ELLIPTIC CURVES AND THEIR APPLICATIONS IN CRYPTOGRAPHY

A Thesis Presented to
the Faculty of the Graduate School
University of Missouri

In Partial Fulfillment
of the Requirements for the Degree

Master of Science

---

by
MICHAEL PEMBERTON

Dr. William Banks, Thesis Supervisor

DECEMBER 2009

The undersigned, appointed by the Dean of the Graduate School,
have examined the thesis entitled

ELLIPTIC CURVES AND THEIR
APPLICATIONS IN CRYPTOGRAPHY

Presented by Michael Pemberton

A candidate for the degree of Master of Science

And hereby certify that in their opinion it is worthy of acceptance.

Professor William Banks

Professor Zhenbo Qin

Professor Youssef Saab

ACKNOWLEDGEMENTS

First of all, I would like to thank my thesis advisor, William Banks, for his support and understanding throughout the process of completing this thesis. His encouragement and guidance has helped me realize my passion for elliptic curves and cryptography and to pursue a career in the field.

To those professors who helped me begin my journey in advanced mathematics, thank you for all your patience and support. You have helped me to develop my love for mathematics and have inspired me to pass on my passion. In particular, would like to thank Ian Aberbach and Zhenbo Qin, for their numerous courses and seminars that I was privileged to enroll in while at Mizzou.

I would also like to thank my family and friends for all their unwavering support, love, patience, and encouragement. To my parents for all their love and inspiration in all that I do, and without their help, none of my accomplishments would be possible.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Figure Page

LIST OF TABLES

Table Page

ELLIPTIC CURVES AND THEIR
APPLICATIONS IN CRYPTOGRAPHY

Michael Pemberton

Dr. William Banks, Thesis Supervisor

ABSTRACT

In 1985, Koblitz and Miller proposed elliptic curves to be used for public key cryptosystems. This present thesis examines the role of elliptic curves on cryptography and basic problems involving implementation and security of some elliptic curve cryptosystems. Some of the aspects we are concerned with include:

- Methods to determine the number of points on an elliptic curve over a finite field
- Implementation of cryptosystems based on the discrete logarithm problem for elliptic curves defined over a finite field
- Examine an elliptic curve analogue of the RSA cryptosystem

We provide answers to these and discuss a number of applications for number theory, such as factorization and primality testing.

Chapter 1

Elliptic Curves

In this chapter we provide motivation for the study of elliptic curves in cryptography. We begin with basic forms in which an elliptic curve may be expressed, then discuss the group law, which provides the foundation for all cryptographic applications. We then provide a method to classify all elliptic curves up to isomorphism and conclude with a discussion of endomorphisms to provide the background needed for Hasse's theorem in Chapter 3.

1.1 Introduction

Let K be a field. For example, K can be the prime field $\mathbb{F}_p$, where p is a prime number, a finite extension field $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$, for some $n \geq 1$, or one of the fields of rational, real, or complex numbers.

Definition 1.1.1. *An elliptic curve E over a field K, denoted $E(K)$, is defined by the Weierstrauss equation for E,*

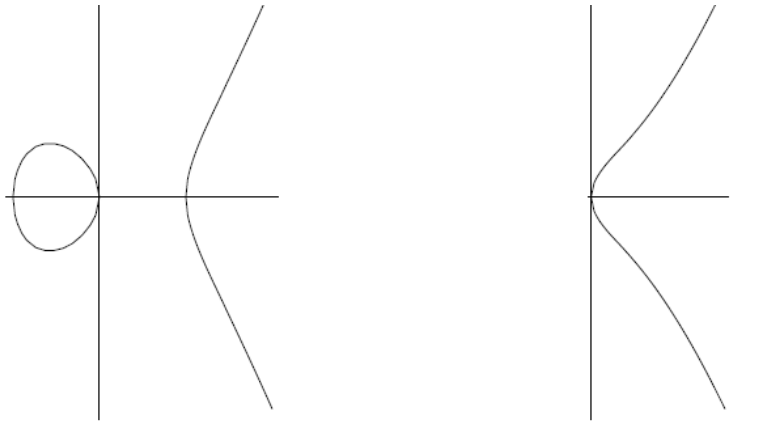
$$y^2 = x^3 + ax + b \tag{1.1}$$

where $a, b \in K$. The number of points on E is called the cardinality of E and is denoted $\#E(K)$, or simply $\#E$.

To consider points with coordinates in a field $L \supset K$, we write $E(L)$. By definition, this set will always contain the point ∞, which will be defined later. In other words,

$$E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + ax + b\} \cup \{\infty\}. \tag{1.2}$$

It is not possible to draw meaningful graphs over most fields, however over the field of real numbers $\mathbb{R}$, graphs of elliptic curves have two basic forms, depicted in Figure 1.1. The cubic $y^2 = x^3 - x = x(x-1)(x+1)$, in the first case has three distinct real roots. In the second case, the cubic $y^2 = x^3 + x = x(x^2+1)$ only has



$(a) \quad y^2 = x^3 - x$ $(b) \quad y^2 = x^3 + x$

Figure 1.1: Basic Forms of Elliptic Curves over $\mathbb{R}$

one real root. We do not allow multiple roots of the cubic by assuming that the discriminant of E, namely $\Delta = -(4a^3 + 27b^2) \neq 0$. Therefore, the roots of the cubic must be distinct.

We also consider elliptic curves over a field K defined by an equation of a more general form, called the generalized Weierstrauss equation.

Definition 1.1.2. *An elliptic curve E over a field K is defined by the generalized*

Weierstrauss equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.3}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

Elliptic curves of the form (1.3) are useful when working over a field K where $\text{char}(K) = 2, 3$. However, over a field of $\text{char}(K) \neq 2, 3$, any equation in generalized Weierstrauss form can be transformed into an equation in Weierstrauss form. If $\text{char}(K) \neq 2$, then we may divide an equation of the form (1.3) and complete the square to obtain

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right), \tag{1.4}$$

which can be written as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6' \tag{1.5}$$

with $y_1 = y + a_1x/2 + a_3/2$ and for some constants a_2', a_4', a_6'. Furthermore, if $\text{char}(K) \neq 3$, then we can let $x_1 = x + a_2'/3$ and obtain $y_1^2 = x_1^3 + ax_1 + b$ for some constants a, b. Therefore, we have arrived at an equation of the form (1.1).

Throughout this paper, we mainly use the Weierstrauss equation or the generalized Weierstrauss equation for an elliptic curve. However, elliptic curves arise in various other forms and is worthwhile to discuss these briefly.
The first form is a variant on the Weierstrauss equation called a Legendre equation. Its advantage is that it allows us to express all elliptic curves over an algebraically closed field K, with $\text{char}(K) \neq 2$, in terms of one parameter.

Proposition 1.1.3. *Let K be a field such that* $\mathrm{char}(K) \neq 2$ *and let*

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3) \tag{1.6}$$

be an elliptic curve E over K with $e_1, e_2, e_3 \in K$. Let

$$x_1 = (e_2 - e_1)^{-1}(x - e_1), \quad y_1 = (e_2 - e_1)^{-3/2}y, \quad \lambda = \frac{e_3 - e_1}{e_2 - e_1}. \tag{1.7}$$

Then, $\lambda \neq 0, 1$ and $y_1^2 = x_1(x_1 - 1)(x_1 - \lambda)$.

The parameter λ for E is not unique. In fact, each of

$$\left\{\lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}\right\} \tag{1.8}$$

yields a Legendre equation for E. They correspond to the six permutations of the roots e_1, e_2, e_3.

1.2 The Group Law

An elliptic curve E defined over a field K can be made into an abelian group by defining an additive operation on its points. Thus, start with two points

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2) \tag{1.9}$$

on an elliptic curve E given by $y^2 = x^3 + ax + b$. Define a new point $P_3 = (x_3, y_3)$ as follows. Draw the line L through the points P_1 and P_2. The line L intersects E in a uniquely determined point, which we denote as P_3'. Now reflect the point P_3' across the x-axis to obtain the point P_3. We define $P_1 + P_2 = P_3$.

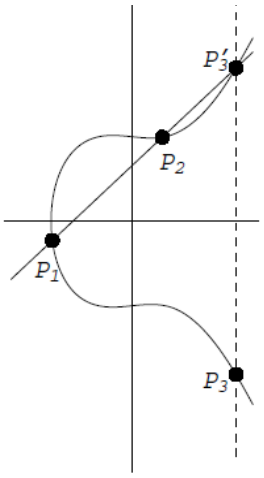


Figure 1.2: Addition on Elliptic Curves

We will now find explicit formulas to enable us to easily add and subtract points on an elliptic curve E. The derivation of these formulas uses elementary analytic geometry, differential calculus to find a tangent line, and a certain amount of algebraic manipulation. When $P_1 \neq P_2$ and that neither is ∞, we draw the line L through P_1 and P_2. The slope of L is given by

$$m = \frac{y_2 - y_1}{x_2 - x_1}. \tag{1.10}$$

Assume that $x_1 \neq x_2$ so that L is not a vertical line, then the equation of L is $y = m(x - x_1) + y_1$. To find the point of intersection with E, we substitute to get

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b \implies 0 = x^3 - m^2x^2 + \cdots . \tag{1.11}$$

Therefore, the three roots of this cubic correspond to the three points of intersection of L with E. We already know two solutions, namely x_1 and x_2. Thus, the third solution is $x = m^2 - x_1 - x_2$ and $y = m(x - x_1) + y_1$. Therefore, $P_3' = (x, y)$ and by reflecting across the x-axis we obtain the point $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1. \tag{1.12}$$

If $x_1 = x_2$ but $y_1 \neq y_2$, then L is a vertical line through P_1 and P_2 which intersects E at the point ∞. By reflecting ∞ across the x-axis we still obtain the same point ∞. Therefore, in this case $P_1 + P_2 = \infty$.

When $P_1 = P_2$ we construct the tangent line L at the point $(x_1, y_1) = (x_2, y_2)$. Hence by implicit differentiation we find that

$$2y\frac{dy}{dx} = 3x^2 + a, \quad \text{so} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}. \tag{1.13}$$

If $y_1 = 0$, then the line L is again a vertical line and we set $P_1 + P_2 = \infty$, as before. Therefore, assume that $y_1 \neq 0$. The equation of L is $y = m(x - x_1) + y_1$ so by substitution we obtain $0 = x^3 - m^2x^2 + \cdots$, as before. However, this time we know only one solution to the cubic, namely x_1, but it is a double root since L is tangent to E at P_1. Thus, $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$.

Finally, suppose that $P_2 = \infty$. The line through $P_1 = (x_1, y_1)$ and P_2 is a vertical line that intersects E at the point P_1'. By reflecting P_1' across the x-axis we obtain P_1, so that $P_1 + P_2 = P_1 + \infty = P_1$ for all points P_1 on E.

Therefore, we summarize our previous discussions into the following theorem, which is called the group law for addition of points on an elliptic curve of the form (1.1).

Theorem 1.2.1. *Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*

(1) If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \textit{where} \quad m = \frac{y_2 - y_1}{x_2 - x_1}. \tag{1.14}$$

(2) *If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.*

(3) *If $P_1 = P_2$ and $y_1 \neq 0$, then*

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \textit{where} \quad m = \frac{3x_1^2 + a}{2y_1}. \tag{1.15}$$

(4) *If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.*

Moreover, define $P + \infty = P$, for all points P on E.

Theorem 1.2.2. *The addition of points on an elliptic curve E satisfies:*

(1) *$P_1 + P_2 = P_2 + P_1$, for all P_1, P_2 on E.*

(2) *$P + \infty = P$, for all P on E.*

(3) *Given P on E, there exists P' on E such that $P + P' = \infty$. We will denote the point P' by $-P$.*

(4) *$P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$, for all P_1, P_2, P_3 on E.*

Proof. To prove commutativity of addition, note that the line through two points P_1 and P_2 on E is the same line through P_2 and P_1. The identity property of ∞ holds by definition. For inverses, let P' be the reflection of P across the x-axis. Then $P + P' = \infty$.

Finally, we need to prove associativity. This is by far the most subtle and non-obvious property of the addition of points on E. The associative law can be verified by calculation with the formulas. There are several cases which makes the proof rather complicated. See [5], [7] for a proof of the associative law on E. □

In other words, the points on E form an additive abelian group with ∞ as the identity element. Note that if E is defined over a finite field K, then there are finitely many points on E. Thus, we instead obtain a finite additive abelian group.

Although, reflection of a point $P = (x, y)$ across the x-axis for an elliptic curve of the form (1.1) is given by $-P = (x, -y)$, for the generalized Weierstrauss equation (1.3) this is no longer the case. In fact, if $P = (x, y)$ is on the curve described by (1.3), then $-P = (x, -a_1x - a_3 - y)$.

Example 1.2.3. Let E be the elliptic curve defined over $\mathbb{Q}$ by

$$y^2 = x^3 + 7x + 3 \tag{1.16}$$

then we have that

$$2(2, 5) = (2, 5) + (2, 5) = \left(-\frac{39}{100}, -\frac{459}{1000}\right). \tag{1.17}$$

Note that we also have

$$(0, 0) + (-2, 0) = (2, 0), \quad 2(0, 0) = 2(-2, 0) = 2(2, 0) = \infty. \tag{1.18}$$

1.3 The j-Invariant

An important invariant used to determine whether two elliptic curves are isomorphic over an algebraically closed field is the j-invariant. Therefore, let E be the elliptic curve given by (1.1) defined over a field K with $\text{char}(K) \neq 2, 3$. If we let

$$x_1 = \mu^2 x, \quad y_1 = \mu^3 y, \tag{1.19}$$

with $\mu \in \overline{K}^{\times}$, then we obtain $y_1^2 = x_1^3 + a_1x_1 + b_1$ where $a_1 = \mu^4 a$ and $b_1 = \mu^6 b$.

