substitute in (1), we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}} 2\frac{z}{l^3} + 3\frac{z^2}{l^4} + 4\frac{z^3}{l^5} + \ldots + (k-1)\frac{z^{k-2}}{l^k} + \ldots$$

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \ldots..(2)$$

We now use (2) to compute the first few terms in the expansions of $\wp(z), \wp(z)^2, \wp(z)^3, \wp'(z)$ and $\wp'(z)^2$

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \ldots \qquad (3)$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8)z^2 + \ldots \qquad (4)$$

$$\wp(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + \ldots \qquad (5)$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + \ldots \qquad (6)$$

Recall that we are interested in finding coefficients a,b,c,d of a cubic

f(x)=ax³+bx²+cx+d such that

$$\wp'(z)^2 = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d$$

and we saw that it suffices to show that both sides agree in their expansion through the constant term. If we multiply equation (6) by a, equation (5) by b, equation (2) by c, and then add them all to the constant d and finally equate the coefficients of z^{-6}, z^{-4}, z^{-2} and the constant term to the corresponding coefficients in (4),we obtain successively

a=4 ; b=0 ; $-24G_4 = 4(9G_4) + c$; $-80G_6 = 4(15G_6) + d$

Thus, $c = -60G_4$, $d = -140G_6$. It is traditional to denote

$$g_2 = g_2(L) = 60G_4 = 60\sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-4}$$

$$g_3 = g_3(L) = 140G_6 = 140\sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-6}$$

We have thereby derived a second form for the differential equation

$$\wp'(z)^2 = f(\wp(z)), \quad \text{where } f(x) = 4x^3 - g_2 x - g_3$$

Theorem 4.4. Let L be a lattice and let E be the elliptic curve $y^2=4x^3-g_2x-g_3$.The map

$$\Phi: C/L \to E(C)$$

$$z \to (\wp(z), \wp'(z))$$

$$0 \to \infty$$

is an isomorphism of groups.

4.3.4 Complex Multiplication

Suppose that E_1 and E_2 are elliptic curves defined over F. An F-rational homomorphism Φ: $E_1 \to E_2$ is a homomorphism of group such that the coordinates of Φ (x; y) are rational functions (with coefficients in F) of x and y. Let $Hom_F(E_1;E_2)$ be all the F-rational homomorphism from E_1 to E_2 Then $Hom_F(E_1 ; E_2)$ has a natural structure of abelian group (through the group structure of E_2). Suppose that E is an elliptic curve defined over F. Then

$$End_F(E) = Hom_F(E;E)$$

has a natural ring structure. Here the ring multiplication is the composition of maps. We always have

$$Z \to End_F(E):$$

E is said to have complex multiplication if

$$Z \subset End_F(E).$$

Suppose that $\Phi \in End_F(E)$, then there exists a unique dual endomorphism

$\Phi \in End_F(E)$ such that

$$\phi + \hat{\phi},\ \phi \circ \hat{\phi} = \hat{\phi} \circ \phi \in \mathbb{Z}$$

and $d_\Phi = \Phi o \Phi$ is the degree of the corresponding extension of the function fields

$$\begin{array}{ccc} \mathbb{F}(E) & = & \mathbb{F}(x,y) \\ & & \Big| d_\phi \\ & & \mathbb{F}(x',y') \end{array}$$

Here (x', y') = Φ (x; y)

We say that is separable (reps. inseparable, purely inseparable) if the field extension F(x, y)/F(x', y') is separable (reps. inseparable, purely inseparable). If Φ is separable, then $|\ker(\Phi)| = d_\Phi$ If Φ is purely inseparable, then $|\ker(\Phi)|=1$

CHAPTER 5

ELLIPTIC CURVE PRIMALITY TESTS

In Chapter 3, we have seen that most of the primality tests are based on Fermat's Little Theorem. Elliptic Curve primality tests use the same idea, too. Goldwasser and Kilian developed the test which is based on a new methodology for applying group theory to the problem of prime certification, and the application of this methodology using groups generated by elliptic curves over finite fields.

5.1 GOLDWASSER-KILIAN ALGORITHM

The idea is to build a decreasing sequence of probable primes $N_0>N_1>\ldots>N_k$ such that the primality of N_{i+1} implies that of N_i, and where N_k is so small that we can check easily if it is a prime or not. Then, each algorithm consists of two parts, in the first one we generate such a sequence and in the second we verify if each N_i is a prime or not.

Our description of the algorithms will be mainly concerned on the exposition of ideas of the two parts of the DOWNRUN rather than in the technical definitions.
The Goldwasser-Killian algorithm mentioned in the introduction follows from theorem 4 and the so called Schoof's algorithm which is used to compute the cardinality of E(Z/NZ) . The description of the algorithm is the following:

GK(N) boolean;

i) Generate an elliptic curve E(a,b) over Z/NZ, until $\gcd(4a^3+27b^2,N)=1$.

ii) Compute its number of points with Schoof's algorithm, call this number m. If m is odd go back to step i, otherwise set q=m/2. If q is a probable prime go to step iii, otherwise go back to step i.

iii) Select a point $P \in E(a,b)$. If $qP=O$ go to step iv, otherwise choose another P.

iv) If $q>N^{1/2}+2N^{1/4}+1$ then return **GK**(q).

v) End.

