ISOMORPHISM CLASSES OF ELLIPTIC CURVES OVER FINITE FIELDS OF CHARACTERISTIC TWO

BARIŞ BÜLENT KIRLAR

AUGUST 2005

ISOMORPHISM CLASSES OF ELLIPTIC CURVES OVER FINITE FIELDS OF CHARACTERISTIC TWO

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OF

MIDDLE EAST TECHNICAL UNIVERSITY

BY

BARIŞ BÜLENT KIRLAR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF MASTER OF SCIENCE

IN

MATHEMATICS

AUGUST 2005

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

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

Prof. Dr. Şafak ALPAY
Head of Department

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

Prof. Dr. Ersan AKYILDIZ
Supervisor

Examining Committee Members

Assoc. Prof. Dr. Ali DOĞANAKSOY (METU, MATH) _____

Prof. Dr. Ersan AKYILDIZ (METU, MATH) _____

Assist. Prof. Dr. Hakan ÖKTEM (METU, IAM) _____

Assoc. Prof. Dr. Ferruh ÖZBUDAK (METU, MATH) _____

Dr. Muhiddin UĞUZ (METU, MATH) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

Name, Last name : Barış Bülent, Kırlar
Signature :

Abstract

ISOMORPHISM CLASSES OF ELLIPTIC CURVES OVER FINITE FIELDS OF CHARACTERISTIC TWO

Kırlar, Barış Bülent
M.Sc., Department of Mathematics
Supervisor: Prof. Dr. Ersan Akyıldız

August 2005, 58 pages

In this thesis, the work of Menezes on the isomorphism classes of elliptic curves over finite fields of characteristic two is studied. Basic definitions and some facts of the elliptic curves required in this context are reviewed and group structure of elliptic curves are constructed.

A fairly detailed investigation is made for the isomorphism classes of elliptic curves due to Menezes and Schoof. This work plays an important role in Elliptic Curve Digital Signature Algorithm. In this context, those isomorphism classes of elliptic curves recommended by National Institute of Standards and Technology are listed and their properties are discussed.

Keywords: Finite Fields, Elliptic Curves, Isomorphism Classes, Group Structure, Elliptic Curve Digital Signature Algorithm.

Öz

KARAKTERİSTİĞİ İKİ OLAN SONLU CİSİMLER ÜZERİNDE ELİPTİK EĞRİLERİN İZOMORFİZM SINIFLARI

Kırlar, Barış Bülent
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Prof. Dr. Ersan Akyıldız

Ağustos 2005, 58 sayfa

Bu tezde, Menezes'in karakteristiği iki olan sonlu cisimler üzerinde eliptik eğrilerin izomorfizm sınıflarıyla ilgili yaptığı çalışma incelenmiştir. Eliptik eğriler ile ilgili konularda gereksinim duyulan temel tanımlar ve bazı gerçekler üzerinde durularak eliptik eğriler üzerinde grup yapısı oluşturulmuştur.

Eliptik Eğri Sayısal İmza Algoritması'nda önemli bir rolü olan eliptik eğrilerin izomorfizm sınıfları, Menezes ve Schoof'un çalışmaları temel alınarak derinlemesine incelenmiştir. Ayrıca, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından önerilen eliptik eğrilerin, izomorfizm sınıfları belirtilmiş ve özellikleri tartışılmıştır.

Anahtar Kelimeler: Sonlu Cisimler, Eliptik Eğriler, İzomorfizm Sınıfları, Grup Yapısı, Eliptik Eğri Sayısal İmza Algoritması.

To My Wife and Parents

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Prof. Dr. Ersan Akyıldız, for his guidance, encouragement and patience at each step of this thesis. I also thank to him for his many great advices in mathematics and for the life.

To my princess, Burcu Kırlar, I offer special thanks for her precious love, patience and encouragement throughout this work.

I am so thankful to my parents and my older brother, Mahmut Kırlar, without whose encouragement, patience, and support this thesis would not be possible.

I am also grateful to Yusuf Aslantaş for his support, tolerance and being with me all the way.

Finally, I deeply thank Caner Akman and all of my close friends for their help and moral support during this work.

Table of Contents

Plagiarism iii

Abstract iv

Öz v

Dedication vi

Acknowledgments vii

Table of Contents viii

List of Figures ix

List of Tables x

CHAPTER

1 Elliptic Curves 1

1.1 Introduction to Elliptic Curves 1

1.2 Basic Facts 2

1.3 The Discriminant and j-Invariant 7

1.4 The Group Structure of an Elliptic Curve 8

1.5 Some Properties over Finite Fields 12

2 Isomorphism Classes of Elliptic Curves over Finite Fields of Characteristic Two 14

2.1 Introduction 14

2.2 Elliptic Curves over F_{2^m} 17

2.3 Isomorphism Classes of $E(F_{2^m})$, $j(E) \neq 0$ 20

2.4 Isomorphism Classes of $E(F_{2^m})$ when m is odd and $j(E) = 0$ . . . 21

2.5 Isomorphism Classes of $E(F_{2^m})$ when m is even and $j(E) = 0$ . . 25

2.6 Number of Points 39

3 Elliptic Curves over Finite Fields of Characteristic Two Used In Ecdsa and Their Properties 45

3.1 Introduction 45

3.2 Elliptic Curve Discrete Logarithm Problem 46

3.3 ECDSA Signature Generation 46

3.4 ECDSA Signature Verification 47

3.5 Selecting An Appropriate Elliptic Curve over F_{2^m} 48

3.6 NIST Recommended Curves over F_{2^m} 48

3.6.1 Koblitz Elliptic Curves 49

3.6.2 Random Elliptic Curves 52

4 Conclusions 56

References 57

List of Figures

1.1 Geometric addition and doubling of elliptic curve points 9

List of Tables

2.1 Representatives of the isomorphism classes of elliptic curves over F_4 39

2.2 Orders of elliptic curves over F_{2^m} with *j-invariant* equal to 0, where m is odd 43

2.3 Orders of elliptic curves over F_{2^m} with *j-invariant* equal to 0, where m is even 44

Chapter 1

Elliptic Curves

1.1 Introduction to Elliptic Curves

Recently, the theory of elliptic curves over finite fields has been applied to various problems in cryptography: factorization of integers, primality testing and construction of cryptosystems. The basic reason for this is that elliptic curves over finite fields provide a large supply of finite abelian groups which are amenable to computation because of their rich structure. The use of elliptic curves has been referred to as the first application of twentieth century mathematics to the problem of prime factor decomposition [8].

In 1985, Miller showed that elliptic curves have a rich enough structure which increases their importance in cryptography [6]. The elliptic curve methods are best as analogous of certain older algorithms which depend on properties of the multiplicative group of a finite field $GF(q)$. It was the difficulty of solving the discrete logarithm problem in $GF(q)$ that led to the elliptic curve cryptosystems using an analogous problem based on the finite abelian group of points on an elliptic curves. In 1987, Koblitz described analogs of some of the public key cryptosystems based on the discrete logarithm problem on an elliptic curve E defined over a finite field $GF(q)$ ([2], [3]). Koblitz and Miller suggested using the abelian group of an elliptic curve over a finite field to implement the ElGamal public key cryptosystem [1].

The use for the first time of elliptic curves in factorization was discovered by H. W. Lenstra who obtained a new factorization method which in many respects is better than earlier known ones.

Elliptic curves can also be used in primality testing. Goldwasser and Killian proved that a probabilistic primality testing algorithm of which the expected running time is bounded by a constant power of $\log n$ where n is the number to be tested. Atkin developed a variant of the algorithm using special elliptic curves to simplify counting the number of points. Lenstra showed that elliptic curves can be applied to primality testing and to factorization giving rise to algorithms with an excellent performance both in theory and practice [8].

When selecting curves over a given field K, it is useful to know when the choosen curves are isomorphic, how many choices of non-isomorphic curves there are and the order of the curve. Having identified the isomorphism classes, we may then pick a representative that could perhaps result in a more efficient implementation of the group addition. Therefore, we are motivated to study the isomorphism classes of elliptic curves. Because of practical interest, we will use elliptic curves over finite fields of characteristic two.

We shall start our discussion by presenting basic definitions and some facts about elliptic curves.

1.2 Basic Facts

Here, we will give some basic facts to understand the elliptic curves and some theorems associated with isomorphism of two elliptic curves.

Let K be a field. n-dimensional **projective space** $P^n(K)$ over K is given by equivalence classes of n-tuples $(x_0, x_1, ..., x_n)$ with $x_0, x_1, ..., x_n \in K$ and at least one of x_i nonzero for $i = 0, 1, ..., n$. Two n-tuples $(x_0, x_1, ..., x_n)$ and $(y_0, y_1, ..., y_n)$ are said to be **equivalent** if there exists a nonzero element $\lambda \in K$ such that

$$(x_0, x_1, ..., x_n) = \lambda(y_0, y_1, ..., y_n)$$

We write $(x_0, x_1, ..., x_n) \sim (y_0, y_1, ..., y_n)$. The equivalence class of $(x_0, x_1, ..., x_n)$ is denoted by $(x_0 : x_1 : ... : x_n)$, and thus $P^n(K) = \{(x_0 : x_1 : ... : x_n) :$

$(x_0, x_1, ..., x_n) \in K^n\}$.

The n-dimensional projective space $P^n(K)$ can be also identified naturally by the set of lines through the origin in K^{n+1}. Let us have close look at the cases $n = 0, 1, 2$: it is clear that $P^0(K) = \{pt\}$.

For $P^1(K)$; let $(x_0 : x_1) \in P^1(K)$ be a point with $x_1 \neq 0$, then $(x_0 : x_1) = (x_0/x_1 : 1)$. These are the finite points in $P^1(K)$. However, if $x_1 = 0$, then dividing by x_1 should be thought of as giving ∞ in x_0 coordinate, and so the points $(x_0 : 0)$ are called the **points at infinity** in $P^1(K)$.

The one-dimensional **affine plane** over K is often denoted by

$$A^1(K) = \{x_0 \in K\}$$

We have an inclusion

$$A^1(K) \hookrightarrow P^1(K)$$

given by

$$x_0 \to (x_0 : 1)$$

It is clear that $P^1(K) \setminus A^1(K) = (1 : 0) : = \infty : \cong P^0(K)$.

For $P^2(K)$; let $(x_0 : x_1 : x_2) \in P^2(K)$ be a point with $x_2 \neq 0$, then $(x_0 : x_1 : x_2) = (x_0/x_2 : x_1/x_2 : 1)$. These points correspond bijectively to the affine plane $A^2(K)$. If $x_2 = 0$, the points $(x_0 : x_1 : 0)$ in $P^2(K)$ are called the **points at infinity** and these points correspond bijectively to $P^1(K)$ in $P^2(K)$. Thus, the **affine plane**

$$A^2(K) = \{(x_0, x_1) \in K \times K\}$$

is imbeded

$$A^2(K) \hookrightarrow P^2(K)$$

by the map

$$(x_0, x_1) \to (x_0 : x_1 : 1)$$

and

$$H_\infty = P^2(K) \setminus A^2(K) = \{(x_0 : x_1 : 0) \in P^2(K)\}$$

called hyperplane at ∞ is identified with $P^1(K)$ with the map $(x_0 : x_1 : 0) \leftrightarrow (x_0 : x_1)$.

Since an elliptic curve is a special subvariety of $P^n(K)$, we want to introduce first, the concept of projective subvarieties. Note that for any homogeneous polynomial $F(x_0, x_1, \ldots, x_n)$ in the variables $x_0, x_1, \ldots, x_n$, it make sense to look at the zeros of $F(x_0, x_1, \ldots, x_n)$ in $P^n(K)$.

$$F(x_0, x_1, \ldots, x_n) = 0 \Longrightarrow F(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^m F(x_0, x_1, \ldots, x_n) = 0$$

By a projective subvariety of $P^n(K)$, we mean the common set of solutions of homogeneous polynomials $F_\alpha(x_0, x_1, \ldots, x_n)$, for $\alpha \in I$. This subset of $P^n(K)$ is denoted by $X = V(F_\alpha : \alpha \in I)$. It is clear that $X = V(F_\alpha : \alpha \in I)$ depends only on the ideal Ω generated by F_α, $\alpha \in I$, and thus any projective subvariety of $P^n(K)$ is a common set of solution of finitely many homogeneous polynomials in $x_0, x_1, ..., x_n$ over K.