Definition 1.3.1. *The j-invariant of an elliptic curve E given by $y^2 = x^3 + ax + b$ is defined to be*

$$j = j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{1.20}$$

Note that the denominator is the negative of the discriminant of the cubic, hence is nonzero by assumption. The change of variables (1.19) leaves j unchanged. The converse is true as well.

Theorem 1.3.2. *Let $y_1^2 = x_1^3 + a_1x_1 + b_1$ and $y_2^2 = x_2^3 + a_2x_2 + b_2$ be two elliptic curves with j-invariants j_1 and j_2 respectively. If $j_1 = j_2$, then there exists $\mu \neq 0$ in $\overline{K}$ such that*

$$a_2 = \mu^4 a_1, \quad b_2 = \mu^6 b_1. \tag{1.21}$$

The transformation $x_2 = \mu^2 x_1$ and $y_2 = \mu^3 y_1$ takes one equation to the other.

Proof. First, assume that $a_1 \neq 0$. Since this is equivalent to $j_1 \neq 0$, we also have that $a_2 \neq 0$. Choose μ such that $a_2 = \mu^4 a_1$. Then we have

$$\frac{4a_2^3}{4a_2^3 + 27b_2^2} = \frac{4a_1^3}{4a_1^3 + 27b_1^2} = \frac{4\mu^{-12}a_2^3}{4\mu^{-12}a_2^3 + 27b_1^2} = \frac{4a_2^3}{4a_2^3 + 27\mu^{12}b_1^2}, \tag{1.22}$$

which implies that $b_2^2 = (\mu^6 b_1)^2$. Therefore, $b_2 = \pm\mu^6 b_1$. If $b_2 = \mu^6 b_1$ then we are finished. If $b_2 = \mu^6 b_1$, then we change μ to $i\mu$. This preserves the relation $a_2 = \mu^4 a_1$ and also gives $b_2 = \mu^6 b_1$.

If $a_1 = 0$, then $a_2 = 0$. Since $\Delta = -(4a^3 + 27b^2) \neq 0$, we have $b_1, b_2 \neq 0$. Choose μ such that $b_2 = \mu^6 b_1$. □

There are two special values of the j-invariant that arise often. First, when an elliptic curve E is of the form $y^2 = x^3 + b$, then $j(E) = 0$. The other case involves when E is of the form $y^2 = x^3 + ax$, where $j(E) = 1728$. The curves with $j = 0$ and with $j = 1728$ have automorphisms other than the automorphism defined by $(x, y) \mapsto (x, -y)$, which is an automorphism for any elliptic curve in Weierstrauss form (1.1).

In particular, $y^2 = x^3 + b$ has the automorphism $(x, y) \mapsto (\zeta x, -y)$, where ζ is a nontrivial cube root of 1 and $y^2 = x^3 + ax$ has the automorphism $(x, y) \mapsto (-x, iy)$. Note that the j-invariant allows us to determine whether two curves are isomorphic over an algebraically closed field. However, if we are working with a non-algebraically closed field, then it is possible to have two curves with the same j-invariant that cannot be transformed into each other using rational functions with coefficients in the field.

The j-invariant can similarly be defined for an elliptic curve in generalized Weierstrauss form (1.3). Associated to the coefficients a_1, a_2, a_3, a_4, a_6 in (1.3) are the coefficients

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned}$$

Note that these quantities are related by $4b_8 = b_2b_6 - b_4^2$. We also introduce the discriminant of a curve in generalized Weierstrauss form in terms of the b_i's,

$$\Delta' = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{1.23}$$

Along with the coefficients a_i from (1.3) and the b_i from above, we define the coefficients

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \tag{1.24}$$

Therefore, the j-invariant of an elliptic curve of the form (1.3) is given as

$$j = j(E) = \frac{c_4^3}{\Delta'}. \tag{1.25}$$

1.4 Fields of Characteristic 2

Since we used the Weierstrass equation rather than the generalized Weierstrass equation, the formulas derived in Theorem (1.2.1) do not apply when the characteristic of the field K is 2. In this section, we focus on the case when E is an elliptic curve in generalized Weierstrauss form and $\text{char}(K) = 2$.

Let E be an elliptic curve of the form (1.3), then by an appropriate power of z we make the generalized Weierstrauss equation homogenous of degree 3, that is given as

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{1.26}$$

By setting $z = 0$ we obtain that $x^3 = 0$ so that $\infty = (0 : 1 : 0)$ is the only point at infinity of E, just as in the standard Weierstrauss equation. Furthermore, if L is the line through (x_0, y_0) and ∞ then we see that L is the vertical line $x = x_0$. If $(x_0, y_0) \in E$, then the other point of intersection of L and E is given by $(x_0, -a_1x_0 - a_3 - y_0)$.

Therefore, we can now describe addition of points. Note that by the definition of ∞ we have that $P + \infty = P$, for all points P on E. Recall that in projective space that three points P, Q, and R are collinear if and only if they sum to ∞. Thus, the negation of a point $P = (x, y)$ is given as

$$-P = -(x, y) = (x, -a_1x - a_3 - y). \tag{1.27}$$

Thus, to add two points P_1 and P_2, we proceed as follows. Draw the line L through P_1 and P_2 and take the tangent line if $P_1 = P_2$. The line L will intersect E at a third point P_3'. Now compute $-P_3' = P_3$ given by the above formula, which is not simply the reflection across the x-axis. Then, we define $P_1 + P_2 = P_3$.

The proof that this addition law is associative is the same as that given in [7]. The points on E, including ∞, therefore form an abelian group.

If we are working over a large finite field, as we will see in Chapter 5, and we are given a point P on an elliptic curve E and a positive integer k, then $kP = P + P + \cdots + P$ (k times). However, a faster way of computing kP is by successive doubling. That is, $P + P = 2P$, $2P + 2P = 4P$, $4P + 4P = 8P$, so that $16P + 2P + P = 19P$. Since we will need it later, we will look at the formula for doubling a point in characteristic 2.

We work with the generalized Weierstrass equation for an elliptic curve E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.28}$$

If $a_1 \neq 0$, then the change of variables

$$x = a_1^2x_1 + \left(\frac{a_3}{a_1}\right), \quad y = a_1^3y_1 + a_1^{-3}(a_1^2a_4 + a_3^2) \tag{1.29}$$

changes the equation to the form

$$y_1^2 = x_1y_1 = x_1^3 + a_2'x_1^2 + a_6'. \tag{1.30}$$

If $a_1 = 0$, we let $x = x_1 + a_2$, $y = y_1$ to obtain an equation of the form

$$y_1^2 + a_3'y_1 = x_1^3 + a_4'x_1 + a_6'. \tag{1.31}$$

The first case will be for curves of the form, $y^2 + xy = x^3 + a_2x^2 + a_6$. An equation of this form is equivalent to $y^2 + xy + x^3 + a_2x^2 + a_6 = 0$, since we are performing operations in characteristic 2. Thus, by implicit differentiation

$$2y\frac{dy}{dx} + x\frac{dy}{dx} + y + 3x^2 + 2a_2x = x\frac{dy}{dx} + y + x^2 = 0 \implies \frac{dy}{dx} = \frac{x^2 + y}{x}, \quad (1.32)$$

we see that the slope of L through $P = (x_0, y_0)$ is

$$m = \frac{dy}{dx} = \frac{y_0 + x_0^2}{x_0}. \quad (1.33)$$

Thus, the equation of L is $y = m(x - x_0) + y_0 = mx + b$ for some b, so by substitution we find

$$x_1 = m^2 + m + a_2 = \frac{y_0^2 + x_0^4 + x_0y_0 + x_0^3 + a_2x_0^2}{x_0^2} = \frac{x_0^4 + a_6}{x_0^2} \quad (1.34)$$

since $y_0^2 = x_0y_0 + x_0^3 + a_2x_0^2 + a_6$ and $y_1 = m(x - x_0) + y_0$. The point $(x_1, y_1) = -2P$ so that $(x_2, y_2) = 2P$ with

$$x_2 = \frac{x_0^4 + a_6}{x_0^2}, \quad y_2 = -x_1 - y_1 = x_1 + y_1. \quad (1.35)$$

For curves of the other form, $y^2 + a_3y = x^3 + a_4x + a_6$, we rewrite this as $y^2 + a_3y + x^3 + a_4x + a_6 = 0$. Therefore, by a similar argument as in the previous case we find that $2P = (x_2, y_2)$ where

$$x_2 = \frac{x_0^4 + a_4^2}{a_3^2}, \quad y_2 = a_3 + y_1. \quad (1.36)$$

1.5 Endomorphisms

The main purpose of this section is to prove Proposition 1.5.1, which will be used in the proof of Hasse's theorem. By an endomorphism of an elliptic curve E,

we mean a group homomorphism $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$ that is given by rational functions. In other words, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, and there are rational functions $R_1(x, y)$, $R_2(x, y)$ with coefficients in $\overline{K}$ with $\alpha(x, y) = (R_1(x, y), R_2(x, y))$ for all $(x, y) \in E(\overline{K})$. Since α is a homomorphism, we have $\alpha(\infty) = \infty$.

It is useful to have a standard form for the rational functions describing an endomorphism. We assume that an elliptic curve E is given in Weierstrauss form. Let $R(x, y)$ be any rational function. Since $y^2 = x^3 + ax + b$ for all $(x, y) \in E(\overline{K})$, we can replace any even power of y by a polynomial in x and obtain a rational function that gives the same function as $R(x, y)$ on points of $E(\overline{K})$. Therefore, we may assume

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{1.37}$$

Thus, by rationalization and replacing y^2 with $x^3 + ax + b$ we obtain

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{1.38}$$

Now consider an endomorphism given by $\alpha(x, y) = (R_1(x, y), R_2(x, y))$ as before. Since α is a homomorphism, $\alpha(x, -y) = -\alpha(x, y)$ so that $R_1(x, -y) = R_1(x, y)$ and $R_2(x, -y) = -R_2(x, y)$. Therefore, if $R_1(x, y)$ is in the form (1.38), then $q_2(x) = 0$ and if $R_2(x, y)$ is in the form (1.38), then $q_1(x) = 0$. Thus, we may assume that $\alpha(x, y) = (r_1(x), r_2(x)y)$ with rational functions $r_1(x)$ and $r_2(x)$.

We can now discuss what happens when a rational function is not defined at a point. Write

$$r_1(x) = \frac{p(x)}{q(x)} \tag{1.39}$$

be such that $\gcd(p(x), q(x)) = 1$. If $q(x) = 0$ for some point (x, y), then we assume

that $\alpha(x, y) = \infty$. If $q(x) \neq 0$, then $r_2(x)$ is defined and thus the rational functions defining α are defined.

We define the degree of an endomorphism α to be

$$\deg(\alpha) = \max\{\deg(p(x)), \deg(q(x))\} \tag{1.40}$$

provided that α is nontrivial, that is, an endomorphism that does not send all points (x, y) to ∞. When $\alpha = 0$, let $\deg(0) = 0$. Define $\alpha \neq 0$ to be a separable endomorphism if the derivative $r_1'(x)$ is not identically zero. Note that this is equivalent to saying that at least one of $p'(x)$ and $q'(x)$ is not identically zero.

We are now ready to state Proposition 1.5.1 which will be crucial in the proof of Hasse's theorem.

Proposition 1.5.1. *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then*

$$\deg(\alpha) = \#\mathrm{Ker}(\alpha), \tag{1.41}$$

where $\mathrm{Ker}(\alpha)$ *is the kernel of the homomorphism $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$. If $\alpha \neq 0$ is not separable, then*

$$\deg(\alpha) > \#\mathrm{Ker}(\alpha). \tag{1.42}$$

Proof. Write $\alpha(x, y) = (r_1(x), r_2(x)y)$ with r_1 and r_2 as above. Then $r_1'(x) \neq 0$, so $p'(x)q(x) - p(x)q'(x) \neq 0$. Let $S = \{x \in \overline{K} \mid (p'(x)q(x) - p(x)q'(x))q(x) = 0\}$. Let $(a, b) \in E(\overline{K})$ be such that

(1) $a \neq 0$, $b \neq 0$, and $(a, b) \neq \infty$,

(2) $\deg(p(x) - aq(x)) = \max\{\deg(p(x)), \deg(q(x))\} = \deg(\alpha)$,

(3) $a \notin r_1(S)$, and

(4) $(a, b) \in \alpha(E(\overline{K}))$.

Since $p'(x)q(x) - p(x)q'(x) \neq 0$, we have S is a finite set and hence $\alpha(S)$ is finite as well. The function $r_1(x)$ takes on infinitely many distinct values as x runs through $\overline{K}$. Since, for each x, there is a point $(x, y) \in E(\overline{K})$, we see that $\alpha(E(\overline{K}))$ is an infinite set. Therefore, such a point (a, b) exists.

We claim that there are exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a, b)$. For such a point, we have

$$\frac{p(x_1)}{q(x_1)} = a, \quad r_2(x_1)y_1 = b. \tag{1.43}$$

Since $(a, b) \neq \infty$, we must have $q(x_1) \neq 0$ so $r_2(x_1)$ is defined. Since $b \neq 0$ and $r_2(x_1)y_1 = b$, we must have $y_1 = b/r_2(x_1)$. Therefore, x_1 determines y_1 in this case, so we only need to count values of x_1.

By assumption (2), $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicities. We therefore must show that $p(x) - aq(x)$ has no multiple roots. Suppose that x_0 is a multiple root. Then $p(x_0) - aq(x_0) = 0$ and $p'(x_0) - aq'(x_0) = 0$. Multiplying the equations $p(x) = aq(x)$ and $aq'(x) = p'(x)$ yields $ap(x_0)q'(x_0) = ap'(x_0)q(x_0)$. Since $a \neq 0$, this implies that x_0 is a root of $p(x)q'(x) - p'(x)q(x)$, so $x_0 \in S$. Therefore, $a = r_1(x_0) \in r_1(S)$, contrary to assumption. It follows that $p(x) - aq(x)$ has no multiple roots, and therefore has $\deg(\alpha)$ distinct roots.