This algorithm has an abort instruction that stops the procedure if it has been running for a long time. This algorithm was presented in [G-K] in 1986, however an update has been published in [G-K2] in 1999. The problem here is that Schoof's algorithm seems almost impossible to implement. Atkin and Morain use elliptic curves over finite fields but based on complex multiplication. Such implementation turned out to be more efficient.

5.2 ATKIN'S ECPP ALGORITHM

Before describing the algorithm we'll recall that a fundamental discriminant D is a positive integer which is not divisible by any square of an odd prime and which satisfies $D\equiv 3 \bmod 4$ or $D\equiv 4,6 \bmod 16$, and let $K=Q(\sqrt{-D})$ denote the quadratic field corresponding to D, The description of the algorithm created by Atkin and Morain is the following.

ECPP(N) boolean;

i) If $N<1000$ check the primality of N directly and return the answer.

ii) Find an imaginary quadratic field $K=Q(\sqrt{-D})$ with D a fundamental discriminant for which the equation

$$4N=x^2+Dy^2$$

has solutions in rational integers x and y.

iii) For each pair (U,V) of solutions of the above equation try to factor

$$m=((U-2)^2+DV^2)/4=N+1-U,$$

if one of these can be written as Fw where F is completely factored and w is a probable prime then go to step iv else go to step ii.

iv) Find the equation of the curve E having m points modulo N and a point P on it. If wP=O and $w>N^{1/2}+2N^{1/4}+1$ then return **ECPP**(w).

v) End.

In step iv we need algorithms to generate elliptic curves of arbitrary cardinality, this can be achieved via several results which depend on D

This algorithm works due to the following analysis. Let's say that N is prime, then it splits as a product of principal ideals in K and this is ensured by step ii, therefore N is the norm of the algebraic integer $\pi= (x+y\sqrt{-D})/2$.

CHAPTER 6

CONCLUSION

We have seen primality testing algorithms, elliptic curves and elliptic curve primality testing. The time is very important while testing the given integer is prime or not. For example, Miller and Rabin probabilistic primality test is polynomial and probability of getting desired result is very high. Recently, a lot of studies have been done on elliptic curves to get algorithms with polynomial time. For example, Atkin used complex multiplication of elliptic curves in order to get better algorithms.

REFERENCES

Adleman L. M., Pomerance C.,_Rumely R. S., *On distinguishing prime numbers from composite numbers*_ Annals of Math., 117, pp 173-206, 1983.

Adleman, L.M., Manders, K. and Miller, G.L. *Obtaining roots in finite fields*. Lecture Notes in Math. Vol 1512. Springer-Verlag. New York, 1977.

Atkin, A.O.L. and Morain, F., *Elliptic curves and primality proving.* Math. Comp., 61(203):29-68, July 1993.

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

Cassels, J.W.S. *Diophantine equations with special reference to elliptic curves*. J. London Mathematical Society. 41 (1966), 193-291

Cohen H., Lenstra A. K., *Implementation of a new primality test*, Math. of Comp.,48, 177, pp 103-121, 1987

Cohen, H. and Lenstra, Jr. H. W. *Primality testing and Jacobi sums. Math*. Comp. (42)1984

Cohn, H. *Advanced Number Theory*. Dover. New York, 1980.

Fulton, W. *Algebraic Curves.* Benjamin, 1959

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

Goldwasser, S. and Killian, J. *Almost all primes can be quickly certified*. Proc. 18th STOC, 316-329. ACM. Berkeley, 1986.

Goldwasser S and Kilian J., *Primality Testing Using Elliptic Curves,* Journal of the ACM, Vol. 46, No. 4, pp. 450 –472, July 1999.

Kendirli, B., *Lecture Notes in Cryptography*, Istanbul, 2005.

Kendirli,B., *Number Theory with Cryptographic Applications*, Fatih University 2006

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.

Lenstra, H. W. Jr. *Factoring integers with elliptic curves*. Annals of Mathematics (2), 126:649-73,1987.

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

Morain F, *Elliptic curves, primality proving and some titanic primes*, 1989

Morain, F. *Primality Proving Using Elliptic Curves: an Update.* Lect. Not. In Comp. Sci. (1423) 111-127. Algorithmic Number Theory. Springer-Verlag. Heideberg, 1998.

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

Pollard, J.M. *Theorems on factorization and primality testing*. Proceeding Cambridge Phil. Soc., vol 76(1974), 521-528.

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.

Scoof, R. *Elliptic curves over finite fields and the computation of square roots* $mod\ p$. Mathematics of Computation, 44(170):483-494, April 1985

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. *Advanced Topics in the Arithmetic of Elliptic Curves*. Vol 151 of Graduate Texts in Mathematics. Springer-Verlag, 1994.

Wunderlich, M.C. *A performance analysis of a simple prime-testing algorithm*. Math. Comp. 40, 162 (1983), 709-714.

Uzunkol O., *Atkin's ECPP (Elliptic Curve Primality Proving) Algorithm*, M.S. Thesis, University of Kaiserslautern, 2004

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