Subvarieties of $P^1(K)$ are trivial. They are either $\emptyset$, $P^1(K)$ or a finite set of points. In fact, if $X \neq \emptyset$ or $P^1(K)$, then $\#X \leq \deg F$ where $X = V(F)$ as the following argument shows:

$$X = V(\Omega) = V\big(F(x_0, x_1)\big) = \big\{V\big(F(\frac{x_0}{x_1}, 1) = 0\big) \cup V\big(F = 0, x_1 = 0\big)\big\}.$$

It is well-known that the subvarieties of $P^2(K)$ are either $\emptyset$, finite set of points, $P^2(K)$ or curves $X = V\big(F(x_0, x_1, x_2)\big)$ associated to a homogeneous polynomial $F(x_0, x_1, x_2)$ over K. When F is a linear or a quadratic polynomial in x_0, x_1, x_2, it is also well-known in algebraic geometry that; either X is $P^1(K)$ or the non-singular model of X is $P^1(K)$. So, the first non-trivial case of a subvariety of $P^2(K)$ occurs when degree of F is 3. These curves $X = V(F)$, $\deg F = 3$, in $P^2(K)$ turns out to be very interesting objects and do appear in many different

areas in mathematics. The cubic curve $X = V(F)$ (i.e. $\deg F = 3$) in $P^2(K)$ is called an elliptic curve if X is a non-singular (smooth) subvariety in $P^2(K)$. The elliptic curves carry a very rich geometric properties as we shall discuss some of them below. The general form of a cubic homogeneous polynomial in X, Y, Z over K is given by

$$G(X, Y, Z) = \sum a_{ijk} X^i Y^j Z^k, \quad i + j + k = 3.$$

By a change of variable, we can transform G into the form

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3, \quad (1.2.1)$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. Thus, it is enough to study $X = V(F)$ where F is in the form (1.2.1). This F is called *Weierstrass equation* over a field K. The subvariety $X = V(F)$ of $P^2(K)$ associated to X is not in general a non-singular. For $X = V(F)$ to be an elliptic curve it has to be non-singular and therefore is necessary and sufficient that the following set is $\emptyset$:

$$X = V(F) \cap \Big\{ P \in P^2(K) : \nabla F(P) = \Big(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P) \Big) = (0, 0, 0) \Big\}.$$

Since F is homogeneous of degree 3, and $Z \nmid F$, we get

$$f(x, y) = F(x, y, 1),$$

and

$$F(X, Y, Z) = Z^3 f(\frac{X}{Z}, \frac{Y}{Z}).$$

This polynomial f is the affine form of F. The affine points $(x, y) \in A^2(K)$ on the original curve correspond to the points $(x : y : 1)$ in the projective plane as discussed above. To see what points on $X = V(F)$ lie at infinity, we set $Z = 0$ in $F(X, Y, Z) = 0$ and obtain $X^3 = 0$. This gives $X = 0$, and therefore $(0 : 1 : 0)$ is the only *point at infinity* which is denoted by O; namely $X \cap H_\infty = \{(0 : 1 :$

0)}. Now, we write the equation (1.2.1) using the affine coordinates $x = X/Z$, $y = Y/Z$,

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2.2}$$

Thus, the elliptic curve defined by E is then the set of solutions in $A^2(K)$, together with the extra point at infinity O. Now, we will give the main theorem associated to the isomorphism of two elliptic curves over K. The proof of this theorem can be found in [11].

Theorem 1.2.1. *Two elliptic curves $E_1(K)$ and $E_2(K)$ given by*

$$\begin{aligned} E_1 \ &: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 \ &: \ y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \end{aligned}$$

are isomorphic over K, denoted $E_1(K) \cong E_2(K)$, if and only if there exists $u, r, s, t \in K$, $u \neq 0$, such that the change of variables, so called admissible change of variables,

$$\psi \ : \ (x, y) \longmapsto (u^2x + r, \ u^3y + u^2sx + t) \tag{1.2.3}$$

transforms equation E_1 to equation E_2.

Proof. We refer the reader to the reference [11] to find the existence of ψ in case $E_1(K) \cong E_2(K)$. For the other implementation we note that the change of variables transforms equation E_1 to equation E_2, then the change of variables

$$\phi \ : \ (x, y) \longmapsto \big(u^{-2}(x - r), \ u^{-3}(y - sx - t + rs)\big) \tag{1.2.4}$$

associated to map ψ in (1.2.3) transforms equation E_2 to equation E_1, and ϕ is the inverse of the map ψ in the sense that $\psi \circ \phi = id_{E_1}$, $\phi \circ \psi = id_{E_2}$.

Since ψ, ϕ are morphisms of varieties and $\psi \circ \phi = id$, $\phi \circ \psi = id$ on E_1 and E_2, respectively, these affine varieties E_1 and E_2 are isomorphic over K. □

It can be checked that the existence of an admissible change of variables $\psi \ : \ (x,y) \longmapsto (u^2x+r,\ u^3y+u^2sx+t)$ is equivalent to the existence of common solution to the following equations in $u,r,s,t \in K,\ u \neq 0$:

$$\left.\begin{array}{rcl} u\bar{a}_1 & = & a_1+2s \\ u^2\bar{a}_2 & = & a_2-sa_1+3r-s^2 \\ u^3\bar{a}_3 & = & a_3+ra_1+2t \\ u^4\bar{a}_4 & = & a_4-sa_3+2ra_2-(t+rs)a_1+3r^2-2st \\ u^6\bar{a}_6 & = & a_6+ra_4+r^2a_2+r^3-ta_3-t^2-rta_1 \end{array}\right\} \tag{1.2.5}$$

For the details we refer the reader to [11]. We state this below:

Theorem 1.2.2. *Two elliptic curves $E_1(K)$ and $E_2(K)$ are isomorphic over K if and only if there exists $u,r,s,t \in K,\ u \neq 0$ satisfying the system of equations* (1.2.5).

Example: Let's consider the elliptic curves $E_1(F_5)$ and $E_2(F_5)$ as follows;

$$\begin{aligned} E_1(F_5) \ &: \ y^2 = x^3+2 \\ E_2(F_5) \ &: \ y^2 = x^3+3 \end{aligned}$$

It follows from the system of equations (1.2.5) that E_1 and E_2 are isomorphic over F_5^* if and only if $3u^6 = 2$ has a solution in F_5^*. Since $u = 2$ and $u = 3$ are solutions of $3u^6 = 2$ in F_5^*, these two curves are isomorphic. However, these two curves are not isomorphic over F_7^* because the corresponding equation $3u^6 = 2$ does not have any solution in F_7^*.

1.3 The Discriminant and j-Invariant

Let E be an elliptic curve over K given by the equation

$$E \ : \ Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3,$$

The following quantities attached to E plays a crucial role in the theory:

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24d_4 \\ \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \qquad (1.3.6) \\ j(E) &= c_4^3/\Delta \qquad (1.3.7) \end{aligned}$$

The quantity Δ is called the *discriminant* of E, while $j(E)$ is called the *j-invariant* of E. The following two theorems explain the significance of these quantities. The proofs of these theorems can be found in [11].

Theorem 1.3.1. *The elliptic curve E is non-singular if and only if $\Delta \neq 0$.*

Theorem 1.3.2. *If two elliptic curves $E_1(K)$ and $E_2(K)$ are isomorphic over K, then $j(E_1) = j(E_2)$. The converse is also true if K is an algebraically closed field.*

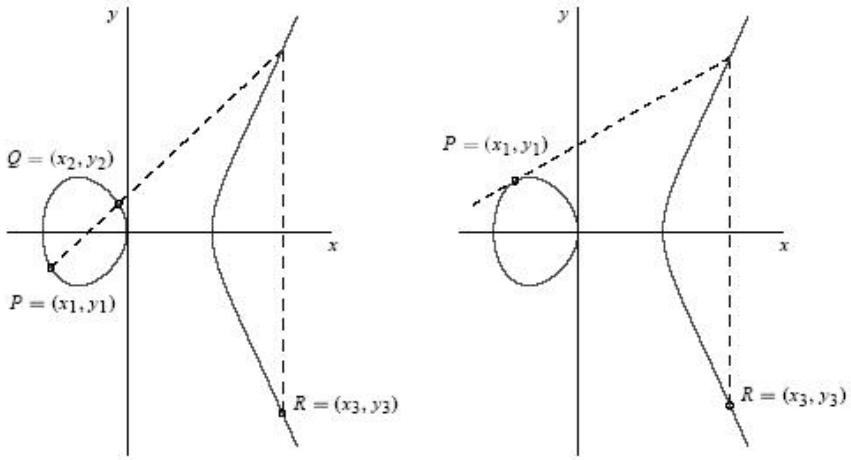
1.4 The Group Structure of an Elliptic Curve

Let K be any field and let E be an elliptic curve over K given by the equation (1.2.2)

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the points on E with $P, Q \neq O$. Let L be the line connecting P and Q (if $P = Q$, then L will be taken to be the tanjent line to E), and $R^{'}$ be the third point of intersection of L with E. Let $L^{'}$ be the line connecting $R^{'}$ and O. Then, $P + Q = R$ is defined as the unique point which is symmetric to the point $R^{'}$ with respect to the x-axis such that $L^{'}$ intersects E at $R^{'}$, O, and $P + Q$. This procedure is so called the **composition law**. Now,

we will derive an explicit formula for the coordinates of $P + Q = R = (x_3, y_3)$ in terms of the coordinates P and Q, where this law can be viewed over the field of real numbers by the following figure:



(a) Addition: $P + Q = R$. (b) Doubling: $P + P = R$.

Figure 1.1: Geometric addition and doubling of elliptic curve points

If $P \neq Q$, then it is clear that the line L passing through P and Q intersects the curve in one and only one third point say $R^{'}$.

Let λ represent the slope of the line passing through P and Q, then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad if\ x_1 \neq x_2.$$

We know that the line L passes through P, Q and intersects the curve E at a third point $R^{'} = (x_3, -y_3 - a_1x_3 - a_3)$. The equation of the line L is $y = \lambda x + \beta$. The sum of the roots of a monic polynomial is equal minus coefficient of the second-to-highest power. In our case, we have $y = \lambda x + \beta$. Substituting in equation (1.2.2), we get

$$(\lambda x + \beta)^2 + a_1x(\lambda x + \beta) + a_3(\lambda x + \beta) = x^3 + a_2x^2 + a_4x + a_6,$$

which gives

$$x^3 + (a_2 - a_1\lambda - \lambda^2)x^2 + (a_4 - a_1\beta - 2\lambda\beta - a_3\lambda)x + (a_6 - \beta^2 - a_3\beta) = 0$$

in which, the coefficient of x^2 is $a_2 - a_1\lambda - \lambda^2$ and the leading coefficient is 1. Thus,

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$$

we conclude that the third root in this case is

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

this leads to an expression for x_3, and since $R^{'} = (x_3, -y_3 - a_1x_3 - a_3)$ is on the line L, it satisfies $y = \lambda x + \beta$. Hence, we get

$$y_3 = -(\lambda + a_1)x_3 - \beta - a_3$$

In the case that $x_1 = x_2$ but $y_1 \neq y_2$, the line L through P and Q is a vertical line. Therefore, these two points P and Q intersects E in the infinity point O. Reflecting O across the x-axis yields the same point O. So, in this case $P+Q = O$.

If $P = Q$, then we take L to be the tangent line to the curve E at P. Therefore, λ is simply the derivative $\frac{\partial y}{\partial x}$ at P. Differentiating equation (1.2.2) gives

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Thus, the other point $P + P = R = (x_3, y_3)$ is as the following:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - 2x_1 \\ y_3 &= -(\lambda + a_1)x_3 - \beta - a_3 \end{aligned}$$

By using the above procedure, we will give the theorems whose proofs can be found in [11].

Theorem 1.4.1. *The* **composition law** *has the following properties:*
(i) If a line L intersects E at any points P, Q, R, then $(P + Q) + R = O$.
(i) $O + P = P$ and $P + O = P$ for all $P \in E$.
(iii) $-O = O$.
(iv) If $P = (x_1, y_1) \neq O$, then $-P = (x_1, -y_1 - a_1x_1 - a_3)$.
(v) If $Q = -P$, then $P + Q = O$.
(vi) $P + Q = Q + P$ for all $P \in E$.
(vii) $(P + Q) + R = P + (Q + R)$ for all $P, Q, R \in E$.

Theorem 1.4.2. *$(E(K), +)$ is an abelian group with identity element O.*

Example: To illustrate the addition law, consider the elliptic curve E on $\mathbb{R}$ given by

$$E \ : \ y^2 = x^3 - 16x + 16.$$

Let $P_1 = (0, 4)$, $P_2 = (1, 1)$. Then, we will find $P_1 + P_2$ and $2P_1$. Using the procedure explained above, we have

$$P_1 = (0, 4) \Rightarrow x_1 = 0, \ y_1 = 4$$
$$P_2 = (1, 1) \Rightarrow x_2 = 1, \ y_2 = 1.$$

Since $P_1 \neq P_2$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1 - 4}{1 - 0} = -3.$$

Then, we get $x_3 = (-3)^2 - 1 = 8$ and $y_3 = (-3)(-8) - 4 = 20$. Therefore, $P_1 + P_2 = (8, \ 20)$. Now, we will find $2P_1$, so we use the other case (i.e. $P_1 = P_2$)

$$\lambda = \frac{3x_1^2 - 16}{2y_1} = \frac{-16}{8} = -2.$$

Then, we get $x_3 = (-2)^2 = 4$ and $y_3 = (-2)(-4) - 4 = 4$. Therefore, $2P_1 = (4, \ 4)$. Using P_1, $2P_1$, we can find $3P_1$, $4P_1$, $5P_1$,..., and so on applying

the same method.

Now if $E_1(K)$ and $E_2(K)$ are isomorphic elliptic curves, then there exists an admissible change of variables $\psi : (x, y) \longmapsto (u^2x + r,\ u^3y + u^2sx + t)$ which transforms equation E_1 to equation E_2. It can be checked that this map ψ preserves the + operation, namely $\psi(P + Q) = \psi(P) + \psi(Q)$, and thus ψ is also an isomorphism of the groups $(E_1(K), +)$ and $(E_2(K), +)$. This gives us the next theorem [11].

Theorem 1.4.3. *If the elliptic curves $E_1(K)$ and $E_2(K)$ are isomorphic as elliptic curves, then they are also isomorphic as abelian groups, and therefore as abelian varieties.*

Example: The converse of the statement in Theorem 1.4.3 is not in general true, and in fact the elliptic curves $y^2 = x^3 + 1$ and $y^2 = x^3 + 2$ over F_5 are isomorphic as group but not isomorphic as elliptic curves because there is no admissible change of variables as in (1.2.3) satisfying the set of equations (1.2.5).

1.5 Some Properties over Finite Fields

We list some of the important properties of elliptic curves E over the finite field $K = F_q$.

If E is given by a Weierstrass equation (1.2.2), then since this equation has at most 2 solutions for each choice of $x \in F_q$, we have atmost $2q$ points in $A^2(K) = K \times K$ and one more point at infinity O, thus $\#E \leq 2q + 1$. The following theorem improves the above bound on the size of E, whose proof is given in [11].