Since there are exactly $\deg(\alpha)$ points (x_1, y_1) with $\alpha(x_1, y_1) = (a, b)$, we see that $\#\mathrm{Ker}(\alpha) = \deg(\alpha)$. Furthermore, if α is not separable, then the steps of the proof hold, except that $p'(x) - aq'(x) = 0$, so $p(x) - aq(x) = 0$ always has multiple

roots and therefore has fewer than $\deg(\alpha)$ solutions. $\square$

One important example of an endomorphism is the Frobenius map, which plays a crucial role in the theory of elliptic curves over $\mathbb{F}_q$. Suppose that E is an elliptic curve defined over a finite field $\mathbb{F}_q$. The Frobenius map is defined as $\varphi_q(x, y) = (x^q, y^q)$. Note that if E is an elliptic curve defined over a finite field $\mathbb{F}_q$, then φ_q is an endomorphism of degree q and is not separable.

1.6 Singular Curves

We have been working with $y^2 = x^3 + ax + b$ under the assumption that $x^3 + ax + b$ has distinct roots. However, when there are multiple roots it turns out that elliptic curve addition becomes either addition of elements in K or multiplication of elements in $K^\times$ or in a quadratic extension of K. This means that an algorithm for a group $E(K)$ arising from elliptic curves, such as the discrete logarithm problem, will probably also apply to these more familiar situations. Moreover, we will also see that singular curves arise naturally when elliptic curves defined over the integers are reduced modulo various primes.

First consider the case where $x^3 + ax + b$ has a triple root at $x = 0$, so the curve becomes $y^2 = x^3$. Note that only $(0, 0)$ is a singular point on the curve, since any line through $(0, 0)$ intersects the curve at most one other point. Therefore, we exlude the point $(0, 0)$ from the group so that addition may be defined on the curve. The set of all remaining form a group with the same group law as in the case when the cubic has distinct roots. We need to check that addition of any two points on the cubic does not yield the excluded point $(0, 0)$. However, a line through

two nonsingular points cannot pass through $(0,0)$, so this is not a problem.

The next theorem is Theorem 2.30 in [7] and shows that whenever the cubic has a triple root, or cusp, the group of nonsingular points on the curve, with coordinates considered in K, is isomorphic to K.

Theorem 1.6.1. *Let E be the curve $y^2 = x^3$ and let $E_{ns}(K)$ be the nonsingular points on this curve, regarded as an additive group, with coordinates in K including the point $\infty = (0:1:0)$. The map*

$$\varphi : E_{ns}(K) \longrightarrow K \tag{1.44}$$

given by $(x,y) \mapsto x/y$ and $\infty \mapsto 0$ is a group isomorphism.

Now we consider the second case where $x^3 + ax + b$ has a double root. By translation we may regard the double root at $x = 0$ so that the curve becomes

$$y^2 = x^2(x + a) \tag{1.45}$$

for some $a \neq 0$. The only singular point is $(0,0)$ for the same reason as above. Again, consider the group of all nonsingular points of the curve with coordinates in K including ∞. Let $\alpha^2 = a$, so that α might lie in an extension of K.

The equation (1.45) may be written as

$$\left(\frac{y}{x}\right)^2 = x + a. \tag{1.46}$$

Note that whenever $x \to 0$, then the right-hand side of (1.46) is approximately a. Therefore, the curve is approximated by tangent lines $y = \alpha x$ and $y = -\alpha x$ near $x = 0$ and we obtain the next theorem, which is Theorem 2.31 in [7].

Theorem 1.6.2. *Let E be the curve $y^2 = x^2(x+a)$, where $a \in K^\times$. Let $E_{ns}(K)$ be the nonsingular points on E with coordinates in K.*

Let $\alpha^2 = a$ and consider the map

$$\varphi : (x, y) \mapsto \frac{y + \alpha x}{y - \alpha x}, \quad \text{and} \quad \infty \mapsto 1. \tag{1.47}$$

(1) If $\alpha \in K$ then $E_{ns}(K) \cong K^\times$, considered a multiplitative group.

(2) If $\alpha \notin K$ then $E_{ns}(K) \cong \{u + \alpha v \mid u, v \in K, u^2 - av^2 = 1\}$, considered a group under multiplication.

One situation that arises when we consider singular curves is when we consider curves with integral coefficients and reduce modulo various prime numbers.

Example 1.6.3. Let E be the elliptic curve $y^2 = x(x+35)(x-55)$, then we have the following situations.

$$E \ (mod\ 5) \ : \ y^2 \equiv x^3 \tag{1.48}$$

$$E \ (mod\ 7) \ : \ y^2 \equiv x^2(x-6) \equiv x^2(x+1) \tag{1.49}$$

$$E \ (mod\ 11) \ : \ y^2 \equiv x^2(x+2) \tag{1.50}$$

The case (1.48) is exactly in the form of Theorem 1.6.1, which implies that $E_{ns}(\mathbb{F}_5) \cong \mathbb{F}_5$ and is called an additive reduction. The second case (1.49) is called a split multiplicative reduction and is covered by Theorem 1.6.2(1) and states that $E_{ns}(\mathbb{F}_7) \cong \mathbb{F}_7^\times$. Finally, (1.50) is in the form of Theorem 1.6.2(2) since $\alpha = 2^2 = 4 \notin \mathbb{F}_{11}$ and is called a nonsplit multiplication reduction.

Chapter 2

Torsion Points

The torsion points, namely those that have finite order, play an important role in the study of elliptic curves. In Chapter 3, we will see that all points are torsion points on an elliptic curve over a finite field. We then study the properties of the Weil pairing, which is used in the proof of Hasse's theorem and in Chapter 4 to attack the elliptic curve discrete logarithm problem.

2.1 Torsion Points

We begin by defining the set of all torsion points of order n.

Defintion 2.1.1. *Let E be an elliptic curve defined over a field K. Let n be a positive integer, then the set of n-torsion points is*

$$E[n] = \left\{ P \in E(\overline{K}) \mid nP = \infty \right\}. \tag{2.1}$$

Note that the set $E[n]$ contains points with coordinates in $\overline{K}$, not just in K.

Whenever $\text{char}(K) \neq 2$, then we can describe the set $E[2]$. Let

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{2.2}$$

with $e_1, e_2, e_3 \in \overline{K}$. Recall from Theorem 1.2.1 that $2P = \infty$ if and only if the

tangent line at P is vertical. Therefore, we see that $y = 0$ and thus

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2. \tag{2.3}$$

However, when $\text{char}(K) = 2$ we have seen that E has the form

$$y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \tag{2.4}$$

or the form

$$y^2 + a_3y + x^3 + a_4x + a_6 = 0. \tag{2.5}$$

To avoid the case where the curve becomes singular, (2.4) must have that $a_6 \neq 0$ and (2.5) must have $a_3 \neq 0$. If $P = (x, y)$ is point of order 2, then the tangent line at P is vertical. This means that $d/dy(x, y) = 0$. In (2.4), this means that $x = 0$ so by substitution we see that

$$y^2 + xy + x^3 + a_2x^2 + a_6 = y^2 + a_6 = 0 \implies (y + \sqrt{a_6})^2 = 0. \tag{2.6}$$

Therefore, $(0, \sqrt{a_6})$ is the only point of order 2, so that $E[2] = \left\{\infty, (0, \sqrt{a_6})\right\} \cong \mathbb{Z}_2$.

In addition, we see that whenever $d/dy(x, y) = a_3 \neq 0$ there is no point of order 2 for elliptic curves of the form (2.5). In this case, $E[2] = \{\infty\}$.

Proposition 2.1.2. *Let E be an elliptic curve over a field K. If* $\text{char}(K) \neq 2$, *then $E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. If* $\text{char}(K) = 2$, *then $E[2] \cong 0$ or $E[2] \cong \mathbb{Z}_2$.*

Now we consider the set $E[3]$. Again we assume that $\text{char}(K) \neq 2, 3$, then we can represent E by (1.1). A point P satisfies $3P = \infty$ if and only if $2P = -P$. Thus, the x-coordinate of $2P$ is the x-coordinate of P, but the y-coordinates of the two points differ by a sign. If the y-coordinates were the same, then $2P = P$ would imply that that $P = \infty$.

Using the formulas derived in Theorem 1.2.1, we see that

$$x = m^2 - 2x \quad \textit{and} \quad y = \frac{3x^2 + a}{2m}. \tag{2.7}$$

Therefore, $y^2 = x^3 + ax + b$ becomes

$$\left(\frac{3x^2 + a}{2m}\right)^2 = x^3 + ax + b \implies 3x^4 + 6ax^2 + 12bx - a^2 = 0. \tag{2.8}$$

The discriminant of this polynomial is $\Delta = -6912(4a^3 + 27b^2)^2 \neq 0$. Hence, the polynomial has no multiple roots, so that there are four distinct values of x. Further, each value of x gives two different values of y. So we have 8 points of order 3 together with ∞. Thus, $E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Whenever the $\text{char}(K) = 2$, we use a similar argument with the formulas given in (1.35) and (1.36). If $\text{char}(K) = 3$ then we may assume that E has the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{2.9}$$

Again we have that $2P = -P$ implies that the x-coordinates of the two points are the same. Since $\text{char}(K) = 3$ we obtain

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0. \tag{2.10}$$

However, (2.10) implies that $a_2x^3 + a_2a_6 - a_4^2 = 0$ since $4 \equiv 1 \pmod 3$. Note that we cannot have that $a_2 = a_4 = 0$, since that would imply $x^3 + a_6 = (x + \sqrt[3]{a_6})^3$ has multiple roots. Thus, at least one of a_2 or a_4 is nonzero.

If $a_2 = 0$, then we have that $-a_4^2 = 0$ which cannot occur. Thus, there are no values of x and $E[3] = \{\infty\}$. On the other hand, if $a_2 \neq 0$ then $a_2(x^3 + a) = 0$ which gives a triple root in characteristic 3. Thus, there is one x-value and two corresponding y-values. This gives two points of order 3 and ∞, so that $E[3] \cong \mathbb{Z}_3$.

The general situation is given as the following, which is Theorem 3.2 in [7].

Theorem 2.1.3. *Let E be an elliptic curve over a field K and let n be a positive integer. If $\mathrm{char}(K) \nmid n$ or $\mathrm{char}(K) = 0$, then*

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n. \tag{2.11}$$

If $\mathrm{char}(K) = p > 0$ and $p|n$, we write $n = p^r n'$ where $p \nmid n'$, then

$$E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{or} \quad E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}. \tag{2.12}$$

In the case where an elliptic curve E is defined over a field K such that $\mathrm{char}(K) = p$, then E is called ordinary if $E[p] \cong \mathbb{Z}_p$. If $E[p] \cong 0$, then E is called supersingular. This is not to be confused with singular curves, which are curves that contain at least one singular point.

Now let n be a positive integer such that $\mathrm{char}(K) \nmid n$. Choose a basis $\{\beta_1, \beta_2\}$ for $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. Then every element of $E[n]$ can be expressed as a linear combination of β_1 and β_2. Note that the coefficients are uniquely determined modulo n.

Let $\alpha_n : E(\overline{K}) \longrightarrow E(\overline{K})$ be a group homomorphism, then α maps $E[n]$ into $E[n]$ by restriction. Thus, there exists $a, b, c, d \in \mathbb{Z}_n$ such that $\alpha(\beta_1) = a\beta_1 + c\beta_2$ and $\alpha(\beta_2) = b\beta_1 + d\beta_2$. Thus, each homomorphism $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$ is represented by a 2×2 matrix

$$\alpha_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{2.13}$$

Composition of group homomorphisms corresponds to multiplication of matrices.

2.2 The Weil Pairing

We now discuss the Weil pairing on the n-torsion of an elliptic curve. Let E be an elliptic curve over a field K and n be an integer such that $\text{char}(K) \nmid n$. Then, Theorem 2.1.3 states that $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Let $\mu_n = \left\{x \in \overline{K} \mid x^n = 1\right\}$ be the group of nth roots of unity in $\overline{K}$. Since $\text{char}(K) \nmid n$, the equation $x^n = 1$ has no multiple roots, thus has n distinct roots in $\overline{K}$. Therefore, μ_n is a cyclic group of order n. Any generator ζ of μ_n is called a primitive nth root of unity.

The following theorem is Theorem 3.9 in [7], which defines the Weil pairing and properties that the pairing must satisfy.

Theorem 2.2.1. *Let E be an elliptic curve defined over a field K and let n be a positive integer such that* $\text{char}(K) \nmid n$. *Then there is a pairing*

$$e_n : E[n] \times E[n] \longrightarrow \mu_n, \tag{2.14}$$

called the Weil pairing that satisfies the following properties:

(1) *e_n is bilinear in each variable. In other words,*

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q) \tag{2.15}$$

and

$$e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2) \tag{2.16}$$

for all $P, P_1, P_2, Q, Q_1, Q_2 \in E[n]$.

(2) *e_n is nondegenerate in each variable. This means that if $e_n(P, Q) = 1$ for all $Q \in E[n]$, then $P = \infty$ and similarly if $e_n(P, Q) = 1$ for all $P \in E[n]$,*

then $Q = \infty$.

(3) $e_n(P, P) = 1$, *for all* $P \in E[n]$.

(4) $e_n(P, Q) = e_n(Q, P)^{-1}$ *for all* $P, Q \in E[n]$.

(5) $e_n(\sigma P, \sigma Q) = \sigma(e_n(P, Q))$ *for all automorphisms* σ *of* $\overline{K}$ *such that* σ *is the identity map on the coefficients of* E.

(6) $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg(\alpha)}$ *for all separable endomorphisms* α *of* E. *If the coefficients of* E *lie in a finite field* $\mathbb{F}_q$, *then the statement also holds when* α *is the Frobenius endomorphism* φ_q.

Corollary 2.2.2. *Let* $\{P_1, P_2\}$ *be a basis of* $E[n]$, *then* $e_n(P_1, P_2)$ *is a primitive* n*th root of unity.*

Proof. Suppose that $e_n(P_1, P_2) = \zeta$ with $\zeta^d = 1$, then $e_n(P_1, dP_2) = 1$. In addition, $e_n(P_2, dP_2) = e_n(P_2, P_2)^d = 1$ by Theorem 2.2.1(1) and (3).

Let $P \in E[n]$ then $P = aP_1 + bP_2$ for some $a, b \in \mathbb{Z}$. Hence,

$$e_n(P, dP_2) = e_n(aP_1 + bP_2, dP_2) = e_n(P_1, dP_2)^a e_n(P_2, dP_2)^b = 1. \tag{2.17}$$

Since (2.17) holds for all $P \in E[n]$, then Theorem 2.2.1(2) implies that $dP_2 = \infty$. Since $dP_2 = \infty$ if and only if $n|d$, we find that ζ is a primitive nth root of unity. □

We now use the Weil pairing to deduce two statements that will be used in the proof of Hasse's theorem in Chapter 3. Recall that α is an endomorphism of E, then we obtain a matrix of the form (2.13) with entries in $\mathbb{Z}_n$, describing the group action α on a basis $\{P_1, P_2\}$.

Proposition 2.2.3. *Let* α *be an endomorphism of an elliptic curve* E *defined*

over a field K. Let n be a positive integer such that $\mathrm{char}(K) \nmid n$. *Then* $\deg(\alpha_n) \equiv \deg(\alpha) \pmod{n}$.

Proof. Suppose that $\zeta = e_n(P_1, P_2)$ be a primitive nth root of unity. By Theorem 2.2.1(6), we see that

$$\begin{aligned} \zeta^{\deg(\alpha)} &= e_n(\alpha(P_1), \alpha(P_2)) = e_n(aP_1 + cP_2, bP_1 + dP_2) \\ &= e_n(P_1, P_1)^{ab} e_n(P_1, P_2)^{ad} e_n(P_2, P_1)^{bc} e_n(P_2, P_2)^{cd} \\ &= e_n(P_1, P_2)^{ad} e_n(P_1, P_2)^{-bc} = e_n(P_1, P_2)^{ad-bc} = \zeta^{ad-bc}, \end{aligned} \tag{2.18}$$

by the properties of the Weil pairing. Since ζ is a primitive nth root of unity, $\deg(\alpha) \equiv (ad - bc) \pmod{n}$. □

The previous result allows us to reduce questions about the degree of an endomorphism to calculations with matrices. Now let α and β be endomorphisms of E and $a, b \in \mathbb{Z}$. If we let $P = (x, y)$ be a point on E, then the endomorphism $a\alpha + b\beta$ is defined by

$$(a\alpha + b\beta)(x, y) = a\alpha(x, y) + b\beta(x, y). \tag{2.19}$$

Here $a\alpha(x, y)$ means multiplication on E of $\alpha(x, y)$ by a. Similiarly for $b\beta(x, y)$, then the results are added on E. This process can all be described by rational functions since this is true for each of the individual steps. Therefore, $a\alpha + b\beta$ is an endomorphism.

Proposition 2.2.4. *Let $a, b \in \mathbb{Z}$. Then for any endomorphisms α and β*

$$\deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)). \tag{2.20}$$

Proof. Let n be a positive integer such that $\mathrm{char}(K) \nmid n$. Represent α and β by matrices α_n and β_n with respect to some basis of $E[n]$. Then $a\alpha_n + b\beta_n$ gives the action of $a\alpha_n + b\beta_n$ on $E[n]$. Therefore, we have that

$$\begin{aligned} &\det\left(a\alpha_n + b\beta_n\right)) = \\ &a^2 \det(\alpha_n) + b^2 \det(\beta_n) + ab(\det(\alpha_n + \beta_n) - \det(\alpha_n) - \det(\beta_n)) \end{aligned} \tag{2.21}$$

for any matrices α_n and β_n. Hence,

$$\begin{aligned} &\deg(a\alpha + b\beta) \equiv \\ &(a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta))) \pmod{n}. \end{aligned} \tag{2.22}$$

Since (2.22) holds for infinitely many n, we obtain (2.20). □

Chapter 3

Elliptic Curves over Finite Fields

Whenever E is an elliptic curve over a finite field K, then there are only finitely many points (x, y) with $x, y \in K$. Therefore, the additive group $E(K)$ is finite and so can we can apply theorems from finite group theory. The main result in this chapter is Hasse's theorem, which is proved in Section 3.2, and allows us to provide a bound on the order of $E(K)$. We conclude this chapter with applications of Hasse's theorem to find the order of points on E and ultimately methods to calculate the order of $E(K)$.

3.1 Introduction

We begin with some examples of elliptic curves over various finite fields. All the results from Chapter 1 still hold, however, all calculations are performed over a finite field K.

Example 3.1.1. Let E be an elliptic curve defined by $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. One way to determine the order of $E(\mathbb{F}_5)$ is to list all possible values of $x \in \mathbb{F}_5$, then calculate $x^3 + x + 1 \pmod 5$. Finally, we find the square roots of $x^3 + x + 1$ over $\mathbb{F}_5$, which gives points on $E(\mathbb{F}_5)$ as shown in Table 3.1.

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

Table 3.1: Points on $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

Therefore, we have that $\#E(\mathbb{F}_5) = 9$. To add points on an elliptic curve, we use the formulas given in Theorem 1.2.1.

Thus, to add $(3,1) + (2,4)$ on $E(\mathbb{F}_5)$ we compute the slope of the line through the two points as

$$m = \frac{4-1}{2-3} \equiv \frac{3}{-1} \equiv \frac{8}{4} \equiv 2 \pmod 5. \tag{3.1}$$

Hence, the line through the two points is given by $y = 2(x-3)+1 \equiv 2x \pmod 5$. So by substitution we get that

$$4x^2 = x^3 + x + 1 \implies x^3 - 4x^2 + x + 1. \tag{3.2}$$

The sum of the roots is 4 so that the remaining root is $x = 4$ and $y = 3$. Now by reflecting across the x-axis we obtain the sum

$$(3,1) + (2,4) = (4,2). \tag{3.3}$$

Example 3.1.2. Let E be an elliptic curve defined by $y^2 = x^3 + 2$ over $\mathbb{F}_7$. Then a similar argument as in the previous example yields that

$$E(\mathbb{F}_7) = \{\infty, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}. \tag{3.4}$$

Note that all points on $P \in E(\mathbb{F}_7)$ satisfy $3P = \infty$, so that the $E(\mathbb{F}_7) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Two main restrictions on the groups $E(\mathbb{F}_q)$ are given in the next two results.

Theorem 3.1.3. *Let E be an elliptic curve over the finite field $E(\mathbb{F}_q)$, then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \tag{3.5}$$

for some $n \geq 1$, or

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \tag{3.6}$$

for some integers $n_1, n_2 \geq 1$ such that $n_1 | n_2$.

Proof. Recall from group theory that a finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_r}, \tag{3.7}$$

with $n_i | n_{i+1}$ for $i \geq 1$. Since, for each i, the group $\mathbb{Z}_{n_i}$ has n_1 elements of order dividing n_1, we find that $E(\mathbb{F}_q)$ has n_1^r elements of order dividing n_1. Thus, by Theorem 2.1.3, there are at most n_1^2 such points. Therefore, $r \leq 2$ and we obtain the result. □

Theorem 3.1.4 (Hasse)**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$, then*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}. \tag{3.8}$$

The theorem will be proved in Section 3.2. Now we turn our attention to the groups that can actually occur as groups $E(\mathbb{F}_q)$. The answer is given in the following two results, which are proved in [2] and [8], respectively.

Theorem 3.1.5. *Let $q = p^n$ be a power of a prime number p and let $N = q + 1 - a$. There is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and a satisfies one of the following:*

(1) $\gcd(a, p) = 1$

(2) *n is even and* $a = \pm 2\sqrt{q}$

(3) *n is even,* $p \not\equiv 1 \pmod 3$*, and* $a = \pm\sqrt{q}$

(4) *n is odd,* $p = 2$ *or* $p = 3$*, and* $a = \pm p^{(n+1)/2}$

(5) *n is even,* $p \not\equiv 1 \pmod 4$*, and* $a = 0$

(6) *n is odd and* $a = 0$.

Theorem 3.1.6. *Let N be an integer that occurs as the order of an elliptic curve over a finite field $\mathbb{F}_q$, as in Theorem 3.1.5. Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 | n_2$. There is an elliptic curve E over $\mathbb{F}_q$ such that*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \tag{3.9}$$

if and only if

(1) *$n_1 | (q-1)$ in (1), (3), (4), (5), and (6) of Theorem 3.1.5.*

(2) *$n_1 = n_2$ in (2) of Theorem 3.1.5.*

These are the only groups that occur as groups $E(\mathbb{F}_q)$.

3.2 The Frobenius Endorphism

Let $\mathbb{F}_q$ be a finite field with algebraic closure $\overline{\mathbb{F}_q}$ and let

$$\varphi_q : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q} \tag{3.10}$$

given by $x \mapsto x^q$ be the Frobenius map for $\mathbb{F}_q$.

Let E be an elliptic curve defined over $\mathbb{F}_q$, then φ_q acts on the coordinates of points in $E(\overline{\mathbb{F}_q})$ by $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi_q(\infty) = \infty$.

Lemma 3.2.1. *Let E be defined over $\mathbb{F}_q$ and let $(x, y) \in E(\mathbb{F}_q)$.*

(1) $\varphi_q(x, y) = (x^q, y^q) \in E(\overline{\mathbb{F}_q})$

(2) $(x, y) \in E(\mathbb{F}_q)$ *if and only if* $\varphi_q(x, y) = (x, y)$

Proof. Since the proofs are the same for the Weierstrauss and the generalized Weierstrauss equations, we work with the general form. We have

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.11}$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$. Now by raising each to the qth power to obtain

$$(y^q)^2 + a_1(x^qy^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6. \tag{3.12}$$

Note this shows that $(x^q, y^q) \in E(\overline{\mathbb{F}_q})$.

To show (2), recall that $x \in \mathbb{F}_q$ if and only if $\varphi_q(x) = x$ and similarly for $y \in \mathbb{F}_q$. Therefore, we find that

$$\begin{aligned}(x, y) \in E(\mathbb{F}_q) &\iff x, y \in \mathbb{F}_q \iff \varphi_q(x) = x \text{ and } \varphi_q(y) = y \\ &\iff \varphi_q(x, y) = (x, y).\end{aligned} \tag{3.13}$$

Hence, we have shown (1) and (2), so we obtain the result. □

The following result is crucial to counting points on an elliptic curve over finite fields. Since φ_q is an endomorphism, then so it $\varphi_q^n = \varphi_q \circ \varphi_q \circ \cdots \circ \varphi_q$ for every $n \geq 1$. Since multiplication by (-1) is also an endorphism, then $\varphi_q^n - 1$ is an endorphism of E.

Proposition 3.2.2. *Let E be defined over $\mathbb{F}_q$ and let $n \geq 1$, then*

(1) $\mathrm{Ker}(\varphi_q^n - 1) = E(\mathbb{F}_{q^n})$

(2) $\varphi_q^n - 1$ *is a separable endomorphism, so* $\#E(\mathbb{F}_{q^n}) = \deg(\varphi_q^n - 1)$.

Proof. Since φ_q^n is the Frobenius map for hte field $\mathbb{F}_{q^n}$, then (1) is a restatement of Lemma 3.2.1. The fact that φ_q^n is separable is due to $q \nmid (-1)$. Therefore, (2) follows from Proposition 1.5.1. □

We need one more result before we are ready to prove Hasse's theorem. In preparation for the next result, let

$$a = q + 1 - \#E(\mathbb{F}_q) = q - 1 - \deg(\varphi_q - 1). \tag{3.14}$$

Lemma 3.2.3. *Let $r, s \in \mathbb{Z}$ with $\gcd(s, q) = 1$, then $\deg(r\varphi_q - s) = r^2q + s^2 - rsa$.*

Proof. Note that Proposition 2.2.4 and (3.14) implies that

$$\begin{aligned}
\deg(r\varphi_q - s) &= r^2 \deg(\varphi_q) + s^2 \deg(-1) + rs((\deg(\varphi_q - 1)) - \deg(\varphi) - \deg(-1)) \\
&= r^2q + s^2 + rs(\deg(\varphi_q - 1) - q - 1) \\
&= r^2q + s^2 + rs(\deg((q + 1 - a) - q - 1)) \qquad (3.15) \\
&= r^2q + s^2 + rsa.
\end{aligned}$$

Note that we did not need the assumption that $\gcd(s, q) = 1$. □

Proof of Theorem 3.1.4. We want to show from (3.14) that $|a| \leq 2\sqrt{q}$. Since $\deg(r\varphi_q - s) \geq 0$, Lemma 4.2.3 implies that

$$r^2q + s^2 - rsa = \frac{qr^2}{s^2} - \frac{rsa}{s^2} + 1 = q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0 \tag{3.16}$$

for all $r, s \in \mathbb{Z}$ with $\gcd(s, q) = 1$. The set

$$\left\{\frac{r}{s} \mid \gcd(s, q) = 1\right\} \subset \mathbb{Q} \tag{3.17}$$

is dense in $\mathbb{R}$. Therefore, $qx^2 - ax + 1 \geq 0$, for all $x \in \mathbb{R}$ and the discriminant is negative or zero, which means that

$$a^2 - 4q \leq 0 \implies |a| \leq 2\sqrt{q}. \tag{3.18}$$

This proves Hasse's theorem and gives bounds for the group of points on an elliptic curve over a finite field. □

3.3 Applications of Hasse's Theorem

Now that we have established Hasse's theorem, we have only found bounds for the order of the group of points on an elliptic curve over a finite field. In this section we provide three methods for actually determining the order of the group.