Theorem 1.5.1 (Hasse's Theorem). *Let $n = \#E(F_q)$. Then $|(q+1) - n| \leq 2\sqrt{q}$.*

If E is an elliptic curve over F_q, then E can also be viewed as an elliptic curve over any finite extension field F_{q^m} of F_q. We next mention a useful result that

enables one to compute $\#E(F_{q^m})$ from $\#E(F_q)$. This result, which was proved by Hasse in 1934, is a specialization to elliptic curves of the Weil Conjecture concerning the number of points on varieties defined over finite fields. The proof of below theorem can be found in [11].

Theorem 1.5.2 (Weil Conjecture). *Let E be an elliptic curve over F_q, and let $N_m = \#E(F_{q^m})$, $m \geq 1$. Define the zeta function $Z(T) = e^{\sum_{m=1} \frac{N_m T^m}{m}}$. Then*

$$Z(T) = \frac{1 - tT + qT^2}{(1-T)(1-qT)}$$

where $t = q+1-N_1$. Let α, β be the complex numbers such that $(1-tT+qT^2) = (1-\alpha T)(1-\beta T)$. Then $N_m = q^m + 1 - \alpha^m - \beta^m$, $m \geq 1$.

The elliptic curve over F_q, where $q = p^m$ is said to be *supersingular* if p divides t, where $\#E(F_q) = q+1-t$. Otherwise, it is called *non-supersingular*. It is well-known that if $p = 2$ or if $p = 3$, then E is supersingular if and only if $j(E) = 0$. This is proved in [13].

We have seen that $E(F_q)$ is an abelian group. The next result further describes the structure of this group. C_m denotes the cyclic group on m elements. Now, we recall some standard results from abelian group theory. Every finite abelian group G can be decomposed into a direct sum of cyclic groups

$$G \ = \ C_{n_1} \oplus C_{n_2} \oplus \ldots \oplus C_{n_s},$$

where $n_{i+1} \mid n_i$ for all $i \ = \ 1, 2, ..., s-1$ and $n_s \geq 2$. Furthermore, this decomposition is unique. For the elliptic curves we have the following whose proof can be found in [11].

Theorem 1.5.3. *$E(F_q) \cong C_{n_1} \times C_{n_2}$, where n_1 and n_2 are integers, with n_2 dividing n_1. Morever, n_2 divides $q-1$.*

Chapter 2

Isomorphism Classes of Elliptic Curves over Finite Fields of Characteristic Two

In this chapter, we obtain the isomorphism classes of elliptic curves over finite fields $K = F_{2^m}$ and give a representative of each isomorphism class of these curves. We also determine $\#E(F_{2^m})$ for each supersingular curve E defined over F_{2^m}.

2.1 Introduction

In this section , we discuss some of the known results on isomorphism classes of elliptic curves over finite fields. We begin with a definition. Let $\left(\frac{a}{b}\right)$ denotes the usual Jacobi symbol, and let

$$\left(\frac{a}{2}\right) = \begin{cases} 1, & \text{if } a \equiv \pm 1 \pmod 8 \\ 0, & \text{if } a \equiv 0 \pmod 2 \\ -1, & \text{if } a \equiv \pm 3 \pmod 8 \end{cases}$$

Waterhouse [9] (see also Schoof [5]) counted the number of isomorphism classes of elliptic curves defined over the finite field F_q by first determining which rings can occur as the endomorphism ring of some elliptic curve, and then counting the number of isomorphism classes of elliptic curves with a given endomorphism ring. He also proceeded to determine the number of isomorphism classes of elliptic

curves over F_q, denoted by $N_q(t)$, such that $\#E(F_q) = q + 1 - t$. The results obtained are the following [5]:

Theorem 2.1.1. *Let F_q be a finite field. Then, the number of isomorphism classes of elliptic curves over F_q equals*

$$N_q = 2q + 3 + \Big(\frac{-4}{q}\Big) + 2\Big(\frac{-3}{q}\Big).$$

Theorem 2.1.2. *Let p be a prime and $q = p^m$. Let t be an integer with $|t| \leq 2\sqrt{q}$. Then,*

$$N_q(t) = \begin{cases} H(t^2 - 4q) & \text{if } t^2 < 4q \text{ and } p \nmid t \\ H(-4p) & \text{if } t = 0 \text{ and } m \text{ odd} \\ 1 & \text{if } t^2 = 2q,\ p = 2 \text{ and } m \text{ odd} \\ 1 & \text{if } t^2 = 3q,\ p = 3 \text{ and } m \text{ odd} \\ \frac{1}{12}\left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right) & \text{if } t^2 = 4q \text{ and } m \text{ even} \\ 1 - \left(\frac{-3}{p}\right) & \text{if } t^2 = q \text{ and } m \text{ even} \\ 1 - \left(\frac{-4}{p}\right) & \text{if } t = 0 \text{ and } m \text{ even} \\ 0 & \text{if otherwise.} \end{cases}$$

Here, $H(\Delta)$ denotes the Kronecker class number of Δ and it is the number of $SL_2(\mathbb{Z})$-orbits of positive definite binary quadratic forms of discriminant Δ, where Δ is a negative integer congruent to 0 or 1 modulo 4. One method of computing $H(\Delta)$ follows from the fact that $H(\Delta) = \#B\ (\Delta)$, where

$$\begin{aligned} B\ (\Delta)\ = \big\{(a,b,c) \in \mathbb{Z}^3\ :\ a > 0,\ \Delta = b^2 - 4ac,\ |b| \leq a \leq c, \\ \text{and } b \geq 0 \text{ whenever } a = |b| \text{ or } a = c\big\}. \end{aligned}$$

It is clear that if $(a,b,c) \in B\ (\Delta)$, then $a \leq \sqrt{|\Delta|/3}$ and so $B\ (\Delta)$ is a finite set. For more details of binary quadratic forms, their relationship of elliptic curves and a table of $H(\Delta)$ for small values of $-\Delta$, consult [5].

A simple proof of Theorem 2.1.2 and also a representative of each isomorphism class of elliptic curves over $F(q)$, $q = 2^m$ has been studied in [12]. Our aim is to give the details of that work. The only background needed to understand the proofs will be some elementary results on finite fields. We are able to simplify the proofs by using Theorem 1.2.2 associated with the definition of isomorphism. Lenstra [8] used a similar approach to count the isomorphism classes of elliptic curves over finite fields of characteristic greater than 3.

Now, we will summarize some elementary results on finite fields (for more details, consult [10]). These results will play very important role classifying the isomorphism classes of elliptic curves of charecteristic 2.

For α in F_{2^m}, the *trace function* Tr denotes the F_2-linear function $Tr : F_{2^m} \longrightarrow F_2$ defined by

$$Tr : \alpha \longmapsto \alpha + \alpha^2 + \alpha^{2^2} + \ldots + \alpha^{2^{m-1}}.$$

It is clear that the trace function satisfies the following properties:
(i) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$ for all $\alpha, \beta \in F_{2^m}$.
(ii) $Tr(\alpha^2) = Tr(\alpha)$ for all $\alpha \in F_{2^m}$.

For α in F_{2^m} where m is even, the *half-trace function* Te denotes the F_4-linear function $Te : F_{2^m} \longrightarrow F_4$ defined by

$$Te : \alpha \longmapsto \alpha + \alpha^{2^2} + \alpha^{2^4} + \ldots + \alpha^{2^{m-2}}.$$

Since x^2+x+1 is the only irreducible polynomial over F_2, $F_4 = F_2[x]/\langle x^2 + x + 1\rangle$ Let $c_1, c_2 \in F_4$ be roots of the irreducible polynomials $x^2 + x + 1 \in F_2[x]$. Then, the elements of F_4 are denoted by $0, 1, c_1$ and c_2. Since $x^2+x+1 = (x-c_1)(x-c_2)$, we get the identities $c_1^2 + c_1 + 1 = 0$, $c_2^2 + c_2 + 1 = 0$, $c_1c_2 = 1$ and $c_1 + c_2 = 1$. We have also $Te(c_1\alpha) = c_1Te(\alpha)$ and $Te(c_2\alpha) = c_2Te(\alpha)$ for $\alpha \in F_{2^m}$.

Now, we will define the quadratic and quartic equations in F_{2^m} and discuss the conditions that these equations have solutions in F_{2^m}. These conditions are obtained by Menichetti in [7].

Using the general results in [7] concerning the number of roots of an affine polynomial over a finite field, we obtain the following special cases:

The quadratic equation over F_{2^m}

$$x^2 + ax + b = 0, \qquad a, b \in F_{2^m}, \quad a \neq 0, \tag{2.1.1}$$

has a solution in F_{2^m} if and only if $Tr(a^{-2}b) = 0$. If x_1 is one solution, then the other solution is $x_1 + a$.

Consider now the quartic equation over F_{2^m}

$$x^4 + ax + b = 0, \qquad a, b \in F_{2^m}, \quad a \neq 0, \tag{2.1.2}$$

then, we have the following:

(i) If m is odd, then (2.1.2) has either no solution or exactly two solutions.
(ii) If m is even and a is not a cube, then (2.1.2) has exactly one solution.
(iii) If m is even and a is a cube, then if $Te(b/a^{4/3}) = 0$, the equation (2.1.2) has four solutions , and if $Te(b/a^{4/3}) \neq 0$, the equation (2.1.2) has no solutions.

2.2 Elliptic Curves over F_{2^m}

Let K be a field of characteristic 2, and let $E(K)$ be the elliptic curve given by the Weierstrass equation

$$E \ : \ y^2 + \bar{a}_1 xy + \bar{a}_3 y = x^3 + \bar{a}_2 x^2 + \bar{a}_4 x + \bar{a}_6.$$

When we specialize (1.3.7) in F_{2^m}, we find that $j(E) = (\bar{a}_1)^{12}/\Delta$. Since E is non-singular, $\Delta \neq 0$.

• If $j(E) \neq 0$, then $\bar{a}_1 \neq 0$. Therefore, the admissible change of variables

$$(x, y) \longrightarrow \Big(\bar{a}_1^2 x + \frac{\bar{a}_3}{\bar{a}_1}, \ \bar{a}_1^3 y + \frac{\bar{a}_1^2 \bar{a}_4 + \bar{a}_3^2}{\bar{a}_1^3}\Big)$$

transforms E to the curve

$$E_1 \ : \ y^2 + xy = x^3 + a_2x^2 + a_6.$$

For E_1, $\Delta = a_6 \neq 0$ and $j(E_1) = 1/a_6$.

- If $j(E) = 0$, then $\bar{a}_1 = 0$. Therefore, the admissible change of variables

$$(x, y) \longrightarrow (x + \bar{a}_2, \ y)$$

transforms E to the curve

$$E_2 \ : \ y^2 + a_3y = x^3 + a_4x + a_6.$$

For E_2, $\Delta = a_3^4$, $a_3 \neq 0$ and $j(E_2) = 0$.

Addition Formula when $j(E) \neq 0$

Let $P = (x_1, y_1) \in E_1$; then it is clear that $-P = (x_1, y_1 + x_1)$. If $Q = (x_2, y_2) \in E_1$ and $Q \neq -P$, then $P + Q = (x_3, y_3)$. Now we will find that x_3 and y_3 using the structure in Section (1.4).

If $P \neq Q$, then the line L passing through P and Q intersects the curve in one and only one third point $R^{'} = (x_3, y_3 + x_3)$. We get

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2, \qquad \lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

and since $R^{'} = (x_3, y_3 + x_3)$ satisfies the line $y = \lambda x + \beta$, we get

$$y_3 = (\lambda + 1)x_3 + \beta$$

As $P = (x_1, y_1) \in E_1$ satisfies the line L, we can write $\beta = \lambda x_1 + y_1$. Therefore,

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

If $P = Q$, then $x_1 = x_2$ and λ is simply the derivative $\frac{\partial y}{\partial x}$ at P. Hence, we get

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2, \qquad \lambda = x_1 + \frac{y_1}{x_1}$$

and since $R^{'} = (x_3, y_3 + x_3)$ satisfies the line $y = \lambda x + \beta$, we get

$$y_3 = x_1^2 + \lambda x_3 + x_3$$

If we rewrite the point $P + Q = R = (x_3, y_3)$, we obtain

$$x_3 = \begin{cases} (\frac{y_1 + y_2}{x_1 + x_2})^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2, & \text{if } P \neq Q \\ \\ x_1^2 + \frac{a_6}{x_1^2}, & \text{if } P = Q \end{cases}$$

and

$$y_3 = \begin{cases} (\frac{y_1 + y_2}{x_1 + x_2})(x_1 + x_3) + x_3 + y_1, & \text{if } P \neq Q \\ \\ x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3, & \text{if } P = Q \end{cases}$$

Addition Formula when $j(E) = 0$

Let $P = (x_1, y_1) \in E_2$; then it is clear that $-P = (x_1, y_1 + a_3)$. If $Q = (x_2, y_2) \in E_2$ and $Q \neq -P$, then $P + Q = R = (x_3, y_3)$. We find that x_3 and y_3 using the structure in Section (1.4) as follows

$$x_3 = \begin{cases} (\frac{y_1 + y_2}{x_1 + x_2})^2 + x_1 + x_2, & \text{if } P \neq Q \\ \\ \frac{x_1^4 + a_4^2}{a_3^2}, & \text{if } P = Q \end{cases}$$

and

$$y_3 = \begin{cases} (\frac{y_1+y_2}{x_1+x_2})(x_1+x_3)+y_1+a_3, & \text{if } P \neq Q \\ \\ (\frac{x_1^2+a_4}{a_3})(x_1+x_3)+y_1+a_3, & \text{if } P = Q \end{cases}$$

From the addition formula, it is evident that the number of field operations involved in adding two points is about the same when $j(E) = 0$ or when $j(E) \neq 0$. If we choose a curve of *j-invariant* equal to 0 with $a_3 = 1$, then the number of field operation is significantly reduced. This helps explain our special interest in curves of *j-invariant* equal to 0.

2.3 Isomorphism Classes of $E(F_{2^m})$, $j(E) \neq 0$

Let $E_1(K)$ and $E_2(K)$ be elliptic curves with non-zero *j-invariants*. It follows from Section (2.2) that these curves upto isomorphism are given by the equations:

$$\begin{aligned} E_1 &: y^2+xy = x^3+a_2x^2+a_6, \qquad \Delta = a_6 \neq 0, \qquad j(E_1) = 1/a_6 \\ E_2 &: y^2+xy = x^3+\bar{a}_2x^2+\bar{a}_6, \qquad \Delta = \bar{a}_6 \neq 0, \qquad j(E_2) = 1/\bar{a}_6 \end{aligned}$$

Using the theorem (1.2.2), we find that $E_1(K) \cong E_2(K)$ if and only if $a_6 = \bar{a}_6$ and there exists $s \in K$ such that $\bar{a}_2 = a_2 + s + s^2$. We know that from (2.1.1) the latter condition is equivalent to having $Tr(\bar{a}_2 + a_2) = 0$, i.e., $Tr(\bar{a}_2) = Tr(a_2)$. Thus, $E_1(K) \cong E_2(K)$ if and only if $a_6 = \bar{a}_6$ and $Tr(\bar{a}_2) = Tr(a_2)$.

Since $Tr(a_2)$ takes 2 values 0 and 1 and there exists $q-1$ values for $a_6 \neq 0$ in F_q, where $q = 2^m$, we obtain the following

Theorem 2.3.1. *There are $2(q-1)$ isomorphism classes of elliptic curves with non-zero j-invariant over F_q, where $q = 2^m$, $m \geq 1$. In fact, the set of representatives of the isomorphism classes is given by*

$$\Big\{ y^2+xy = x^3+a_2x^2+a_6 \mid a_6 \in F_{2^m}^*,\ a_2 \in \{0, \gamma\} \Big\},$$

where γ is an element of F_{2^m} such that $Tr(\gamma) = 1$. Note that, if m is odd, γ can be taken obviously as 1.

We know that the trace of the half of the elements in F_{2^m} are 0 and the others are 1; so, the $q/2$ curves isomorphic to E_1 are the curves $y^2 + xy = x^3 + \alpha x^2 + a_6$, where α ranges over the $q/2$ elements of F_{2^m} which satisfy $Tr(\alpha) = Tr(a_2)$.

2.4 Isomorphism Classes of $E(F_{2^m})$ when m is odd and $j(E) = 0$

If m is odd, then $2^m - 1 \equiv 1 \pmod 3$. This implies that $3 \nmid 2^m - 1$. Hence, $F_{2^m}^*$ has no elements of order 3, and so the map $f : F_{2^m}^* \longrightarrow F_{2^m}^*$ defined by $f : x \longmapsto x^3$ is 1-1. Infact, if $x,\ y$ are in $F_{2^m}^*$ such that $f(x) = f(y)$, then we get

$$x^3 = y^3 \Rightarrow (xy^{-1})^3 = 1$$

This gives $xy^{-1} = 1$ and so $x = y$. In this case we see that $x \mapsto x^3$ is a bijective map on $F_{2^m}^*$, and therefore we get a unique cube root $\sqrt[3]{\alpha}$ of any $\alpha \in F_{2^m}^*$.

Let $E^{'}$ be the curve given by the equation

$$E^{'} : y^2 + a_3^{'}y = x^3 + a_4^{'}x + a_6^{'} \qquad (a_3^{'} \neq 0).$$

Let $r = \sqrt[3]{a_3^{'}}$. Then the admissible change of variables $(x, y) \longrightarrow (r^2x,\ r^3y)$ transforms $E^{'}$ to a curve given by

$$E : y^2 + y = x^3 + a_4x + a_6. \tag{2.4.3}$$

Thus, we can assume that any elliptic curve over F_{2^m} where m is odd (with $j(E) = 0$) has the form (2.4.3). If $\bar{E}$ is the curve given by

$$\bar{E} : y^2 + y = x^3 + \bar{a}_4x + \bar{a}_6,$$

then, using the theorem (1.2.2), we see that $E \cong \bar{E}$ over F_{2^m} if and only if there exists $s = s_1,\ t = t_1 \in F_{2^m}$ satisfying the equations

$$s^4 + s + a_4 + \bar{a}_4 = 0 \tag{2.4.4}$$

$$t^2 + t + s^6 + a_4 s^2 + a_6 + \bar{a}_6 = 0 \tag{2.4.5}$$

The admissible change of variables which tranforms the equation E into the equation $\bar{E}$ is of the form $\psi : (x, y) \longrightarrow (x + s^2,\ y + sx + t)$, where $s, t \in F_{2^m}$. This gives us the isomorphism $\psi : E \to \bar{E}$.

Let E_1 be the elliptic curve over F_{2^m} given by

$$E_1 \ : \ y^2 + y = x^3,$$

and let E be any elliptic curve over F_{2^m} given by the form (2.4.3)

$$E \ : \ y^2 + y = x^3 + a_4 x + a_6,$$

which is isomorphic to E_1. Then, there exists $s_1, t_1 \in F_{2^m}$, satisfying the equations

$$s^4 + s + a_4 = 0 \tag{2.4.6}$$

$$t^2 + t + s^6 + a_6 = 0 \tag{2.4.7}$$

Now, we proceed to count the number of admissible change of variables which transform E to E_1. We achieve this by counting the total number of solutions (s, t) to the equation (2.4.6) and (2.4.7). This leads us to the number of elliptic curves E isomorphic to E_1.

Using the quartic equation (2.1.2), we see that the equation (2.4.6) has always two solutions $s = s_1$ and $s = s_1 + 1$ in F_{2^m}, because m is odd. On the other hand, since (s_1, t_1) is a solution to the quadratic equation (2.4.7), we have $Tr(s_1^6 + a_6) = 0$.

However,

$$\begin{aligned} Tr\big((s_1+1)^6+a_6\big) &= Tr\big(s_1^6+s_1^4+s_1^2+1+a_6\big) \\ &= Tr\big(s_1^6+a_6\big)+Tr\big(s_1^4+s_1^2+1\big) \\ &= Tr\big(s_1^4\big)+Tr\big(s_1^2\big)+1 \\ &= 1 \end{aligned}$$

because $Tr\big(s_1^4\big) = Tr\big(s_1^2\big)$ for any $s_1 \in F_{2^m}$. Therefore, there are exactly two solutions (s_1, t_1) and (s_1, t_1+1) to the equations (2.4.6) and (2.4.7).

Since s and t are free in F_{2^m}, there are q^2 admissible change of variables. Therefore, there are $q^2/2$ elliptic curves isomorphic to E_1. Since both a_4 and a_6 can take q values, there are q^2 elliptic curves over F_{2^m} when m is odd. So, the number of elliptic curves isomorphic to E_1 is only half of the total elliptic curve over F_{2^m} when m is odd.

Let E_2 be the elliptic curve over F_{2^m} given by

$$E_2 \ : \ y^2+y = x^3+x.$$

Note that $E_2 \ncong E_1$, because the equation

$$s^2+s+1 = 0$$

has no solution when m is odd. Now, we are going to count the elliptic curves

$$E \ : \ y^2+y = x^3+a_4x+a_6,$$

which is isomorphic to E_2. If $E \cong E_2$, then there exists $s_1, t_1 \in F_{2^m}$, satisfying the equations

$$s^4+s+1+a_4 = 0 \tag{2.4.8}$$

$$t^2+t+s^6+s^2+a_6 = 0 \tag{2.4.9}$$

The quartic equation (2.4.8) has always two solutions $s = s_1$ and $s = s_1 + 1$ in F_{2^m} by (2.1.2). Since $t = t_1$ is a solution of the quadratic equation (2.4.9) associated to the choice $s = s_1$ in (2.4.9), we get $Tr(s_1^6 + s_1^2 + a_6) = 0$. This gives

$$\begin{aligned} Tr\big((s_1+1)^6 + (s_1+1)^2 + a_6\big) = Tr\big(s_1^6 + s_1^4 + a_6\big) &= Tr\big(s_1^4\big) + Tr\big(s_1^2\big) \\ &= 0 \end{aligned}$$

Thus, there are 4 solutions (s_1, t_1), (s_1+1, t_1), (s_1, t_1+1) and (s_1+1, t_1+1) to the equations (2.4.8) and (2.4.9). Since there are q^2 admissible change of variables, as mentioned above $q^2/4$ elliptic curves isomorphic to E_2. So, the number of elliptic curves isomorphic to E_2 is $1/4$ of the total elliptic curve over F_{2^m} when m is odd. It is clear that there are $q^2/4$ elliptic curves left.

Let E_3 be the elliptic curve over F_{2^m} given by

$$E_3 \ : \ y^2 + y = x^3 + x + 1.$$

It is easy to see that $E_1 \ncong E_3$ and $E_2 \ncong E_3$ by checking that the set of equations (1.2.5) have no solutions in F_{2^m}. Now, we will count the elliptic curves

$$E \ : \ y^2 + y = x^3 + a_4 x + a_6,$$

which is isomorphic to E_3. If $E \cong E_3$, then there exists $s = s_1, \ t = t_1 \in F_{2^m}$, satisfying the equations

$$s^4 + s + 1 + a_4 = 0 \tag{2.4.10}$$

$$t^2 + t + s^6 + s^2 + a_6 + 1 = 0 \tag{2.4.11}$$

The quartic equation (2.4.10) in s has always two solutions s_1 and $s_1 + 1$. Since $t = t_1$ is a solution of the quadratic equation (2.4.11) associated to the choice $s = s_1$ in (2.4.11), we get $Tr(s_1^6 + s_1^2 + a_6 + 1) = 0$.

This gives

$$\begin{aligned} Tr\big((s_1+1)^6+(s_1+1)^2+a_6+1\big) &= Tr\big(s_1^6+s_1^4+a_6+1\big) \\ &= Tr\big(s_1^4\big)+Tr\big(s_1^6+a_6+1\big) \\ &= Tr\big(s_1^4\big)+Tr\big(s_1^2\big) \\ &= 0 \end{aligned}$$

So, the quadratic in t associated to the choice $s = s_1 + 1$ has two solutions as well. It is clear that there are 4 solutions (s_1, t_1), $(s_1 + 1, t_1)$, $(s_1, t_1 + 1)$ and $(s_1 + 1, t_1 + 1)$ to the equations (2.4.10) and (2.4.11). Therefore, from the same reason as above, there are $q^2/4$ elliptic curves isomorphic to E_3.

We have accounted the number of non-isomorphic elliptic curves over F_{2^m} with zero *j-invariant*, where m is odd. We summarize this result as the next theorem.

Theorem 2.4.1. *There are* 3 *isomorphism classes of elliptic curves over* F_{2^m} *with* j*-invariant equal to* 0*, where* m *is odd. A representative from each class is:*
(i) $y^2 + y = x^3$
(ii) $y^2 + y = x^3 + x$
(iii) $y^2 + y = x^3 + x + 1$.

2.5 Isomorphism Classes of $E(F_{2^m})$ when m is even and $j(E) = 0$

In this section, we will prove that there are exactly seven isomorphism classes of elliptic curves over F_q, where $q = 2^m$, m even, with *j-invariant* equal to 0. We will also obtain a representative of each of these seven isomorphism classes in this section.

Recall that $F_4 = F_2[x]/(x^2 + x + 1) = \{0, 1, c_1, c_2\}$ and the *half-trace function*

Te denotes the F_4-linear function $Te : F_{2^m} \longrightarrow F_4$ defined by

$$Te : \alpha \longmapsto \alpha + \alpha^{2^2} + \alpha^{2^4} + \ldots + \alpha^{2^{m-2}}.$$

Now, we will define the cube elements in F_{2^m}, where m is even. If there exists any x in F_{2^m} such that $x^3 = a$, then a is said to be a cube in F_{2^m}. Since m is even, it is clear that $3 \mid 2^m - 1$. This gives that there exists an element of order 3 in $F_{2^m}^*$. Therefore, the map $f : F_{2^m}^* \longrightarrow F_{2^m}^*$ given by $x \longmapsto x^3$ is 3 - 1 map. In conclusion, when m is even, $F_{2^m}^*$ have $(q-1)/3$ cube elements.

Let E be the curve

$$E : y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad (a_3 \neq 0). \tag{2.5.12}$$

We will consider the following three types of curves:
Type I: a_3 is not a cube.
Type II: a_3 is a cube, and $Te(a_4) \neq 0$.
Type III: a_3 is a cube, and $Te(a_4) = 0$.

We note the following:

(a) For Type I; there are exactly $\big(2(q-1)q^2\big)/3$ elliptic curves, because a_4, a_6 are free and a_3 is not a cube.

(b) For Type II; there are exactly $\big((q-1)q^2\big)/4$ elliptic curves, because a_6 is free, a_3 is a cube and a_4 takes $3q/4$ values due to the fact that $Te : F_{2^m} \to F_4$ and $Te(a_4) \neq 0$.

(c) For Type III; there are exactly $\big((q-1)q^2\big)/12$ elliptic curves, because a_6 is free, a_3 is a cube and a_4 takes $q/4$ values due to the fact that $Te : F_{2^m} \to F_4$ and $Te(a_4) = 0$.

It follows from these results that $\big(2(q-1)q^2\big)/3 + \big((q-1)q^2\big)/4 + \big((q-1)q^2\big)/12 = (q-1)q^2$ which is the total number of elliptic curves over F_{2^m} when m is even.

Now, we will examine these 3 types of curves, respectively.