Suppose that we have an elliptic curve E defined over a finite field $\mathbb{F}_q$ and we want to know $\#E(\mathbb{F}_{q^n})$ for some n. We can determine $\#E(\mathbb{F}_{q^n})$ when $n = 1$ by listing the elements, which allows us to determine $\#E(\mathbb{F}_{q^n})$ for some n as the following theorem illustrates.

Theorem 3.3.1. *Let $\#E(\mathbb{F}_q) = q + 1 - a$. Write $x^2 - ax + q = (x - \alpha)(x - \beta)$, then*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) \tag{3.19}$$

for all $n \geq 1$.

Proof. First, recall that $\alpha^n + \beta^n$ is an algebraic integer and a rational number,

so that $\alpha^n + \beta^n$ is an integer. Now let

$$\begin{aligned} f(x) &= (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha x)^n - (\beta x)^n + (\alpha\beta)^n \\ &= x^{2n} - (\alpha^n + \beta^n)x + (\alpha\beta)^n \\ &= x^{2n} - (\alpha^n + \beta^n)x + q^n. \end{aligned} \tag{3.20}$$

Then, $x^2 - ax + q = (x - \alpha)(x - \beta)|f(x)$. Therefore, it follows from the division algorithm that the quotient $g(x) \in \mathbb{Z}[x]$. Thus,

$$(\varphi_q^n)^2 - (\alpha^n + \beta^n)\varphi_q^n + q^n = f(\varphi_q) = g(\varphi_q)(\varphi_q^2 - a\varphi_q + q) = 0 \tag{3.21}$$

as endorphisms of E. Note that $\varphi_q^n = \varphi_{q^n}$, so there is only one integer k such that $\varphi_{q^n}^2 - k\varphi_{q^n} + q^n = 0$ and such k is determined by $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$. Thus,

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}). \tag{3.22}$$

This completes the proof of Theorem 3.3.1. □

In the previous section, to make a list of points on $y^2 = x^3 + ax + b$ over a finite field, we tried each possible value of x, then found the square roots y of $x^3 + ax + b$ if they existed. This method is the foundation for a simple point counting algorithm.

Recall the Legendre symbol $\left(\frac{x}{p}\right)$ for an odd prime p is defined as follows:

$$\left(\frac{x}{p}\right) = \begin{cases} +1 \text{ if } t^2 \equiv x \pmod{p} \text{ has a solution } t \not\equiv 0 \pmod{p}, \\ -1 \text{ if } t^2 \equiv x \pmod{p} \text{ has no solution } t, \\ \ \ 0 \text{ if } x \equiv 0 \pmod{p}. \end{cases} \tag{3.23}$$

This idea can be generalized to any finite field $\mathbb{F}_q$ with q an odd prime by defining

for $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 \text{ if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^\times, \\ -1 \text{ if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q, \\ \ \ 0 \text{ if } x = 0. \end{cases} \tag{3.24}$$

Theorem 3.3.2. *Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, then we have that*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right). \tag{3.25}$$

Proof. For a given x_0 there are two points (x, y) with x-coordinate x_0 if $x_0^3 + ax_0 + b$ is a nonzero square in $\mathbb{F}_q$, one point if it is zero, and no points if it is not a square.

Therefore, the number of points with x-coordinate x_0 equals $1 + \left(\frac{x_0^3 + ax_0 + b}{\mathbb{F}_q}\right)$. Summing over all $x_0 \in \mathbb{F}_q$ and including 1 for the point ∞ gives

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right)\right) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{\mathbb{F}_q}\right). \tag{3.26}$$

This completes the proof of Theorem 3.3.2. □

Example 3.3.3. Let E be the elliptic curve defined by $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. The nonzero squares modulo 5 are 1 and 4. Therefore,

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x \in \mathbb{F}_5} \left(\frac{x^3 + x + 1}{\mathbb{F}_5}\right) = 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5}\right) \\ &= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{11}{5}\right) + \left(\frac{31}{5}\right) + \left(\frac{69}{5}\right) \\ &= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) \\ &= 6 + 1 - 1 + 1 + 1 + 1 = 9. \end{aligned} \tag{3.27}$$

Theorem 3.3.2 is sometimes referred to as the Lang-Trotter method, which works quickly for small values of q, that is for $q < 100$, but is slow for larger values of q and is impossible to use when q is around 10^{100} or larger.

Another useful technique to find the order of the group is to determine the order of points on an elliptic curve along with Hasse's theorem to narrow the search for the order of the group. Thus, let $P \in E(\mathbb{F}_q)$ then the order of P is the smallest positive integer k such that $kP = \infty$. By Lagrange's theorem, the order of P always divides the order of the group $E(\mathbb{F}_q)$. Furthermore, recall that if $nP = \infty$ for $n \in \mathbb{Z}$ if and only if the order of P divides n.

By Hasse's theorem, the order of $E(\mathbb{F}_q)$ lies in an interval of length $4\sqrt{q}$. Therefore, if we find that a point that has order greater than $4\sqrt{q}$, then there can only be one multiple of the order of the point smaller than $4\sqrt{q}$ and must be $\#E(\mathbb{F}_q)$. In addition, using a few more points often shortens the list enough that there is a unique possibility for $\#E(\mathbb{F}_q)$.

Example 3.3.4. Let E be the elliptic curve $y^2 = x^3 + 7x + 12$ over $\mathbb{F}_{103}$. It is possible to see that $(-1, 2)$ has order 13 and the point $(19, 0)$ has order 2, so that $N_{103} = \#E(\mathbb{F}_{103})$ is a multiple of 26. Hasse's theorem implies that

$$103 + 1 - 2\sqrt{103} \leq N_{103} \leq 103 + 1 + 2\sqrt{103} \implies 84 \leq N_{103} \leq 124. \tag{3.28}$$

The only multiple of 26 in this interval is 104, so $N_{103} = \#E(\mathbb{F}_{103}) = 104$.

Example 3.3.5. Let E be the elliptic curve $y^2 = x^3 + 2$ over $\mathbb{F}_7$ as in Example 4.1.2. We have already observed that $E(\mathbb{F}_7) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$, since every point except ∞ has order 3. Thus, we can only conclude that $N_7 = \#E(\mathbb{F}_7)$ is a multiple of 3 and by Hasse's theorem get that $3 \leq N_7 \leq 13$. This leaves 3, 6, 9, and 12 as possibilities.

If we can find two points of order 3 that are not multiples of one another, then

they generate a subgroup of order 9. This means that the order of the group is a multiple of 9, so that $N_7 = 9$.

The situation where $E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ as in the previous example makes it more difficult to find $\#E(\mathbb{F}_q)$, but due to the next result, this situation is rare.

Proposition 3.3.6. *Let E be an elliptic curve over $\mathbb{F}_q$ and suppose that*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n \tag{3.29}$$

for some $n \in \mathbb{Z}$. Then either $q = n^2 + 1$ or $q = n^2 \pm n + 1$, or $q = (n \pm 1)^2$.

Proof. By Hasse's theorem, $n^2 = q + 1 - a$ with $|a| \leq 2\sqrt{q}$. Thus to prove the statement, we need the following lemma that places a restriction on a. □

Lemma 3.3.7. $a \equiv 2 \pmod{n}$.

Proof. Let $\mathrm{char}(\mathbb{F}_q) = p$, then $p \nmid n$. Since, if $p|n$ then there would be p^2 in $E[p]$, which is impossible in characteristic p by Theorem 2.1.3.

Since $E[n] \subset E(\mathbb{F}_q)$, then the nth roots of unity are in $\mathbb{F}_q$, so $q - 1$ must be a multiple of n. Hence, $a = q + 1 - n^2 \equiv 2 \pmod{n}$. □

Proof of Proposition 3.3.6. Write $a = kn + 2$ for some $k \in \mathbb{Z}$. Then

$$n^2 = q + 1 - a = q + 1 - kn, \quad \text{so} \quad q = n^2 + kn + 1. \tag{3.30}$$

By Hasse's theorem, $|kn + 2| \leq 2\sqrt{q}$. By squaring this inequality, we get that

$$k^2n^2 + 4kn + 4 \leq 4q = 4(n^2 + kn + 1). \tag{3.31}$$

Therefore, $|k| \leq 2$. The possibilities $k = 0, \pm 1, \pm 2$ gives the values of q listed in the proposition. □

In fact, most q are such that all elliptic curves over $\mathbb{F}_q$ have points of order greater than $4\sqrt{q}$. Therefore, we can usually find points with orders that allow us to determine $\#E(\mathbb{F}_q)$.

3.4 Schoof's Algorithm

In 1985, Schoof [3] published an algorithm for computing the number of points on an elliptic curve over finite fields $\mathbb{F}_q$ that runs much faster than existing algorithms, at least for very large q. In fact, Schoof's algorithm requires at most a constant times $\log^8(q)$ bit operations. Recently, Atkin and Elkies [1] refined and improved Schoof's method. It has been successfully used when q has several hundred decimal digits.

In order to describe Schoof's algorithm, we first need to define division polynomials that may be generalized for an elliptic curve over any field K, not necessarily finite. Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$, where $a, b \in K$. Then we define the division polynomials $\psi_m \in \mathbb{Z}[x, y, a, b]$ by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \qquad (3.32) \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3.
\end{aligned}$$

Therefore, Schoof's algorithm is given as follows:

Suppose that E is an elliptic curve of the form (1.1) over $\mathbb{F}_q$. By Hasse's theorem, $\#E(\mathbb{F}_q) = q + 1 - a$, where $|a| \leq 2\sqrt{q}$. We want to compute $\#E(\mathbb{F}_q) = q + 1 - a$.

(1) Choose a set of primes $S = \{2, 3, 5, 7, 11, \ldots, L\}$, with $p \notin S$ such that

$$\prod_{\ell \in S} \ell > 4\sqrt{q}. \tag{3.33}$$

(2) If $\ell \neq 2$, we have $a \equiv 0 \pmod 2$ if and only if $\gcd(x^q - x, x^3 + ax + b) \neq 1$.

(3) For each odd prime $\ell \in S$, perform the following:

(a) Let $q_\ell \equiv q \pmod \ell$ with $|q_\ell| < \ell/2$.

(b) Compute the x-coordinate x' of

$$(x', y') = ((x^{q^2}, y^{q^2}) + q_\ell(x, y)) \pmod{\psi_\ell}. \tag{3.34}$$

(c) For $j = 1, 2, 3, \ldots, (\ell - 1)/2$ do the following:

(i) Compute the x-coordinate x_j of $(x_j, y_j) = j(x, y)$.

(ii) If $(x' - x_j^q) \equiv 0 \pmod{\psi_\ell}$, go to step (iii). If not, try the next value of j. If all values $1 \leq j \leq (\ell - 1)/2$ have been tried, go to step (d).

(iii) Compute y' and y_j. If $(y' - y_j)/y \equiv 0 \pmod{\psi_\ell}$, then $a \equiv j \pmod \ell$. If not, then $a \equiv -j \pmod \ell$.

(d) If all values $1 \leq j \leq (\ell - 1)/2$ have been tried without success, let $w^2 \equiv q \pmod \ell$. If w does not exist, then $a \equiv 0 \pmod \ell$.

(e) If $\gcd(\text{numerator}(x^q - x_w), \psi_\ell) = 1$, then $a \equiv 0 \pmod \ell$. Otherwise, compute

$$\gcd(\text{numerator}((y^q - y_w)/y), \psi_\ell). \tag{3.35}$$

If $\gcd(\text{numerator}(x^q - x_w), \psi_\ell) \neq 1$, then $a \equiv 2w \pmod{\ell}$. Otherwise, $a \equiv -2w \pmod{\ell}$.

(4) Use the knowledge of $a \pmod{\ell}$ for each $\ell \in S$ to compute $a \pmod{\prod_{\ell \in S} \ell}$. Choose the value of a that satisfies the congruences and is such that $|a| \leq 2\sqrt{q}$.

Therefore, we have an algorithm to determine the order of the group $E(\mathbb{F}_q)$ for very large values of q. Moreover, $\#E(\mathbb{F}_q) = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

3.5 Supersingular Curves

Recall that an elliptic curve E over a field of K such that $\text{char}(K) = p$ is called supersingular if $E[p] = \{\infty\}$. In other words, there are no points of order p. Note that supersingular curves are not to be confused with singular curves. The following results are useful in that it gives a simple criterion for determining whether or not an elliptic curve over a finite field is supersingular.

Lemma 3.5.1. *Let E be an elliptic curve over $\mathbb{F}_q$. Let $a = q + 1 - \#E(\mathbb{F}_q)$ and write $x^2 - ax + q = (x - \alpha)(x - \beta)$ as in Theorem 3.3.1. Let $s_n = \alpha^n + \beta^n$, then*

$$s_0 = 2, s_1 = a, \text{ and } s_{n+1} = as_n - qs_{n-1} \tag{3.36}$$

for all $n \geq 1$.