Type I Curves

Let E_1 be the Type I curve given by

$$E_1 \ : \ y^2 + a_3 y = x^3, \quad a_3 \neq 0 \textit{ and not a cube.}$$

and let $\bar{E}$ be any elliptic curve over F_{2^m} given by

$$\bar{E} \ : \ y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6, \quad \bar{a}_3 \neq 0$$

which is isomorphic to E_1. Then, by theorem (1.2.2), there exists an admissible change of variables in the form $(x, y) \longrightarrow (u^2 x + s^2,\ u^3 y + u^2 s x + t)$ and solutions $u = u_1, s = s_1, t = t_1 \in F_{2^m}$ of the equations

$$u^3 = a_3/\bar{a}_3 \tag{2.5.13}$$

$$s^4 + a_3 s + u^4 \bar{a}_4 = 0 \tag{2.5.14}$$

$$t^2 + a_3 t + s^6 + u^6 \bar{a}_6 = 0 \tag{2.5.15}$$

Since $\bar{a}_3 = a_3/u^3$ and a_3 is a non-cube, $\bar{a}_3$ is also a non-cube. Hence, $\bar{E}$ is also a Type I curve. We proceed to count the number of admissible change of variables which transform $\bar{E}$ to E_1. We achieve this by counting the total number of solutions (u, s, t) to the equations (2.5.13), (2.5.14) and (2.5.15). This leads us to the number of elliptic curves E isomorphic to E_1.

Now, (2.5.13) has exactly 3 solutions. Since $F_4 \subset F_{2^m}$, we can represent these solutions as u_1, $c_1 u_1$ and $c_2 u_1$. Since a_3 is a non-cube, (2.5.14) has exactly one solution for each choice of u by (2.1.2). These unique solutions to (2.5.14) are (u_1, s_1), $(c_1 u_1, c_1 s_1)$ and $(c_2 u_1, c_2 s_1)$. For each choice of the pairs (u, s), there are always 2 solutions $t = t_1$ and $t = t_1 + a_3$ to (2.5.15). So, there are 6 solutions of the equations (2.5.13), (2.5.14) and (2.5.15) in F_{2^m}.

Since $u \neq 0$ and s, t are free in F_{2^m}, there are $(q-1)q^2$ admissible change of variables. Therefore, the number of elliptic curves isomorphic to E_1 is $(q-1)q^2/6$. Since $a_3 \neq 0$ and not a cube takes $2(q-1)/3$ values, a_4 and a_6 take q values,

there are $2(q-1)q^2/3$ Type I elliptic curves over F_{2^m} when m is even. So, the number of elliptic curves isomorphic to E_1 is $1/4$ of the total Type I elliptic curve over F_{2^m} when m is even.

Let E_2 be the Type I curve given by

$$E_2 \ : \ y^2 + b_3 y = x^3 + b_6, \quad b_3 \neq 0 \textit{ and not a cube, } Tr\big(b_3^{-2} b_6\big) = 1$$

Note that $E_2 \ncong E_1$, because the equations

$$\begin{aligned} u^3 &= a_3/b_3 \\ s^4 + a_3 s &= 0 \\ t^2 + a_3 t + s^6 + u^6 b_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $s^4 + a_3 s = 0$ has always only one solution $s = 0$, because a_3 is a non-cube. This implies the latter equation has no solution, because $Tr(a_3^{-2} u^6 b_6) = Tr(b_3^{-2} b_6) = 1$.

Now, we are going to count the elliptic curves

$$\bar{E} \ : \ y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6, \quad \bar{a}_3 \neq 0$$

which is isomorphic to E_2. Then, by theorem (1.2.2), there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$, satisfying the equations

$$u^3 = b_3/\bar{a}_3 \tag{2.5.16}$$

$$s^4 + b_3 s + u^4 \bar{a}_4 = 0 \tag{2.5.17}$$

$$t^2 + b_3 t + s^6 + u^6 \bar{a}_6 + b_6 = 0 \tag{2.5.18}$$

Now, (2.5.16) has exactly 3 solutions , namely u_1, $c_1 u_1$ and $c_2 u_1$. Since b_3 is a non-cube, (2.5.17) has exactly one solution for each choice of u by (2.1.2). These unique solutions to (2.5.17) are (u_1, s_1), $(c_1 u_1, c_1 s_1)$ and $(c_2 u_1, c_2 s_1)$. For each choice of the pairs (u, s), there are always 2 solutions $t = t_1$ and $t = t_1 + b_3$ to

(2.5.18). So, there are 6 solutions of the equations (2.5.16), (2.5.17) and (2.5.18) in F_{2^m}.

Since there are $(q-1)q^2$ admissible change of variables, as mentioned above $(q-1)q^2/6$ elliptic curves isomorphic to E_2. So, the number of elliptic curves isomorphic to E_2 is 1/4 of Type I elliptic curves over F_{2^m} when m is even.

Let E_3 be the Type I elliptic curve given by

$$E_3 \ : \ y^2 + a_3^2 y = x^3, \quad a_3 \neq 0 \textit{ and not a cube}$$

Note that $E_3 \ncong E_1$, because the equations

$$\begin{aligned} u^3 &= a_3/a_3^2 \\ s^4 + a_3 s &= 0 \\ t^2 + a_3 t + s^6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $u^3 = a_3^{-1}$ has no solution, because the inverse of the non-cube element is also non-cube.

Note also that $E_3 \ncong E_2$, because the equations

$$\begin{aligned} u^3 &= a_3^2/b_3 \\ s^4 + a_3^2 s &= 0 \\ t^2 + a_3^2 t + s^6 + u^6 b_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $s^4 + a_3^2 s = 0$ has always only one solution $s = 0$, because a_3 is a non-cube. This implies the latter equation has no solution, because $Tr(a_3^{-4} u^6 b_6) = Tr(b_3^{-2} b_6) = 1$.

Now, we are going to count the elliptic curves

$$\bar{E} \ : \ y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6, \quad \bar{a}_3 \neq 0 \textit{ and not a cube}$$

which is isomorphic to E_3. For $\bar{E} \cong E_3$, there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$,

satisfying the equations

$$\begin{aligned} u^3 &= a_3^2/\bar{a}_3 && (2.5.19)\\ s^4 + a_3^2 s + u^4\bar{a}_4 &= 0 && (2.5.20)\\ t^2 + a_3^2 t + s^6 + u^6\bar{a}_6 &= 0 && (2.5.21) \end{aligned}$$

Now, (2.5.29) has exactly 3 solutions, namely u_1, c_1u_1 and c_2u_1. Since a_3 is a non-cube, (2.5.20) has exactly one solution for each choice of u by (2.1.2). These unique solutions to (2.5.20) are (u_1, s_1), (c_1u_1, c_1s_1) and (c_2u_1, c_2s_1). For each choice of the pairs (u, s), there are always 2 solutions $t = t_1$ and $t = t_1 + a_3^2$ to (2.5.21). So, there are 6 solutions of the equations (2.5.19), (2.5.20) and (2.5.21) in F_{2^m}.

Since there are $(q-1)q^2$ admissible change of variables, as mentioned above $(q-1)q^2/6$ elliptic curves isomorphic to E_3. So, the number of elliptic curves isomorphic to E_3 is 1/4 of Type I elliptic curves over F_{2^m} when m is even.

Let E_4 be the Type I elliptic curve given by

$$E_4 \ : \ y^2 + b_3^2 y = x^3 + c_6, \quad b_3 \neq 0 \textit{ and not a cube, } Tr\big(b_3^{-4}c_6\big) = 1$$

Note that $E_4 \ncong E_1$, because the equations

$$\begin{aligned} u^3 &= a_3/b_3^2\\ s^4 + a_3 s &= 0\\ t^2 + a_3 t + s^6 + u^6 c_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $s^4 + a_3 s = 0$ has always only one solution $s = 0$, because a_3 is a non-cube. This implies the latter equation has no solution, because $Tr(a_3^{-2}u^6c_6) = Tr(b_3^{-4}c_6) = 1$.

Note that $E_4 \ncong E_2$, because the equations

$$\begin{aligned} u^3 &= b_3/b_3^2 \\ s^4 + b_3 s &= 0 \\ t^2 + b_3 t + s^6 + b_6 + u^6 c_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $u^3 = b_3^{-1}$ has no solution, because the inverse of the non-cube element is also non-cube.

Note also that $E_4 \ncong E_3$, because the equations

$$\begin{aligned} u^3 &= a_3^2/b_3^2 \\ s^4 + a_3^2 s &= 0 \\ t^2 + a_3^2 t + s^6 + u^6 c_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $s^4 + a_3^2 s = 0$ has always only one solution $s = 0$, because a_3 is a non-cube. This implies the latter equation has no solution, because $Tr(a_3^{-4} u^6 c_6) = Tr(b_3^{-4} c_6) = 1$.

Now, we are going to count the elliptic curves

$$\bar{E} \ : \ y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6, \quad \bar{a}_3 \neq 0 \textit{ and not a cube.}$$

which is isomorphic to E_4. For $\bar{E} \cong E_4$, there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$, satisfying the equations

$$u^3 = b_3^2/\bar{a}_3 \tag{2.5.22}$$

$$s^4 + b_3^2 s + u^4 \bar{a}_4 = 0 \tag{2.5.23}$$

$$t^2 + b_3^2 t + s^6 + c_6 + u^6 \bar{a}_6 = 0 \tag{2.5.24}$$

Now, (2.5.22) has exactly 3 solutions , namely u_1, $c_1 u_1$ and $c_2 u_1$. Since b_3 is a non-cube, (2.5.23) has exactly one solution for each choice of u by (2.1.2). These unique solutions to (2.5.23) are (u_1, s_1), $(c_1 u_1, c_1 s_1)$ and $(c_2 u_1, c_2 s_1)$. For each

choice of the pairs (u, s), there are always 2 solutions $t = t_1$ and $t = t_1 + b_3^2$ to (2.5.24). So, there are 6 solutions of the equations (2.5.22), (2.5.23) and (2.5.24) in F_{2^m}.

Since there are $(q-1)q^2$ admissible change of variables, as mentioned above $(q-1)q^2/6$ elliptic curves isomorphic to E_4. So, the number of elliptic curves isomorphic to E_4 is 1/4 of Type I elliptic curves over F_{2^m} when m is even.

Type II Curves

Let $E^{'}$ be the general form of the Type II (and later Type III) curves given by

$$E^{'} \ : \ y^2 + a_3^{'}y = x^3 + a_4^{'}x + a_6^{'}, \quad a_3^{'} \neq 0 \ \textit{and a cube},$$

Since $a_3^{'} = u^3$ is a cube, it can be check that the admissible change of variables $(x, y) \rightarrow (u^2x, u^3y)$ transforms $E^{'}$ into the Type II (and Type III) elliptic curves $\bar{E}$ given by

$$\bar{E} \ : \ y^2 + y = x^3 + \bar{a}_4 x + \bar{a}_6,$$

From now on, we can assume that the Type II (and later Type III) curves have the form

$$\bar{E} \ : \ y^2 + y = x^3 + \bar{a}_4 x + \bar{a}_6,$$

Let E_1 be the Type II curve given by

$$E_1 \ : \ y^2 + y = x^3 + a_4 x, \quad Te(a_4) = 1$$

Suppose that $\bar{E} \cong E_1$, then there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$, satisfying the equations

$$u^3 = 1 \tag{2.5.25}$$

$$s^4 + s + a_4 + u\bar{a}_4 = 0 \tag{2.5.26}$$

$$t^2 + t + s^6 + a_4 s^2 + \bar{a}_6 = 0 \tag{2.5.27}$$

Note that

$$Te(\bar{a}_4) = Te\Big(\frac{s^4+s+a_4}{u}\Big) = Te\Big(\frac{s^4}{u^4}\Big) + Te\Big(\frac{s}{u}\Big) + Te\Big(\frac{a_4}{u}\Big) = Te\Big(\frac{a_4}{u}\Big).$$

Since $u^3 = 1$, we have $u = 1, c_1$ *or* c_2. Therefore, $Te(a_4/u) = 1, c_2$ *or* c_1, respectively. Thus, $Te(\bar{a}_4) \neq 0$ and $\bar{E}$ is also a Type II curve. We proceed to count the number of admissible change of variables which transform $\bar{E}$ to E_1. We achieve this by counting the total number of solutions (u, s, t) to (2.5.25), (2.5.26) and (2.5.27) in F_{2^m}. This leads us to the number of the elliptic curves $\bar{E}$ isomorphic to E_1.

For each choice of u, the equation (2.5.26) has exactly 4 distinct solutions or no solution in F_{2^m}, according to whether $Te(a_4 + u\bar{a}_4) = 0$ or $Te(a_4 + u\bar{a}_4) \neq 0$, respectively. We find that for $u = 1, c_1, c_2$, the equation (2.5.26) has 4 solutions if and only if $Te(\bar{a}_4) = 1, c_2, c_1$, respectively. Without loss of generality, we can assume that $Te(\bar{a}_4) = 1$. Then, the equation

$$s^4 + s + a_4 + \bar{a}_4 = 0$$

has 4 distinct solutions, namely $s = s_1, s_1+1, s_1+c_1$ and s_1+c_2. There are always 2 solutions to (2.5.27) in t. If (s_1, t_1) and $(s_1, t_1 + 1)$ are solutions to (2.5.27), then we have

$$Tr(s_1^6 + a_4 s_1^2 + \bar{a}_6) = 0.$$

Since the trace $Tr_{F_{2^m}/F_2}$ is the composition of the half trace $Te_{F_{2^m}/F_4}$ and the trace Tr_{F_4/F_2}, we get

$$\begin{aligned}
Tr\Big((s_1+1)^6 + a_4(s_1+1)^2 + \bar{a}_6\Big) &= Tr(a_4) = 0, \\
Tr\Big((s_1+c_1)^6 + a_4(s_1+c_1)^2 + \bar{a}_6\Big) &= Tr(c_2 a_4) = 1, \\
Tr\Big((s_1+c_2)^6 + a_4(s_1+c_2)^2 + \bar{a}_6\Big) &= Tr(c_1 a_4) = 1.
\end{aligned}$$

Thus, the equation (2.5.27) has solutions only when $s = s_1$ and $s = s_1 + 1$. We conclude that there are 4 solutions (u, s, t) to the equations (2.5.25), (2.5.26) and (2.5.27).

Since u takes 3 values and s, t are free in F_{2^m}, there are $3q^2$ admissible change of variables. Therefore, the number of elliptic curves isomorphic to E_1 is $3q^2/4$. Since a_6 takes q values and a_4 takes $3q/4$ values due to the fact that $Te(a_4) \neq 0$, there are $3q^2/4$ Type II elliptic curves over F_{2^m} when m is even. Therefore, we can conclude that the Type II curves form an isomorphism class of elliptic curves.

Type III Curves

Let E_1 be the Type III curve given by

$$E_1 \ : \ y^2 + y = x^3,$$

and let $\bar{E}$ be any elliptic curve given by

$$\bar{E} \ : \ y^2 + y = x^3 + \bar{a}_4 x + \bar{a}_6,$$

which is isomorphic to E_1. Then, by using Theorem (1.2.2), there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$, satisfying the equations

$$u^3 = 1 \tag{2.5.28}$$

$$s^4 + s + u\bar{a}_4 = 0 \tag{2.5.29}$$

$$t^2 + t + s^6 + \bar{a}_6 = 0 \tag{2.5.30}$$

Note that

$$Te(\bar{a}_4) = Te\Big(\frac{s^4 + s}{u}\Big) = Te\Big(\frac{s^4}{u^4}\Big) + Te\Big(\frac{s}{u}\Big) = 0,$$

and hence $\bar{E}$ is also a Type III curve. Now, we proceed to count the number of admissible change of variables which transform $\bar{E}$ to E_1. We achieve this by counting the total number of solutions (u, s, t) to the equation (2.5.28), (2.5.29)

and (2.5.30). This leads us to the number of the elliptic curves $\bar{E}$ isomorphic to E_1.

Since $u^3 = 1$, we have $u = 1, c_1$ *or* c_2. Since $Te(\bar{a}_4) = 0$, we have $Te(c_1\bar{a}_4) = 0$ and $Te(c_2\bar{a}_4) = 0$. Therefore, for each choice of u, equation (2.5.29) has exactly 4 distinct solutions in F_{2^m}. We find that these 12 solutions (u, s) to (2.5.29) are as follows:

$$\left.\begin{array}{cccc} (1,\ s_1) & (1,\ s_1+1) & (1,\ s_1+c_1) & (1,\ s_1+c_2) \\ (c_1,\ c_1s_1) & (c_1,\ c_1s_1+1) & (c_1,\ c_1s_1+c_1) & (c_1,\ c_1s_1+c_2) \\ (c_2,\ c_2s_1) & (c_2,\ c_2s_1+1) & (c_2,\ c_2s_1+c_1) & (c_2,\ c_2s_1+c_2) \end{array}\right\} \qquad (2.5.31)$$

Since (s_1, t_1) is a solution to (2.5.30), we have that $Tr(s_1^6 + \bar{a}_6) = 0$. Using this fact, we can easily check that $Tr(s^6 + \bar{a}_6) = 0$ for each of the 12 choices for s in (2.5.31). So, for each choices of s in (2.5.31), equation (2.5.30) have 2 solutions. Therefore, there are 24 solutions (u, s, t) to the equations (2.5.28), (2.5.29) and (2.5.30).

Since there are $3q^2$ admissible change of variables, as mentioned before the number of elliptic curves isomorphic to E_1 is $3q^2/24 = q^2/8$. Since a_6 takes q values and a_4 takes $q/4$ values due to the fact that $Te(a_4) = 0$, there are $q^2/4$ Type III elliptic curves over F_{2^m} when m is even. So, the number of elliptic curves isomorphic to E_1 is $1/2$ of Type III elliptic curves over F_{2^m} when m is even.

Let E_2 be the Type III curve given by the equation

$$E_2 \ : \ y^2 + y = x^3 + a_6, \quad Tr(a_6) = 1,\ a_6 \in F_{2^m}$$

Note that, $E_1 \ncong E_2$, because the equations

$$\begin{aligned} u^3 &= 1 \\ s^4 + s &= 0 \\ t^2 + t + s^6 + a_6 &= 0 \end{aligned}$$

have no solution (u, s, t) in F_{2^m}. In fact, the equation $s^4 + s = 0$ has always

4 solutions $s = 0$, $s = 1$, $s = c_1$ and $s = c_2$ over F_{2^m}. This implies the latter equation has no solution, because $Tr(s^6 + a_6) = 1$ for each choice of s.

Now, we are going to count the elliptic curves

$$\bar{E} \ : \ y^2 + y = x^3 + \bar{a}_4 x + \bar{a}_6,$$

which is isomorphic to E_2. Then, there exists $u = u_1, s = s_1, t = t_1 \in F_{2^m}$, satisfying the equations

$$u^3 = 1 \tag{2.5.32}$$

$$s^4 + s + u\bar{a}_4 = 0 \tag{2.5.33}$$

$$t^2 + t + s^6 + \bar{a}_6 + a_6 = 0 \tag{2.5.34}$$

Note that

$$Te(\bar{a}_4) = Te\Big(\frac{s^4 + s}{u}\Big) = Te\Big(\frac{s^4}{u^4}\Big) + Te\Big(\frac{s}{u}\Big) = 0,$$

and hence $\bar{E}$ is also a Type III curve. Now, we proceed to count the number of admissible change of variables which transform $\bar{E}$ to E_2. We achieve this by counting the total number of solutions (u, s, t) to the equation (2.4.32), (2.4.33) and (2.4.34). This leads us to the number of the elliptic curves $\bar{E}$ isomorphic to E_2.

Since $u^3 = 1$, we have $u = 1, c_1$ *or* c_2. Since $Te(\bar{a}_4) = 0$, we have $Te(c_1\bar{a}_4) = 0$ and $Te(c_2\bar{a}_4) = 0$. Therefore, for each choice of u, equation (2.5.33) has exactly 4 distinct solutions in F_{2^m}. We find that these 12 solutions (u, s) to (2.5.33) are as follows:

$$\left.\begin{array}{cccc} (1,\ s_1) & (1,\ s_1+1) & (1,\ s_1+c_1) & (1,\ s_1+c_2) \\ (c_1,\ c_1s_1) & (c_1,\ c_1s_1+1) & (c_1,\ c_1s_1+c_1) & (c_1,\ c_1s_1+c_2) \\ (c_2,\ c_2s_1) & (c_2,\ c_2s_1+1) & (c_2,\ c_2s_1+c_1) & (c_2,\ c_2s_1+c_2) \end{array}\right\} \tag{2.5.35}$$

Since (s_1, t_1) is a solution to (2.5.34), we have that $Tr(s_1^6 + \bar{a}_6) = 0$. Using this fact, we can easily check that $Tr(s^6 + \bar{a}_6) = 0$ for each of the 12 choices for s in (2.5.35). So, for each choices of s in (2.5.35), the equation (2.5.34) have 2 solutions. Therefore, there are 24 solutions (u, s, t) to the equations (2.5.32), (2.5.33) and (2.5.34).

Since there are $3q^2$ admissible change of variables, as mentioned before the number of elliptic curves isomorphic to E_2 is $3q^2/24 = q^2/8$. Since a_6 takes q values and a_4 takes $q/4$ values due to the fact that $Te(a_4) = 0$, there are $q^2/4$ Type III elliptic curves over F_{2^m} when m is even. So, we can deduce that the remaining $q^2/8$ Type III curves which is not isomorphic to E_1 must lie in an isomorphism class, that is represented by E_2.

Now, we will show that these 3 types of curves are not isomorphic to each other. Let E_1 be a Type I curve given by

$$E_1 \ : \ y^2 + a_3 y = x^3 + a_4 x + a_6 \quad a_3 \neq 0 \textit{ and not a cube}$$

and let E_2 be a Type II curve given by

$$E_2 \ : \ y^2 + y = x^3 + a_4^{'} x + a_6^{'} \quad a_3^{'} \neq 0 \textit{ and a cube}, \ Te(a_4^{'}) = 1$$

Since a_3 is not a cube, the equation

$$u^3 \ = \ a_3$$

has no solution. So, $E_1 \ncong E_2$. Let E_3 be a Type III curve given by

$$E_3 \ : \ y^2 + y = x^3 + \bar{a}_4 x + \bar{a}_6 \quad a_3 \neq 0 \textit{ and a cube}, \ Te(\bar{a}_4) = 0$$

By using the same reason above, $E_1 \ncong E_3$. On the other hand, $E_2 \ncong E_3$ because

the equations

$$\begin{aligned} u^3 &= 1 \\ s^4 + s + u\bar{a}_4 + a_4^{'} &= 0 \\ t^2 + t + s^6 + a_4^{'}s^2 + a_6^{'} + \bar{a}_6 &= 0 \end{aligned}$$

have no common solution. In fact, $Te(u\bar{a}_4 + a_4^{'}) \neq 0$ for each choice of u in the second equation above. Therefore, there is no s satisfying the above equations.

In conclusion, these 3 types of curves are not isomorphic to each other. We summarize these results in the next theorem.

Theorem 2.5.1. *There are 7 isomorphism classes of elliptic curves over F_{2^m} with j-invariant equal to 0, where m is even. Let γ be a non-cube in F_{2^m}. Let $\alpha, \beta, \delta, \omega \in F_{2^m}$ be such that $Tr(\gamma^{-2}\alpha) = 1$, $Tr(\gamma^{-4}\beta) = 1$, $Te(\delta) \neq 0$ and $Tr(\omega) = 1$. Then, a representative from each class is:*
(i) $y^2 + \gamma y = x^3$ *(Type I)*
(ii) $y^2 + \gamma y = x^3 + \alpha$ *(Type I)*
(iii) $y^2 + \gamma^2 y = x^3$ *(Type I)*
(iv) $y^2 + \gamma^2 y = x^3 + \beta$ *(Type I)*
(v) $y^2 + y = x^3 + \delta x$ *(Type II)*
(vi) $y^2 + y = x^3$ *(Type III)*
(vii) $y^2 + y = x^3 + \omega$ *(Type III).*

Example: We list a representative of each of the 13 isomorphism classes of elliptic curves over F_4, together with the j-invariant, size and group structure of each curve. Here, we denote the elements of F_4 by $0,\ 1,\ c_1,\ c_2$ as before.

Let us consider the first curve E given by the equation

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

over F_4. Here, $a_1 = a_6 = 1$ and $a_2 = a_3 = a_4 = 0$. We know by Section 2.2 that $j(E) = (a_1)^{12}/\Delta$ and if $a_1 \neq 0$, then $\Delta = a_6$ and $j(E) = 1/a_6$. Therefore, for the given curve E, we find that $\Delta = 1$ and so $j(E) = 1$. The total number of 8

points satisfying the given curve E are as follows:

$$(0,\ 1)\ ,\ (1,\ 0)\ ,\ (1,\ 1)\ ,\ (c_1,\ 0)$$
$$(c_2,\ 0)\ ,\ (c_1,\ c_1)\ ,\ (c_2,\ c_2)\ ,\ O$$

It follows from Section 1.5 that $E(F_4) \cong C_8$, where C_8 denotes the cyclic group on 8 elements.

Using similar computations, one compute the *j-invariant*, size and the group structure of the 13 isomorphism classes of elliptic curves over F_4. We give this list in the table below:

Table 2.1: Representatives of the isomorphism classes of elliptic curves over F_4

Representative Curve	$j-invariant$	Number of Points	Group Type
$y^2+xy=x^3+1$	1	8	C_8
$y^2+xy=x^3+c_1x^2+1$	1	2	C_2
$y^2+xy=x^3+c_1$	c_2	4	C_4
$y^2+xy=x^3+c_1x^2+c_1$	c_2	6	C_6
$y^2+xy=x^3+c_2$	c_1	4	C_4
$y^2+xy=x^3+c_1x^2+c_2$	c_1	6	C_6
$y^2+c_1y=x^3$(Type I)	0	3	C_3
$y^2+c_1y=x^3+1$(Type I)	0	7	C_7
$y^2+c_2y=x^3$(Type I)	0	3	C_3
$y^2+c_2y=x^3+1$(Type I)	0	7	C_7
$y^2+y=x^3+x$(Type II)	0	5	C_5
$y^2+y=x^3$(Type III)	0	9	$C_3 \times C_3$
$y^2+y=x^3+c_1$(Type III)	0	1	C_1

2.6 Number of Points

In this section, we determine the order of the elliptic curves over F_{2^m} having *j-invariant* zero. First, we will give some theorems which are very useful determining the orders. For proofs of these theorems and the group type of these curves, we refer reader to [5].

Theorem 2.6.1. *Let E be defined over F_q. Then, E is supersingular if and only if $t^2 = 0,\ q,\ 2q,\ 3q$ or $4q$.*

Theorem 2.6.2. *Let $q = 2^m$, and let E be an elliptic curve over F_q with $\#E(F_q) = q + 1 - t$.*
(i) If $t^2 = 0,\ q$ or $2q$, then $E(F_q)$ is cyclic.
(ii) If $t = 2\sqrt{q}$ or $-2\sqrt{q}$, then $E(F_q) \cong C_{\sqrt{q}-1} \times C_{\sqrt{q}-1}$ or $E(F_q) \cong C_{\sqrt{q}+1} \times C_{\sqrt{q}+1}$, respectively.

Now, we will obtain the general form of the order of the elliptic curves over F_{2^m} with $j(E) = 0$.