Proof. Notice that by multiplying the relation $\alpha^2 - a\alpha + q = 0$ by α^{n-1} we obtain $a^{n+1} = a\alpha^n - q\alpha^{n-1}$. Similarly there is an expression for β. Add the two expressions together to obtain the result. □

Proposition 3.5.2. *Let E be an elliptic curve over $\mathbb{F}_q$ where $q = p^n$ for some $n \geq 1$. Let $a = q+1-\#E(\mathbb{F}_q)$, then E is supersingular if and only if $a \equiv 0 \pmod{p}$, which is if and only if $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$.*

Proof. Write $x^2 - ax + q = (x - \alpha)(x - \beta)$. Theorem 3.3.1 implies that

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n). \tag{3.37}$$

Lemma 3.5.1 now gives that $s_n = \alpha^n + \beta^n$ satisfies the recurrence relation (3.36). Suppose that $a \equiv 0 \pmod{p}$, then $s_1 = a \equiv 0 \pmod{p}$, and $s_{n+1} \equiv 0 \pmod{p}$ for all $n \geq 1$. Thus,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p}, \tag{3.38}$$

so there are no points of order p in $E(\mathbb{F}_{q^n})$ for any $n \geq 1$. Since

$$\overline{\mathbb{F}}_{q^n} = \cup_{n \geq 1} \mathbb{F}_{q^n}, \tag{3.39}$$

there are no points of order p in $E(\overline{\mathbb{F}_q})$ so that E is supersingular.

On the other hand, suppose that $a \not\equiv 0 \pmod{p}$, then (3.33) implies that $s_{n+1} \equiv a s_n \pmod{p}$ for $n \geq 1$. Since $s_1 = a$ we have that $s_n \equiv a^n \pmod{p}$ for all $n \geq 1$. Thus,

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv (1 - a^n) \pmod{p}. \tag{3.40}$$

By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ so that $\#E(\mathbb{F}_{q^{p-1}})$ is divisible by p. Hence, $E(\mathbb{F}_{q^{p-1}})$ contains a point of order p, which implies that E is not supersingular.

For the last statement of the proposition, notice that

$$\#E(\mathbb{F}_q) \equiv q + 1 - a \equiv (1 - a) \pmod{p}, \tag{3.41}$$

so that $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$. □

Corollary 3.5.3. *Suppose that $p \geq 5$ is prime, then E is supersingular if and only if $a = 0$, which is the case if and only if $\#E(\mathbb{F}_p) = p + 1$.*

Proof. If $a = 0$ then E is supersingular by Proposition 3.5.2. Conversely, suppose that E is supersingular but $a \neq 0$, then $a \equiv 0 \pmod{p}$ and that $|a| \geq p$. By Hasse's theorem, $|a| \leq 2\sqrt{p}$ so we have $p \leq 2\sqrt{p}$. This only occurs when $p \leq 4$. □

In Section 2.1, it was shown that the elliptic curve $y^2 + a_3y = x^3 + a_4x + a_6$ over a field K with $\mathrm{char}(K) = 2$ is supersingular. Furthermore, over a field K of $\mathrm{char}(K) = 3$, the curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is supersingular if and only if $a_2 = 0$. The following result gives a way to construct supersingular curves in many other characteristics, which will be implemented in Section 5.5.

Proposition 3.5.4. *Suppose that q is odd and $q \equiv 2 \pmod{3}$. Let $b \in \mathbb{F}_q^\times$, then the elliptic curve E given by $y^2 = x^3 + b$ is supersingular.*

Proof. Let $\psi : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$ be the homomorphism given by $\psi(x) = x^3$. Since $q - 1$ is not a multiple of 3, there are no elements of order 3 in $\mathbb{F}_q^\times$. Thus, we have that $\mathrm{Ker}(\psi) = \{\infty\}$ and ψ is injective and must be surjective, since it is map from a finite group to itself. In particular, every element of $\mathbb{F}_q$ has a unique cube root in $\mathbb{F}_q$.

For each $y \in \mathbb{F}_q$ there is exactly one $x \in \mathbb{F}_q$ such that (x, y) lies on the curve, so x is a unique cube root of $y^2 - b$. Since there are q distinct y-values, we obtain q points. Therefore, including the point ∞ we obtain $\#E(\mathbb{F}_q) = q + 1$ and E is supersingular. □

Chapter 4

The Discrete Logarithm Problem

Let G be any group, written multplicatively for the moment, and let $a, b \in G$. Suppose that we know that there exists some $k \in \mathbb{Z}$ such that $a^k = b$. The discrete logarithm problem is to find k. For example, G could be the multiplicative group $\mathbb{F}_q^\times$ of a finite field. Similarly, G could be the group $E(\mathbb{F}_q)$ for some elliptic curve E, in which case a and b are points on E and we are trying to solve the problem $ka = b$.

In the next chapter we will be concerned with implementation of the discrete logarithm problem in cryptography and the security of which will depend on the difficulty of solving the discrete logarithm problem. One possible attack is brute force, however, this approach is impractical whenever $k \in \mathbb{Z}$ is several hundred digits. In this chapter we discuss one possible attack, called the index calculus, that can be used in $\mathbb{F}_p^\times$, and more generally in the multiplicative group of a finite field. We then discuss the Baby Step, Giant Step method, and Pollard's ρ method. These methods all work for general finite groups, specifically for elliptic curves.

4.1 The Index Calculus

Let p be prime and let g be a primitive root modulo p, this means that g is a generator for the cyclic group $\mathbb{F}_p^\times$. In other words, every $h \not\equiv 0 \pmod{p}$ can be written in the form

$$h \equiv g^k \text{ for some } k \in \mathbb{Z} \tag{4.1}$$

and is uniquely determined modulo $p-1$.

Let $k = L(h)$ denote the discrete logarithm of h with respect to g and p so

$$g^{L(h)} \equiv h \pmod{p}. \tag{4.2}$$

Suppose that h_1 and h_2 satisfy

$$g^{L(h_1 h_2)} \equiv h_1 h_2 \equiv g^{L(h_1)} g^{L(h_2)} \equiv g^{L(h_1)+L(h_2)} \pmod{p}. \tag{4.3}$$

This implies that $L(h_1 h_2) \equiv (L(h_1) + L(h_2)) \pmod{(p-1)}$. Thus, L changes multiplication into addition.

Definition 4.1.1. *The index calculus is a method for computing values of the discrete log function L. The idea to compute $L(\ell)$ for several primes ℓ, then use this information to compute $L(h)$ for arbitrary h.*

Example 4.1.2. Let $p = 1217$ and $q = 3$, so that we want to solve $3^k \equiv 37 \pmod{1217}$. We first choose a set of small primes called the factor base, to be $B = \{2, 3, 5, 7, 11, 13\}$. Next we find relations of the form

$3^x \equiv \pm$(product of primes in B)(mod 1217). Eventually we find

$$\begin{aligned} 3^1 &\equiv 3 \pmod{1217} \\ 3^{24} &\equiv 2^2 \cdot 7 \cdot 13 \pmod{1217} \\ 3^{25} &\equiv 5^3 \pmod{1217} \\ 3^{30} &\equiv -2 \cdot 5^2 \pmod{1217} \\ 3^{54} &\equiv -5 \cdot 11 \pmod{1217} \\ 3^{87} &\equiv 13 \pmod{1217} \end{aligned} \tag{4.4}$$

These computations can be changed into equations for discrete logs where now all congruences are modulo $p - 1 = 1216$. Note that we already know that

$$3^{(p-1)/2} \equiv -1 \pmod{p} \tag{4.5}$$

so that $L(-1) = 608$.

$$\begin{aligned} 1 &\equiv L(3) \pmod{1216} \\ 24 &\equiv (L(-1) + 2L(2) + L(7) + L(13)) \pmod{1216} \\ 25 &\equiv 3L(5) \pmod{1216} \\ 30 &\equiv (L(-1) + L(2) + 2L(5)) \pmod{1216} \\ 54 &\equiv (L(-1) + L(5) + L(11)) \pmod{1216} \\ 87 &\equiv L(13) \pmod{1216}. \end{aligned} \tag{4.6}$$

Note that the first equation implies that $L(3) \equiv 1$. Similarly,

$$\begin{aligned} 3L(5) \equiv 25 \pmod{1216} &\implies L(5) \equiv (3^{-1} \cdot 25) \pmod{1216} \\ &\implies L(5) \equiv (811 \cdot 25) \pmod{1216} \\ &\implies L(5) \equiv 819 \pmod{1216}. \end{aligned} \tag{4.7}$$

The fourth equation gives that

$$\begin{aligned} L(2) &\equiv 30 - 608 - 2L(5) \equiv 30 + 608 - 2(819) \\ &\equiv -1000 \pmod{1216} \equiv 216 \pmod{1216}. \end{aligned} \tag{4.8}$$

The fifth equation yields

$$L(11) \equiv (54 + 608 - L(5)) \equiv (662 - 819) \equiv -157 \equiv 1059 \pmod{1216}. \tag{4.9}$$

Thus, the second equation now yields the following:

$$L(7) \equiv (24+608-2L(2)-L(13)) \equiv (632-2(216)-87) \equiv 113 \pmod{1216}. \tag{4.10}$$

Now we know the discrete logs of each element in our factor base B. Recall that we want to solve $3^k \equiv 37 \pmod{1217}$. We compute $3^j \cdot 37 \pmod{1217}$ for several random j until we obtain

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}. \tag{4.11}$$

which is the first appearance of only factors in B. Therefore,

$$L(37) \equiv (3L(2) + L(7) + L(11) - 16) \equiv 588 \pmod{1217} \tag{4.12}$$

and in fact $3^{588} \equiv 37 \pmod{1217}$.

The choice of the factor base is extremely important. If B is chosen too small, then the computations become harder. On the other hand, if B is too large the computations become easier. An example that was completed in 2001 by Joux and Lercier used the first one million primes to compute discrete logs modulo a 120-digit prime.

4.2 Attacks on Discrete Logs

In the following, we discuss general attacks that work for arbitrary groups. Since our main motivation is for elliptic curves, we write our group G additively. Therefore, we are given $P, Q \in G$ and we are trying to solve $kP = Q$. Let $|G| = n$ be the order of G.

4.2.1 Baby Step, Giant Step

The first attack on the discrete logarithm problem that we will discuss was developed by Shanks [4] and requires approximatley $\sqrt{n}$ steps and around $\sqrt{n}$ storage, so that the algorithm works well for moderately sized n. Shanks' algorithm, now called the Baby Step, Giant Step algorithm, is as follows:

(1) Fix an integer $m \geq \sqrt{n}$ and compute mP.

(2) Make and store a list of iP for $0 \leq i \leq m$.

(3) Compute the points $Q - jmP$ for $j = 0, 1, \ldots, m-1$ until one matches a point from the stored list.

(4) If $iP = Q - jmP$, then $Q = kP$ with $k \equiv (i + jm) (\text{mod } n)$. Therefore, $Q = iP + jmP = (i + jm)P = kP$.

This algorithm works since if we fix an integer $m \geq \sqrt{n}$, then $m^2 \geq n$ so we may assume that the solution k is such that $0 \leq k < m^2$. Now write $k = k_0 + mk$ where $k_0 \equiv k \pmod{m}$ and $0 \leq k_0 < m$ and let $k_1 = (k - k_0)/m$.

Then, $0 \leq k_1 < m$ when $i = k_0$ and $j = k_1$ we have that

$$Q - jmP = Q - k_1 mP = kP - k_1 mP = (k - k_1 m)P = k_0 P, \tag{4.13}$$

so there is a match.

Note that we did not need to know $n = |G|$, only an upper bound. Therefore, for elliptic curves over $\mathbb{F}_q$, we could use this method with $m^2 \geq q + 1 + 2\sqrt{q}$, by Hasse's theorem.

Example 4.2.1. Let $G = E(\mathbb{F}_{41})$, where E is given by $y^2 = x^3 + 2x + 1$. Let $P = (0, 1)$ and $Q = (30, 40)$. By Hasse's theorem, we know that

$$|41 + 1 - \#E(\mathbb{F}_{41})| \leq 2\sqrt{41} \implies 29.194 \leq \#E(\mathbb{F}_{41}) \leq 54.806, \tag{4.14}$$

so that $n = |G| \leq 54$. Thus, we let $m = 8$ since $m \geq \sqrt{54}$. The points iP for $1 \leq i \leq 7$ are

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9). \tag{4.15}$$

When we calculate $Q - jmP$ for $j = 0, 1, 2$, we obtain

$$(30, 40), (9, 25), (26, 9), \tag{4.16}$$

at which we have arrived at a match. Since $j = 2$ gave the match with $7P$, we have

$$Q = (30, 40) = 7P + 16P = 23P. \tag{4.17}$$

4.2.2 Pollard's ρ Method

The major disadvantage of the Baby Step, Giant Step algorithm is that it requires a lot of storage. Pollard's ρ method runs in approximately the same time as Baby Step, Giant Step, but requires very little storage.

Let G be a finite group such that $|G| = n$. Choose a function $f : G \longrightarrow G$ that behaves randomly. We start with a point P_0 and compute iterations, $P_{i+1} = f(P_i)$. Since $|G| = n$, there will be some indices $i_0 < j_0$ such that $P_{i_0} = P_{j_0}$. Then,

$$P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1} \tag{4.18}$$

and similarly, $P_{i_0+\ell} = P_{j_0+\ell}$ for all $\ell \geq 0$. Therefore, $\{P_i\}_{i\in\mathbb{N}}$ is periodic with period $j_0 - i_0$ or possibly a divisor of $j_0 - i_0$. The figure describing this process is given in Figure 4.1 looks like the Greek letter ρ, which is why it is called Pollard's ρ method. If f is a randomly chosen random function, then we expect to find a match with j_0 at most a constant times $\sqrt{n}$.