(i) m odd

In section 2.4, we have obtained 3 isomorphism classes of elliptic curves over F_{2^m} when m is odd. Now, we will find the order of these curves using the Theorem 1.5.2 (Weil Conjecture). First, let us consider the curve

$$y^2 + y = x^3 \tag{2.6.36}$$

It is clear that the number of points satisfying the equation (2.6.36) over F_2 is 3. In fact, $\#E(F_2) = N_1 = 3$. So, we get $t = 0$, where $t = q + 1 - N_1$ and $q = 2$. When we solve the equation

$$1 + 2T^2 = (1 - \alpha T)(1 - \beta T)$$

we get $\alpha = i\sqrt{2}$ and $\beta = -i\sqrt{2}$. Since m is odd, we get

$$\#E(F_{2^m}) \ = \ 2^m + 1 - (i\sqrt{2})^m - (-i\sqrt{2})^m \ = \ 2^m + 1 \ = \ q + 1$$

Now, we will consider the curve

$$y^2 + y = x^3 + x \tag{2.6.37}$$

It is easy to see that the 5 points $(0,0),(0,1),(1,0),(1,1)$ and O satisfy the equation (2.6.37) over F_2. In fact, $\#E(F_2) = 5$. So, we get $t = q + 1 - N_1 = 2 + 1 - 5 = -2$. When we solve the equation

$$1 + 2T + 2T^2 = (1 - \alpha T)(1 - \beta T),$$

we get $\alpha = -1 + i$ and $\beta = -1 - i = i\alpha$. Therefore,

$$\begin{aligned} \#E(F_{2^m}) &= 2^m + 1 - (-1+i)^m - (-1-i)^m \\ &= 2^m + 1 - \left[(-1+i)^m(1+i^m)\right] \\ &= 2^m + 1 - \left[\alpha^m(1+i^m)\right] \end{aligned}$$

Since

$$i^m = \begin{cases} 1, & \text{if } m = 4l \\ i, & \text{if } m = 4l+1 \\ -1, & \text{if } m = 4l+2 \\ -i, & \text{if } m = 4l+3 \end{cases}$$

we get

$$1 + i^m = \begin{cases} 2, & \text{if } m = 4l \\ 1+i, & \text{if } m = 4l+1 \\ 0, & \text{if } m = 4l+2 \\ 1-i, & \text{if } m = 4l+3 \end{cases}$$

Now, we will take some power of α to reach the α^m:

$$\begin{aligned}
\alpha &= (-1+i) \\
\alpha^2 &= (-1+i)^2 = -2i \\
\alpha^3 &= (-1+i)^3 = 2(1+i) = -2\bar{\alpha} \\
\alpha^4 &= (-1+i)^4 = -4 \\
\alpha^5 &= (-1+i)^5 = 4(1-i) = -4\alpha \\
\alpha^6 &= (-1+i)^6 = 8i \\
\alpha^7 &= (-1+i)^7 = -8(1+i) = 8\bar{\alpha} \\
\alpha^8 &= (-1+i)^8 = 16.
\end{aligned}$$

So, we get

$$(-1+i)^m(1+i^m) = \alpha^m(1+i^m) = \begin{cases} 2(i-1)^m, & \text{if } m = 4l \\ -2(i-1)^{m-1}, & \text{if } m = 4l+1 \\ 0, & \text{if } m = 4l+2 \\ -(i-1)^{m+1}, & \text{if } m = 4l+3 \end{cases}$$

For $m = 4l+1$, m odd

$$\#E(F_{2^m}) = 2^m + 1 + 2(i-1)^{m-1}$$

$$2(i-1)^{m-1} = \begin{cases} 2^{\frac{m+1}{2}}, & \text{if } m = 1 \pmod 8 \\ -2^{\frac{m+1}{2}}, & \text{if } m = 5 \pmod 8 \end{cases}$$

$$= \begin{cases} \sqrt{2q}, & \text{if } m = 1 \pmod 8 \\ -\sqrt{2q}, & \text{if } m = 5 \pmod 8 \end{cases}$$

For $m = 4l+3$, m odd

$$\#E(F_{2^m}) = 2^m + 1 + (i-1)^{m+1}$$

$$(i-1)^{m+1} = \begin{cases} -2^{\frac{m+1}{2}}, & \text{if } m = 3 \pmod 8 \\ 2^{\frac{m+1}{2}}, & \text{if } m = 7 \pmod 8 \end{cases}$$

$$= \begin{cases} -\sqrt{2q}, & \text{if } m = 3 \pmod 8 \\ \sqrt{2q}, & \text{if } m = 7 \pmod 8 \end{cases}$$

Using the procedure as above, we can easily determine the order of the curve

$$y^2 + y = x^3 + x + 1 \tag{2.6.38}$$

as well. We list these results in the table below:

Table 2.2: Orders of elliptic curves over F_{2^m} with *j-invariant* equal to 0, where m is odd

Curve	m	Order	Group Type
$y^2 + y = x^3$	odd	$q+1$	cyclic
$y^2 + y = x^3 + x$	$m \equiv 1, 7 \pmod 8$	$q + 1 + \sqrt{2q}$	cyclic
	$m \equiv 3, 5 \pmod 8$	$q + 1 - \sqrt{2q}$	cyclic
$y^2 + y = x^3 + x + 1$	$m \equiv 1, 7 \pmod 8$	$q + 1 - \sqrt{2q}$	cyclic
	$m \equiv 3, 5 \pmod 8$	$q + 1 + \sqrt{2q}$	cyclic

(ii) m **even**

Let $\#E_i = q + 1 - t_i$ for $1 \leq i \leq 7$, where $q = 2^m$, and the curves E_i are those of Theorem 2.5.1. By Theorem 2.6.1, we obtain that the 7 values of t_i are $0,\ 2\sqrt{q},\ -2\sqrt{q},\ \sqrt{q},\ \sqrt{q},\ -\sqrt{q},\ -\sqrt{q}$.

We first observe that $\#E_1 + \#E_2 = 2q + 2$, and so $t_1 = -t_2$. This holds because for each $x \in F_q$, either $Tr(\gamma^{-2}x^3) = 0$ or $Tr(\gamma^{-2}x^3 + \gamma^{-2}\alpha) = 0$, but not both. We note that, the curves E_1, E_2 are an example of a twisted pair of elliptic curves. E_3, E_4 and E_6, E_7 are also twisted pairs, and so $t_3 = -t_4$ and $t_6 = -t_7$. It follows then that $t_5 = 0$.

Since the coefficients of E_6 are in F_2, we can apply the Theorem 1.5.2 (Weil Conjecture) to determine $\#E_6$, and so $\#E_7$. We find that $t_6 = 2\sqrt{q}$ or $-2\sqrt{q}$

according to whether $m \equiv 0$ *or* $2 \pmod 4$, respectively.

Now, we know that $t_1, t_3 = \sqrt{q}$ *or* $-\sqrt{q}$. We determine their exact values as follows. Let $\gamma = g^{-1}$, where g is a generator of F_{2^m}. Then,

$$\begin{aligned} A = \{x^3 \ : \ x \in F_{2^m}\} &= \{g^{3i} \ : \ 0 \leq i \leq (2^m - 1)/3\}, \\ B = \{\gamma^{-2}x^3 \ : \ x \in F_{2^m}\} &= \{g^{3i+2} \ : \ 0 \leq i \leq (2^m - 1)/3\}, \\ C = \{\gamma^{-4}x^3 \ : \ x \in F_{2^m}\} &= \{g^{3i+1} \ : \ 0 \leq i \leq (2^m - 1)/3\}. \end{aligned}$$

Since $(A,\ B,\ C)$ is a partition of F_{2^m}, and since the half of the elements of F_{2^m} have trace equal to 0, we deduce that

$$\#E_1 + \#E_3 + \#E_6 = 3q + 3,$$

and so $t_1 + t_3 = -t_6$. Thus, we must have $t_1 = t_3 = -\sqrt{q}$ if $m \equiv 0 \pmod 4$, and $t_1 = t_3 = \sqrt{q}$ if $m \equiv 2 \pmod 4$. The orders of the curves E_i, $1 \leq i \leq 7$, are given below:

Table 2.3: Orders of elliptic curves over F_{2^m} with *j-invariant* equal to 0, where m is even

Curve	m	Order	Group Type
$y^2 + \gamma y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 + \sqrt{q}$	cyclic
	$m \equiv 2 \pmod 4$	$q + 1 - \sqrt{q}$	cyclic
$y^2 + \gamma y = x^3 + \alpha$	$m \equiv 0 \pmod 4$	$q + 1 - \sqrt{q}$	cyclic
	$m \equiv 2 \pmod 4$	$q + 1 + \sqrt{q}$	cyclic
$y^2 + \gamma^2 y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 + \sqrt{q}$	cyclic
	$m \equiv 2 \pmod 4$	$q + 1 - \sqrt{q}$	cyclic
$y^2 + \gamma^2 y = x^3 + \beta$	$m \equiv 0 \pmod 4$	$q + 1 - \sqrt{q}$	cyclic
	$m \equiv 2 \pmod 4$	$q + 1 + \sqrt{q}$	cyclic
$y^2 + y = x^3 + \delta x$	m even	$q + 1$	cyclic
$y^2 + y = x^3$	$m \equiv 0 \pmod 4$	$q + 1 - \sqrt{2q}$	$C_{\sqrt{q}-1} \times C_{\sqrt{q}-1}$
	$m \equiv 2 \pmod 4$	$q + 1 + \sqrt{2q}$	$C_{\sqrt{q}+1} \times C_{\sqrt{q}+1}$
$y^2 + y = x^3 + \omega$	$m \equiv 0 \pmod 4$	$q + 1 + \sqrt{2q}$	$C_{\sqrt{q}+1} \times C_{\sqrt{q}+1}$
	$m \equiv 2 \pmod 4$	$q + 1 - \sqrt{2q}$	$C_{\sqrt{q}-1} \times C_{\sqrt{q}-1}$

Chapter 3

Elliptic Curves over Finite Fields of Characteristic Two Used In Ecdsa and Their Properties

3.1 Introduction

By ECDSA, we mean the Elliptic Curve Digital Signature Algorithm. The Elliptic Curve Digital Signature Algorithm is the elliptic curve anologue of the Digital Signature Algorithm (DSA). ECDSA was first proposed in 1992 by Scott Vanstone [14] in response to National Institute of Standards and Technology's (NIST) request for public comments on their first proposal for Digital Signature Scheme. It was accepted later by International Standards Organization (ISO 14888-3), American National Standards Institute (ANSI X9.62), Institute of Electrical and Electronics Engineering (IEEE P1363) and Federal Information Processing Standard (FIPS 186-2).

In this chapter, we shall discuss ECDSA over a field F_q, and present the ECDSA signature and verification algorithms. Finally, we will give the list of those isomorphism classes of elliptic curves over F_{2^m} recommended by NIST and recall their properties discussed in Chapter 2. ([15], [16])

3.2 Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve defined over F_q, $P \in E(F_q)$ be a point of order N and Q be any point in the subgroup $\langle P \rangle$ of $E(F_q)$ generated by P. Finding x, $0 \leq x \leq N-1$, such that $Q = xP$ is called The Elliptic Curve Discrete Logarithm Problem (ECDLP).

The ECDSA basically rely on the difficulty of solving the ECDLP. If anyone is able to solve the ECDLP, then it is easy to break the ECDSA. Therefore, it is of great importance to understand the methods of dealing with the ECDLP. There are some known attacks on ECDLP such as Baby Step-Giant Step, Silver-Pohlig-Hellman, Pollard's Algorithm, MOV, Frey-Rück, etc. These algorithms are general exponential time algorithms. We will see later that choosing an appropriate elliptic curve, we should be care of these attacks. The ECDLP has an application generating digital signatures as we shall discuss, now.

E is an elliptic curve defined over F_q and P is a point of prime order N in $E(F_q)$ which are public parameters. Throughout this chapter, we shall use Ayşe and Bilal instead of the users. Ayşe constructs her keys by selecting a random integer x in the interval $[1, N-1]$ and computing $Q = xP$. She obtain that her public key is Q and her private key is x.

3.3 ECDSA Signature Generation

To sign a message m having hash value H, i.e. SHA-1(m)=H, $0 < H < N$, Ayşe does the following:

1. She selects a random integer k in the inteval $[1, N-1]$.

2. She computes $kP = (x_1, y_1)$ and sets r equal to the least nonnegative residue of $x_1 \pmod{N}$, where x_1 is regarded as an integer between 0 and $q-1$. If $r = 0$, then she must go back to step 1 and select another k.

3. She computes $k^{-1} \pmod{N}$ and sets s equal to the least nonnegative residue

of $k^{-1}(H + xr) \pmod N$. If $s = 0$, then she must go back to step 1.

4. The signature for the message m is the pair of integers (r, s).

Recall that The Secure Hash Algorithm (SHA-1) was proposed by the NIST for certain U.S. Federal Government applications. The SHA-1 produces 160-bit output called a message digest when a message has input with length $< 2^{64}$ bits. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest.

3.4 ECDSA Signature Verification

In order to verify Ayşe's signature (r, s) on the message m, Bilal should do the following:

1. He obtains an authenticated copy of Ayşe's public key Q.
2. He verify that r and s are integers in the interval $[1, N - 1]$ and computes the hash value of the message.
3. He computes $u_1 = s^{-1}H \pmod N$ and $u_2 = s^{-1}r \pmod N$.
4. He computes $u_1P + u_2Q = (x_0, y_0)$ and regarding x_0 as an integer between 0 and $q-1$, he sets v equal to the least nonnegative residue of $x_0 \pmod N$.
5. Accept the signature if and ony if $v = r$.

Notice that if Ayşe generated her signature correctly, then $u_1P + u_2Q = (u_1 + xu_2)P = kP$ because $k \equiv s^{-1}(H + xr) \pmod N$, and so $v = r$ as required.

In order to obtain a security level, the parameter N should have about 160 bits. The advantages of ECDSA are well-known. For example, it gives us a chance giving an elliptic curve to each user by choosing the parameters over the same field. At the same time, there are an enormous number of choices of elliptic curves E over the fixed F_q.