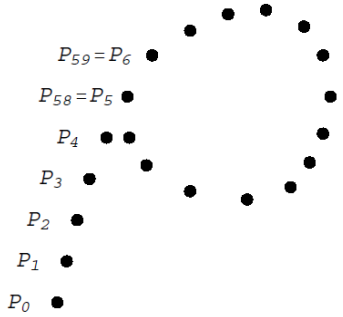


Figure 4.1: Pollard's ρ Method

One implementation of the method stores all the points P_i until a match is found. This takes around $\sqrt{n}$ storage, which is similar to Baby Step, Giant Step. However, it is possible to do much better at the expense of a little more computation. The idea is once there is a match for two indices that differ by d, all subsequent indices that differ by d will also be matches. Therefore, we can compute pairs (P_i, P_{2i}) for $i = 1, 2, 3, \ldots$ but we only keep the current pair. We will not store the previous pairs

$$P_{i+1} = f(P_i) \quad \text{and} \quad P_{2(i+1)} = f(f(P_{2i})). \tag{4.19}$$

Suppose that $i \geq i_0$ and i is a multiple of d, then $2i$ and i differ by a multiple of d. Hence, we have a match $P_i = P_{2i}$. Since $d \leq j_0$ and $i_0 < j_0$, there is a match for $i \leq j_0$. Thus, the number of steps to find a match is expected to be at most a constant multiple of $\sqrt{n}$.

The problem remains how to choose a suitable function f. One way to do this is to divide G into s disjoint subsets $S_1, S_2, \ldots, S_s$ of approximately the same size. Choose $2s$ random integers $a_i, b_i \pmod{n}$. Let

$$M_i = a_i P + b_i Q. \tag{4.20}$$

Finally, define

$$f(g) = g + M_i \quad \text{if } g \in S_i. \tag{4.21}$$

Now choose random integers a_0, b_0 and let $P_0 = a_0 P + b_0 Q$ be the starting point. While computing P_j we also record how these points are expressed in terms of P and Q.

If $P_j = u_j P + v_j Q$ and $P_{j+1} = P_j + M_i$, then

$$P_{j+1} = u_j P + v_j Q + a_i P + b_i Q = (u_j + a_i)P + (v_j + b_i)Q \tag{4.22}$$

so $(u_{j+1}, v_{j+1}) = (u_j + v_j) + (a_i, b_i)$. When we first find a match $P_{i_0} = P_{j_0}$, then

$$u_{j_0} P + v_{j_0} Q = u_{i_0} P + v_{i_0} Q \implies (u_{i_0} - u_{j_0})P = (v_{j_0} - v_{i_0})Q. \tag{4.23}$$

If $\gcd(v_{j_0} - v_{i_0}, n) = d$, then

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \pmod{n/d}. \tag{4.24}$$

This gives d choices for k. Typically, d will be small so we can try all possibilities until $Q = kP$.

Example 4.2.2. Let $G = E(\mathbb{F}_{1093})$ where E is the elliptic curve $y^2 = x^3 + x + 1$. We will use $s = 3$. Let $P = (0.1)$ and $Q = (413, 959)$. It can be shown that $|P| = 1067$ and we want to find $k \in \mathbb{Z}$ such that $Q = kP$.

Let $P_0 = 3P + 5Q$, $M_0 = 4P + 3Q$, $M_1 = 9P + 17Q$, and $M_2 = 19P + 6Q$.

Let $f : E(\mathbb{F}_{1093}) \longrightarrow E(\mathbb{F}_{1093})$ be defined by

$$f(x, y) = (x, y) + M_i \quad \text{if } x \equiv i \pmod 3. \tag{4.25}$$

Here x is considered an integer such that $0 \leq x \leq 1093$. We may also define $f(\infty) = \infty$. If we compute P_0, $P_1 = f(P_0)$, $P_2 = f(P_1), \ldots$, we obtain

$$\begin{aligned} &P_0 = (326, 69), P_1 = (727, 589), P_2 = (560, 365), P_3 = (1070, 260), \\ &P_4 = (473, 903), P_5 = (1006, 951), P_6 = (523, 938), \ldots, \\ &P_{57} = (895, 337), P_{58} = (1006, 951), P_{59} = (523, 938), \ldots. \end{aligned} \tag{4.26}$$

Therefore, $P_5 = P_{58}$ and we keep track of the coefficients of P and Q we find

$$P_5 = 88P + 46Q \quad \text{and} \quad P_{58} = 685P + 620Q. \tag{4.27}$$

Thus, $P_{58} - P_5 = 597P + 574Q = \infty$. Since $|P| = 1067$, we calculate

$$-574^{-1}597 \equiv 499 \pmod{1067}. \tag{4.28}$$

Hence, $Q = 499P$ so that $k = 499$.

4.3 Attack with Pairings

One strategy for attacking the discrete logarithm problem is to reduce it to an easier discrete logarithm problem. This can be done using the Weil pairing, which reduces a discrete logarithm problem on an elliptic curve to one in the multiplicative group of a finite field.

The MOV attack, named after Menezes, Okamoto, and Vanstone uses the Weil pairing to convert a discrete logarithm problem in $E(\mathbb{F}_q)$ to one in $\mathbb{F}_{q^m}^{\times}$. In other words, we change the elliptic curve discrete logarithm problem into a discrete logarithm problem. One advantage to this method is that discrete logarithm problems in finite fields can be attacked by index calculus methods, which solves discrete logarithm problems faster than elliptic curve discrete logarithm problems, provided that the field $\mathbb{F}_{q^m}$ is not much larger than $\mathbb{F}_q$.

Let E be an elliptic curve over $\mathbb{F}_q$. Let $P, Q \in E(\mathbb{F}_q)$ and let $n = |P|$. Assume that $\gcd(n, q) = 1$. We need to find $k \in \mathbb{Z}$ such that $Q = kP$. First we check that k actually exists.

Lemma 4.3.1. *There exists $k \in \mathbb{Z}$ such that $Q = kP$ if and only if $nQ = \infty$ and the Weil pairing $e_n(P, Q) = 1$.*

Proof. If $Q = kP$, then $nQ = nkP = k(nP) = \infty$. In addition, we have that

$$e_n(P, Q) = e_n(P, kP) = e_n(P, P)^k = 1^k = 1. \tag{4.29}$$

On the other hand, if $nQ = \infty$ then $Q \in E[n]$. Since $\gcd(n, q) = 1$, then by Theorem 2.1.3, $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Now choose a point R such that $\{P, Q\}$ is a basis for $E[n]$. Then we can write $Q = aP + bR$ for some $a, b \in \mathbb{Z}$. By Corollary 2.2.2, $e_n(P, R) = \zeta$ is a primitive nth root of unity. Therefore, if $e_n(P, Q) = 1$, we have

$$1 = e_n(P, Q) = e_n(P, aP + bR) = e_n(P, P)^a e_n(P, R)^b = 1 \cdot \zeta^b = \zeta^b. \tag{4.30}$$

This implies that $b \equiv 0 \pmod{n}$, so that $bR = \infty$. Thus, $Q = aP$. □

The MOV attack on the elliptic curve discrete logarithm problem is as follows: Choose m such that $E[n] \subset E(\mathbb{F}_{q^m})$. Since all the points of $E[n]$ have coordinates in $\overline{F}_q = \cup_{j \geq 1} \mathbb{F}_{q^j}$, such an m exists. Note that the group of nth roots of unity, μ_n, is contained in $\mathbb{F}_{q^m}$. All of the following calculations are performed in $\mathbb{F}_{q^m}$.

(1) Choose a random point $T \in E(\mathbb{F}_{q^m})$.

(2) Compute the order of T, $|T| = M$.

(3) Let $d = \gcd(n, M)$ and let $T_1 = (M/d)T$. Then $|T_1| = d$ and $d|n$, so that $T_1 \in E[n]$.

(4) Compute $\zeta_1 = e_n(P, T_1)$ and $\zeta_2 = e_n(Q, T_1)$. Then both $\zeta_1, \zeta_2 \in \mu_d \subset \mathbb{F}_{q^m}^{\times}$.

(5) Solve the discrete logarithm problem $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{q^m}^{\times}$. This gives $k \pmod d$.

(6) Repeat with random points $T_2, T_3, \ldots$ until the least common multiple of the various d's obtained is n. This determines $k \pmod n$.

There is the possibility that $m \in \mathbb{Z}$ could be very large, in which case the discrete logarithm problem in the group $\mathbb{F}_{q^m}^{\times}$, which has order $q^m - 1$, is just as difficult to solve the discrete logarithm problem in the smaller group $E(\mathbb{F}_q)$. However, for supersingular curves, we can usually take $m = 2$ as the next result states.

Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of a prime p. Then $\#E(\mathbb{F}_q) = q + 1 - a$ for some $a \in \mathbb{Z}$. The curve E is supersingular if $a \equiv 0 \pmod p$. Corollary 3.5.3 states that $a \equiv 0 \pmod p$ is equivalent to $a = 0$ when $q = p \geq 5$.

Proposition 4.3.2. *Let E be an elliptic curve over $\mathbb{F}_q$ and suppose that $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Let $n \in \mathbb{Z}^+$. If there exists a point $P \in E(\mathbb{F}_q)$ such that $|P| = n$, then $E[n] \subset E(\mathbb{F}_{q^2})$.*

Proof. The Frobenius endomorphism φ_q satisfies the equation $\varphi_q^2 - a\varphi_q + q = 0$.

Since $a = 0$, this reduces to $\varphi_q^2 = -q$. Let $S \in E[n]$. Since $\#E(\mathbb{F}_q) = q + 1$ and since there is a point P of order n we have that $n|(q+1)$ or $-q \equiv 1 \pmod{n}$. Therefore,

$$\varphi_q^2(S) = -qS = 1 \cdot S. \tag{4.31}$$

Thus, $S \in E(\mathbb{F}_{q^2})$. □

Therefore, discrete logarithm problems over $\mathbb{F}_q$ for supersingular curves with $a = 0$ can be reduced to discrete logarithm calculations in $\mathbb{F}_{q^2}^{\times}$, which make the computations much easier.

Chapter 5

Elliptic Curve Cryptography

In this chapter, we discuss several cryptosystems based on elliptic curves. However, most of our attention will be on the discrete logarithm problem for elliptic curves. We also introduce the idea of a digital signature and a public key cryptosystem based on factoring as the elliptic curve analogue of RSA.

5.1 Basic Setup

Alice wants to send a message called plaintext to Bob. In order to keep the eavesdropper Eve from reading the message, she encrypts the message using an encryption key to obtain ciphertext. Bob then receives the ciphertext and uses a decryption key to decrypt the ciphertext and read the message from Alice.

There are two basic types of encryption. The first type is called symmetric encryption since the encryption and decryption keys are the same or can be easily obtained from the other. A few popular symmetric encryption methods include Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). In this case, Alice and Bob need some way of establishing a key.

The other type of encryption is called public key encryption or asymmetric

encryption. In this case, Bob publishes a public encryption key which Alice uses. In addition, Bob also has a private decryption key to decrypt ciphertexts. Since everyone knows the encryption key, it should be infeasible to deduce the decryption key from the encryption key. Some popular public key cryptosystems include RSA, which relies on the difficulty of factoring integers into primes, and another cryptosystem due to ElGamal that is based on the difficulty of solving the discrete logarithm problem.

5.2 Diffie-Hellman Key Exchange

Suppose that Alice and Bob want to establish a common key that can be used to exchange data as part of a symmetric encryption scheme. One method to produce a secret key is due to Diffie and Hellman.

(1) Alice and Bob first agree on an elliptic curve E over a finite field $\mathbb{F}_q$, such that the discrete logarithm problem is infeasible in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$ such that the subgroup generated by P has large order.

(2) Alice chooses a secret $a \in \mathbb{Z}$ and computes $aP = P_a$ and sends P_a to Bob.

(3) Bob chooses a secret $b \in \mathbb{Z}$ and computes $bP = P_b$ and sends P_b to Alice.

(4) Alice computes $aP_b = abP$.

(5) Bob computes $bP_a = abP$.

(6) Alice and Bob use some publicly agreed upon method to extract a key from abP, such as they could use the last 256 bits of the x-coordinate of abP.

The only information that the eavesdropper Eve intercepts is the elliptic curve

E, the finite field $\mathbb{F}_q$ and the points P, aP, and bP. Therefore, Eve's problem is that she needs to use just P, aP, and bP to determine abP. If Eve could solve discrete logs over $E(\mathbb{F}_q)$, then she could use P and aP to find Alice's secret key a. Eve could then compute $a(bP)$ to get abP. However, solving this problem requires the knowledge of solving discrete logs, which were assumed to be infeasible to solve over $E(\mathbb{F}_q)$.

A similar problem, known as the Decision Diffie-Hellman problem, is that given $P, aP, bP \in E(\mathbb{F}_q)$ and given a point $Q \in E(\mathbb{F}_q)$, determine whether or not $Q = abP$. In other words, if one is given abP as a tip, can you verify the information is correct? The Weil pairing can be used in some cases to solve the Decision Diffie-Hellman problem, as we show below.

Example 5.2.1. Let E be the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_q$ for $q \equiv 2 \pmod 3$. Note that E is supersingular, that is $E[q] \cong 0$. Let $\omega \in \mathbb{F}_{q^2}$ be a primitive third root of unity. Notice that $\omega \notin \mathbb{F}_q$ since the order of $\mathbb{F}_q^\times$ is $q - 1$, which is not a multiple of 3.

Define a map $\beta : E(\overline{\mathbb{F}_q}) \longrightarrow E(\overline{\mathbb{F}_q})$ defined by $(x, y) \mapsto (\omega x, y)$ and $\infty \mapsto \infty$, which is an isomorphism. Suppose that $P \in E(\overline{\mathbb{F}_q})$ has order n. Then $\beta(P)$ also has order n. Now define the modified Weil pairing

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \beta(P_2)). \tag{5.1}$$

where e_n is the Weil pairing and $P_1, P_2 \in E[n]$.

Suppose that we are given the points $P, aP, bP, Q \in E(\mathbb{F}_q)$ and are asked to determine whether $Q = abP$. First, we use the Weil pairing to decide whether

or not Q is a multiple of P. By Lemma 4.3.1, Q is a multiple of P if and only if $e_n(P,Q) = 1$. Assume that this is the case, so that $Q = tP$ for some $t \in \mathbb{Z}$. Thus, we have that

$$\tilde{e}_n(aP, bP) = \tilde{e}_n(P,P)^{ab} = \tilde{e}_n(P, abP) \tag{5.2}$$

and

$$\tilde{e}_n(P,Q) = \tilde{e}_n(P,tP) = \tilde{e}_n(P,P)^t. \tag{5.3}$$

To complete our computations with the modified Weil pairing, we need the following statement, which is Lemma 6.1 in [7].