3.5 Selecting An Appropriate Elliptic Curve over F_{2^m}

By an "appropriate" elliptic curve, we mean an elliptic curve E defined over a finite field F_{2^m} where the ECDLP in $E(F_{2^m})$ resists all known attacks. In particular the following conditions should be satisfied:

1. To resist the Pollard-ρ attack $\#E(F_{2^m})$ should be divisible by a sufficiently large prime N (for example, $N > 2^{160}$).

2. To resist the Weil and Tate pairing attacks, N should not divide $q^k - 1$ for all $1 \leq k \leq C$, where C is large enough so that it is computationally infeasible to find discrete logarithms in $F^*_{q^C}$ ($C = 20$ suffices in practice). For example, the elliptic curves of $j(E) = 0$ should be avoided.

3. To resist the GHS (Gaudry, Hess, Smart) attack, the degree of the reduction polynomial should be choosen prime, constructing the underlying field.

3.6 NIST Recommended Curves over F_{2^m}

In this section, we will discuss the 10 elliptic curves over F_{2^m} that were recommended by NIST in June 1999 for U.S. Federal Government use. These elliptic curves are also recommended in the FIPS 186-2 standard. There are two types of recommended elliptic curves over F_{2^m}. These are Koblitz Elliptic Curves and Randomly Choosing Elliptic Curves [16]. Their equations are in the form

$$y^2 + xy = x^3 + a_2x^2 + a_6,$$

where $a_6 \neq 0, a_2 \in F_{2^m}$ and the explicit expression is given in Section 2.2, where this class belongs to the non-supersingular class. Now, we shall give Koblitz Elliptic Curves and Randomly Choosing Elliptic Curves, respectively. In the following, we are going to represent the elements of F_{2^m} in the hexadecimal form

to distinguish them from the integers in the decimal form where they are used to represent the order of an element in the groups. The hexadecimal form is also useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier to read hexadecimal numbers than binary numbers. For example, '0111 1011 1010' is the binary representation of the number 1978 and hexadecimal representation of the integer 1978 is '0× 7ba', where '0×' is attaching to the beginning of the number to indicate hexadecimal form.

3.6.1 Koblitz Elliptic Curves

The general form of Koblitz Curve is in the form

$$y^2 + xy = x^3 + a_2x^2 + 1,$$

where $a_2 \in F_{2^m}$. x_P and y_P are the coordinates of the base point P of order N and these coordinates are represented as the hexadecimal base: {0, 1,. . . , 9,a,b,. . . , f}

Curve K-163

We first fix the underlying field $F_{2^{163}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$. For this class, the elliptic curve is choosen by taking $a_2 = 1$. Namely, the elliptic curve is given by the form $y^2 + xy = x^3 + x^2 + 1$. Now, we choose the base point $P = (x_P, y_P)$ as follows:

$$x_P = 0\times\ 2\ \text{fe13c053}\ \text{7bbc11ac}\ \text{aa07d793}\ \text{de4e6d5e}\ \text{5c94eee8}$$

and

$$y_P = 0\times\ 2\ \text{89070fb0}\ \text{5d38ff58}\ \text{321f2e80}\ \text{0536d538}\ \text{ccdaa3d9}$$

The order of P turns out to be the prime N is given by

$$\text{N} = 5846006549323611672814741753598448348329118574063,$$

which is a 163-bit prime integer.

Curve K-233

We first fix the underlying field $F_{2^{233}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{233} + x^{74} + 1$. For this class, the elliptic curve is choosen by taking $a_2 = 0$. Namely, the elliptic curve is given by the form $y^2 + xy = x^3 + 1$. Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P =$ 0× 172 32ba853a 7e731af1 29f22ff4 149563a4 19c26bf5 0a4c9d6e efad6126

and

$y_P =$ 0× 1db 537dece8 19b7f70f 555a67c4 27a8cd9b f18aeb9b 56e0c110 56fae6a3

The order of P turns out to be the prime N is given by

N = 3450873173395281893717377931138512760570940988862252126328087024741343,

which is a 232-bit prime integer.

Curve K-283

We first fix the underlying field $F_{2^{283}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$. For this class, the elliptic curve is choosen by taking $a_2 = 0$. Namely, the elliptic curve is given by the form $y^2 + xy = x^3 + 1$. Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P =$ 0× 503213f 78ca4488 3f1a3b81 62f188e5 53cd265f 23c1567a 16876913 b0c2ac24 58492836

and

$y_P =$ 0× 1ccda38 0f1c9e31 8d90f95d 07e5426f e87e45c0 e8184698 e4596236 4e341161 77dd2259

The order of P turns out to be the prime N is given by

N = 3885337784451458141838923813647037813284811733793061324295874997529815829704422603873,

which is a 282-bit prime integer.

Curve K-409

We first fix the underlying field $F_{2^{409}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{409} + x^{87} + 1$. For this class, the elliptic curve is choosen by taking $a_2 = 0$. Namely, the elliptic curve is given by the form $y^2 + xy = x^3 + 1$. Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 060f05f 658f49c1 ab3ab189 0f718421 0efd0987 e307c84c 27accfb8 f9f67cc2 c460189e b5aaaa62 ee222eb1 b35540cf e9023746

and

$y_P = 0\times$ 1e36905 0b7c4e42 acba1dac bf04299c 3460782f 918ea247 e6325165 e9ea10e3 da5f6c42 e9c55215 aa9ca27a 5863ec48 d8e0286b

The order of P turns out to be the prime N is given by

N = 330527984395124299475957654016385519914202341482140609642324395022880711289249191050673258457777458014096366590617731358671,

which is a 408-bit prime integer.

Curve K-571

We first fix the underlying field $F_{2^{571}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$. For this class, the elliptic curve is choosen by taking $a_2 = 0$. Namely, the elliptic curve is given by the form $y^2 + xy = x^3 + 1$. Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 26eb7a8 59923fbc 82189631 f8103fe4 ac9ca297 0012d5d4 60248048 01841ca4 43709584 93b205e6 47da304d b4ceb08c bbd1ba39 494776fb 988b4717 4dca88c7 e2945283 a01c8972

and

$y_P = 0\times$ 349dc80 7f4fbf37 4f4aeade 3bca9531 4dd58cec 9f307a54 ffc61efc 006d8a2c 9d4979c0 ac44aea7 4fbebbb9 f772aedc b620b01a 7ba7af1b 320430c8 591984f6 01cd4c14 3ef1c7a3

The order of P turns out to be the prime N is given by

N = 193226876150862917234767594546599367214946366485321749932861762
57257595711447802122681339785227067118347067128008253514612736 7
4974066617311929682421617092503555733685276673,

which is a 570-bit prime integer.

3.6.2 Random Elliptic Curves

The general form of Random Elliptic Curve is in the form

$$y^2 + xy = x^3 + x^2 + a_6,$$

where $a_6 \in F_{2^m}$. x_P and y_P are the coordinates of the base point P of order N and these coordinates are represented as the hexadecimal base: {0, 1,. . . , 9,a,b,. . . , f}

Curve B-163

We first fix the underlying field $F_{2^{163}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$. For this class, the elliptic curve is choosen by taking

$$a_6 = 0 \times \ 2 \ \ 0a601907 \ \ b8c953ca \ \ 1481eb10 \ \ 512f7874 \ \ 4a3205fd$$

Now, we choose the base point $P = (x_P, y_P)$ as follows:

$$x_P = 0 \times \ 3 \ \ f0eba162 \ \ 86a2d57e \ \ a0991168 \ \ d4994637 \ \ e8343e36$$

and

$$y_P = 0 \times \ 0 \ \ d51fbc6c \ \ 71a0094f \ \ a2cdd545 \ \ b11c5c0c \ \ 797324f1$$

The order of P turns out to be the prime N is given by

$$\mathrm{N} = 5846006549323611672814742442876390689256843201587,$$

which is a 163-bit prime integer.

Curve B-233

We first fix the underlying field $F_{2^{233}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{233} + x^{74} + 1$. For this class, the elliptic curve is choosen by taking

$a_6 = 0\times$ 066 647ede6c 332c7f8c 0923bb58 213b333b 20e9ce42
81fe115f 7d8f90ad

Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 0fa c9dfcbac 8313bb21 39f1bb75 5fef65bc 391f8b36
f8f8eb73 71fd558b

and

$y_P = 0\times$ 100 6a08a419 03350678 e58528be bf8a0bef f867a7ca
36716f7e 01f81052

The order of P turns out to be the prime N is given by

N = 6901746346790563787434755862277025555839812737345013555379383634485463,

which is a 233-bit prime integer.

Curve B-283

We first fix the underlying field $F_{2^{283}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$. For this class, the elliptic curve is choosen by taking

$a_6 = 0\times$ 27b680a c8b8596d a5a4af8a 19a0303f ca97fd76 45309fa2
a581485a f6263e31 3b79a2f5 7d8f90ad

Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 5f93925 8db7dd90 e1934f8c 70b0dfec 2eed25b8 557eac9c
80e2e198 f8cdbecd 86b12053

and

$y_P = 0\times$ 3676854 fe24141c b98fe6d4 b20d02b4 516ff702 350eddb0
826779c8 13f0df45 be8112f4

The order of P turns out to be the prime N is given by

N = 7770675568902916283677847627294075626569625924376904889
109196526770044277787378692871,

which is a 283-bit prime integer.

Curve B-409

We first fix the underlying field $F_{2^{409}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{409} + x^{87} + 1$. For this class, the elliptic curve is choosen by taking

$a_6 = 0\times$ 021a5c2 c8ee9feb 5c4b9a75 3b7b476b 7fd6422e f1f3dd67 4761fa99
d6ac27c8 a9a197b2 72822f6c d57a55aa 4f50ae31 7b13545f 7d8f90ad

Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 15d4860 d088ddb3 496b0c60 64756260 441cde4a f1771d4d
b01ffe5b 34e59703 dc255a86 8a118051 5603aeab 60794e54 bb7996a7

and

$y_P = 0\times$ 061b1cf ab6be5f3 2bbfa783 24ed106a 7636b9c5 a7bd198d
0158aa4f 5488d08f 38514f1f df4b4f40 d2181b36 81c364ba 0273c706

The order of P turns out to be the prime N is given by

N = 661055968790248598951915308032771039828404682964281219284648798
30415777482737480520814372376217911096597986728836656752677 1,

which is a 409-bit prime integer.

Curve B-571

We first fix the underlying field $F_{2^{571}} = F_2[x]/\langle f(x)\rangle$ by choosing the reduction polynomial $f(x) = x^{571} + x^{10} + x^5 + x^2 + 1$. For this class, the elliptic curve is choosen by taking

$a_6 = 0 \times$ 2f40e7e 2221f295 de297117 b7f3d62f 5c6a97ff cb8ceff1 cd6ba8ce
4a9a18ad 84ffabbd 8efa5933 2be7ad67 56a66e29 4afd185a 78ff12aa
520e4de7 39baca0c 7ffeff7f 2955727a

Now, we choose the base point $P = (x_P, y_P)$ as follows:

$x_P = 0\times$ 303001d 34b85629 6c16c0d4 0d3cd775 0a93d1d2 955fa80a a5f40fc8
db7b2abd bde53950 f4c0d293 cdb711a3 5b67fb14 99ae6003 8614f139
4abfa3b4 c850d927 e1e7769c 8eec2d19

and

$y_P = 0\times$ 37bf273 42da639b 6dccfffe b73d69d7 8c6c27a6 009cbbca 1980f853
3921e8a6 84423e43 bab08a57 6291af8f 461bb2a8 b3531d2f 0485c19b
16e2f151 6e23dd3c 1a4827af 1b8ac15b

The order of P turns out to be the prime N is given by

N = 3864537523017258344695351890931987344298927329706434998657235251451519142289560424536143999389415773083133881121926944486246872462816813070234528288303332411393191105285703,

which is a 571-bit prime integer.

Chapter 4

Conclusions

In this thesis, we studied the isomorphism classes of elliptic curves over finite fields of characteristic 2. We listed those elliptic curves which are recommended by National Institute of Standards and Technology and gave all the details to be used in Elliptic Curve Digital Signature Algorithm. The implementation part of this work has not been done in this thesis, and we hope to do this as a future project.

References

[1] T. ElGamal, *A public key cryptosystems and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, **31**, 469-472 (1985)

[2] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computations, **48**, 203-209 (1987)

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, (1984)

[4] R. Schoof, *Elliptic Curves over Finite Fields and The Computation of Square Roots* mod p, Mathematics of Computation, **44**, 483-494 (1985)

[5] R. Schoof, *Nonsingular Plane Cubic Curves over Finite Fields*, Journal of Combinatorial Theory, **A 46**, 183-211 (1987)

[6] V. S. Miller, *Uses of Elliptic Curves in Cryptography*, Advances in Cryptology: Proceeding of Crypto '85, Lecture Notes in Computer Science, Springer-Verlag, **218**, 417-426 (1986)

[7] G. Menichetti, *Roots of Affine Polynomials*, Annals of Discrete Mathematics, **30**, 303-310 (1986)

[8] H. W. Lenstra, *Factoring Integers with Elliptic Curves*, Annals of Mathematics, **126**, 649-673 (1987)

[9] E. Waterhouse, *Abelian Varieties over Finite Fields*, Ann. Sci. Ecole. Norm. Sup., **2**, 521-560 (1969)

[10] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, (1986)

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, (1986)

[12] A. J. Menezes and S. Vanstone, *Isomorphism Classes of Elliptic Curves over Finite Fields of Characteristic Two*, Utilitas Mathematica, **38**, 135-153 (1990)

[13] A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, (1993)

[14] S. Vanstone, *Responses to NIST's Proposal*, Communications of the ACM, **35**, 50-52 (1992)

[15] N. Koblitz and A. J. Menezes, *A Survey of Public-Key Cryptosystems*, SIAM Review, **46**, 599-634 (2004)

[16] D. Johnson and A. J. Menezes, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, Univ. of Waterloo, (1999), "http://cacr.math.waterloo.ca"