Lemma 5.2.2. *Assume that $3 \nmid n$. If $P \in E(\mathbb{F}_q)$ has order exactly n, then $\tilde{e}_n(P,P)$ is a primitive nth root of unity.*

Therefore, if assume that $3 \nmid n$ then

$$Q = abP \iff t \equiv ab \pmod{n} \iff \tilde{e}_n(aP, bP) = \tilde{e}_n(P,Q). \tag{5.4}$$

This solves the Decision Diffie-Hellman problem in this case and it did not involve solving the discrete logarithm problem, nor did the process involve solving the discrete logarithm problem over finite fields. All that was required was the Weil pairing.

5.3 ElGamal Public Key Encryption

Suppose that Alice wants to send a message to Bob. First, Bob establishes his public key as follows. He chooses an elliptic curve E over $\mathbb{F}_q$ such that the discrete logarithm problem is infeasible for $E(\mathbb{F}_q)$ and he also chooses a point $P \in E(\mathbb{F}_q)$

such that the order of P is a large prime. In addition, Bob chooses a secret $s \in \mathbb{Z}$ and computes $B = sP$. Therefore, Bob's public key is E, $\mathbb{F}_q$, P and B and his private key is s.

Therefore, for Alice to send a message to Bob, she does the following:

(1) Downloads Bob's public key.

(2) Expresses her message as a point $M \in E(\mathbb{F}_q)$.

(3) She chooses a secret random $k \in \mathbb{Z}$ and computes $M_1 = kP$.

(4) Computes $M_2 = M + kB$.

(5) Sends M_1 and M_2 to Bob.

For Bob to decrypt the ciphertext, he calculates

$$M_2 - sM_1 = (M + kB) - s(kP) = (M + skP) - skP = M. \tag{5.5}$$

Eve knows Bob's public key and the points M_1 and M_2, however, if she does not know how to solve discrete logs then there does not appear a way to obtain M.

One important note about $k \in \mathbb{Z}$ that Alice chooses randomly is that she must use a different $k \in \mathbb{Z}$ each time a message is sent to Bob. If she uses the same value of k and computes M and M', then Eve will immediately recognize that Alice has used the same integer k since $M_1 = M_1'$. Eve can then compute $M_2 - M_2' = M - M'$ so that she can recover the message M by noting that $M' = M - M_2 + M_2'$.

5.4 ElGamal Digital Signatures

Suppose that Alice wants to sign an electronic document. One way is to digitalize Alice's signature, however, eavesdropper Eve can copy and then append Alice's digital signature to any document. Therefore, steps need to be implemented

so that such a digital signature can only be used once. However, it must be possible for someone to verify that the signature is valid and it should be possible to verify that Alice was the person who signed the document. One solution to the problem relies on the difficulty of the discrete logarithm problem.

Alice first chooses an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is infeasible in $E(\mathbb{F}_q)$. She also chooses a point $A \in E(\mathbb{F}_q)$ such that $|A| = N$ is a large prime. Alice also chooses a secret $a \in \mathbb{Z}$ and computes the point $B = aA$. Finally, she chooses a function $f : E(\mathbb{F}_q) \longrightarrow \mathbb{Z}$ and has the property that its image is large and only a small number of inputs result in any given output.

Therefore, Alice's public key is E, $\mathbb{F}_q$, f, A, and B. Her private key is the secret $a \in \mathbb{Z}$. However, the order of the point A does not need be made public. Hence, to sign a document Alice does the following:

(1) Represents the document as $m \in \mathbb{Z}$. If $m > N$, then Alice chooses a larger curve.

(2) Chooses a random $k \in \mathbb{Z}$ with $\gcd(k, N) = 1$ and compute $R = kA$.

(3) Computes $s \equiv k^{-1}(m - af(R)) \pmod{N}$.

The signed message is then (m, R, s). Notice that Alice does not want to keep the message m secret. If she wants to do that, then she needs to use a form of encryption. Bob then verifies the message is from Alice as follows:

(1) Bob downloads Alice's public information.

(2) Computes $V_1 = f(R)B + sR$ and $V_2 = mA$.

(3) If $V_1 = V_2$, then Bob declares that the signature is valid.

If the signature is valid, then $V_1 = V_2$ since

$$\begin{aligned} V_1 = f(R)B + sR &= f(R)aA + skA \\ &= f(R)aA + (m - af(R))A \\ &= mA = V_2. \end{aligned} \tag{5.6}$$

Here we have used the fact that $sk \equiv m - af(R)$, hence $sk = m - af(R) + zN$ for some $z \in \mathbb{Z}$. Therefore,

$$\begin{aligned} skA = (m - af(R) + zN)A &= (m - af(R))A + zNA \\ &= (m - af(R))A + \infty \\ &= (m - af(R))A. \end{aligned} \tag{5.7}$$

This is why the congruence defining s was taken modulo N.

If Eve can compute discrete logs then she can use A and B to find the secret $a \in \mathbb{Z}$. Therefore, she can then forge Alice's digital signature on any message. Even worse, Eve could use A and R to find k. Since she knows $s, f(R), m$, she can then use

$$ks \equiv (m - af(R)) \pmod{N} \tag{5.8}$$

to find a. If $d = \gcd(f(R), N) \neq 1$ then $af(R) \equiv (m - ks) \pmod{N}$ has d solutions for a. Provided that d is small, Eve can then try each possibility until she obtains $B = aA$. In this case, Eve can now use a to forge Alice's signature on arbitrary messages.

Therefore, Alice must keep a and k secret. In addition, as in ElGamal public key encryption, Alice must choose a different k for each signature. Suppose that Alice signs messages m and m' using the same $k \in \mathbb{Z}$ to obtained signed messages (m, R, s) and (m', R, s'). Eve will immediately recognize that k has been used

twice, since R is the same for both signatures. The equations for s, s' give the following:

$$\begin{aligned} ks &\equiv (m - af(R)) \pmod{N} \\ ks' &\equiv (m' - af(R)) \pmod{N}. \end{aligned} \tag{5.9}$$

Subtracting these two congruences gives $k(s - s') \equiv (m - m') \pmod{N}$. Let $d = \gcd(s - s', N)$ then there are d possible values of k. Eve tries each one until $R = kA$ is identified. Once she knows k she can then find a as before.

5.5 Elliptic Curve Analogue of RSA

Most cryptosystems using elliptic curves are based on solving the discrete logarithm problem, in contrast to classical cryptosytems that are sometimes based on solving discrete logarithms or the difficulty of factoring. The most famous public key cryptosystem is called RSA, named after Rivest, Shamir, and Adleman, and is the following algorithm. Alice wants to send a message to Bob.

(1) Bob secretly chooses two distinct large primes p, q and computes $n = pq$.

(2) Bob also chooses integers e, d with

$$ed \equiv 1 \pmod{\varphi(pq)} \equiv 1 \pmod{(p-1)(q-1)}. \tag{5.10}$$

(3) Bob makes n and e public and keeps d, p, and q secret.

(4) Alice represents her message as a number $m \pmod{n}$.

(5) Alice then computes $c \equiv m^e \pmod{n}$ and sends c to Bob.

(6) Bob computes $m \equiv c^d \pmod{n}$ to obtain the message m.

This decryption procedure works since

$$m \equiv c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}. \tag{5.11}$$

Since $ed \equiv 1 \pmod{\varphi(pq)} \implies ed = 1 + k\varphi(pq)$ for some $k \in \mathbb{Z}$, we have

$$m^{ed} \equiv m^{1+k\varphi(pq)} \equiv m(m^{\varphi(pq)})^k \equiv m \pmod{n}. \tag{5.12}$$

If Eve can determine the factorization $n = pq$, then she can solve $ed \equiv 1 \pmod{n}$ to obtain d. However, it can be shown [6] that if Eve can find the decryption key d, then she can probably factor n. Therefore, the difficulty of factoring n is the key to the security of RSA.

In the following, we present one cryptosystem that is an elliptic curve analogue of RSA due to Koyama, Maurer, Okamoto, and Vanstone, which is not used much in practice. Alice wants to send a message to Bob, then they do the following:

(1) Bob chooses two distinct large primes p, q with $p \equiv q \equiv 2 \pmod{3}$ and computes $n = pq$.

(2) Bob also chooses integers e, d with

$$ed \equiv 1 \pmod{(p+1)(q+1)}. \tag{5.13}$$

(3) Bob makes n and e public and keeps d, p, and q secret.

(4) Alice represents her message as a pair of integers $(m_1, m_2) \pmod{n}$. She regards (m_1, m_2) as a point M on the elliptic curve E given by

$$y^2 = (x^3 + b) \pmod{n} \tag{5.14}$$

where $b = (m_2^2 - m_1^3) \pmod{n}$. She does not need to compute b.

(5) Alice computes $C = (c_1, c_2) = eM$ with operations performed on E and sends C to Bob.

(6) Bob computes $M = dC$ on E to obtain M.

Note that the formulas for addition on E never use the value of b, so Alice and Bob never need to compute it. Eve can compute it if she wants as $b = c_2^2 - c_1^3$.

By the Chinese Remainder Theorem an integer modulo n may be regarded as a pair of integers, one modulo p and the other modulo q. Therefore, we may regard a point on E in $\mathbb{Z}_n$ as a pair of points with one on E modulo p and the other on E modulo q. Hence, we have that

$$E(\mathbb{Z}_n) \cong E(\mathbb{F}_p) \oplus E(\mathbb{F}_q). \tag{5.15}$$

Thus, we see that $\#E(\mathbb{Z}_n) = \#E(\mathbb{F}_p) \cdot \#E(\mathbb{F}_q)$. By Proposition 3.5.4, E is supersingular modulo p and modulo q, so by Corollary 3.5.3 we see

$$\#E(\mathbb{F}_p) = p + 1 \quad \text{and} \quad \#E(\mathbb{F}_q) = q + 1. \tag{5.16}$$

Therefore, $(p+1)M = \infty \pmod{p}$ and $(q+1)M = \infty \pmod{q}$ so that the decryption works.

Write $de = 1 + k(p+1)$ for some $k \in \mathbb{Z}$, then

$$dC = deM = (1 + k(p+1))M = M + k(p+1)M = M + \infty = M \pmod{p}, \tag{5.17}$$

and similarly modulo q. Therefore, $dC = M$.

Again, if Eve knows how to factor n as pq, then she knows $(p+1)(q+1)$, so she can find d with $ed \equiv 1 \pmod{(p+1)(q+1)}$. Thus, she can decrypt Alice's message. We see that the difficulty of factoring n is again the key to the security of this algorithm.

Chapter 6

Applications in Number Theory

In the 1980s, two applications of elliptic curves were found, which involved factoring and primality testing. These are generalizations of the classical methods in number theory that worked over the multiplicative group $\mathbb{Z}_n^\times$. The advantage of using elliptic curves is that more than one elliptic curve may be used, since there are more than one elliptic curve modulo n. Thus, if one elliptic curve does not work, another can be used.

6.1 Factoring Using Elliptic Curves

In 1987, Hendrik Lenstra developed a factoring algorithm using the properties of elliptic curves, which turned out to be very effective for factoring positive integers of around 60 decimal digits. We start with the classical $p-1$ factorization method.

Suppose that n is a composite integer that we want to factor. We choose a random $a \in \mathbb{Z}$ and a large $B \in \mathbb{Z}$ and compute $a_1 \equiv a^{B!} \pmod{n}$ and $\gcd(a_1 - 1, n)$ by recursively computing

$$a^{b!} \equiv \left(a^{(b-1)!}\right)^b \pmod{n} \quad \text{for } b = 2, 3, 4, \ldots, B \tag{6.1}$$

Definition 6.1.1. *An integer m is B-smooth if all the prime factors of m are less than or equal to B. That is, if*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{6.2}$$

is the prime factorization of m, then $p_i \leq B$ for all $i = 1, 2, \ldots, k$.

For simplicity assume that $n = pq$ is a product of two large primes. Suppose that $p-1$ is B-smooth. Since $B!$ contains all the prime factors up to B, it is likely that $B!$ is a multiple of $p-1$. Therefore,

$$a_1 \equiv a^{B!} \equiv 1 \pmod{p} \tag{6.3}$$

by Fermat's little theorem.

Now suppose that $q-1$ is divisible by a prime $\ell > B$. Of all the elements in the cyclic group $\mathbb{Z}_q^\times$, there are at most $(q-1)/\ell$ elements that have order not divisible by ℓ and at least $(\ell-1)(q-1)/\ell$ that have order divisible by ℓ. Hence, it is very unlikely that the order of a is divisible by ℓ and

$$a_1 \equiv a^{B!} \not\equiv 1 \pmod{q}. \tag{6.4}$$

Hence, $a_1 - 1$ is a multiple of p, but is not a multiple of q, so that $\gcd(a_1 - 1, pq) = p$.

In the elliptic curve factorization method, we need to choose random elliptic curves modulo n and random points on these curves. One way to do this is to first choose a random $a \in \mathbb{Z}_n$ and a random pair $P = (u, v) \pmod{n}$. Then choose c such that

$$c = (v^2 - u^3 - au) \pmod{n}. \tag{6.5}$$

This gives an elliptic curve E defined by $y^2 = x^3 + ax + c$ with a point $P = (u, v)$.

Now we give the elliptic curve factorization method. We begin with an odd composite integer n that we want to factor and perform the following:

(1) Choose around 10 to 20 random elliptic curves $E_i : y^2 = x^3 + a_i x + c_i$ and points $P_i \pmod{n}$.

(2) Choose an integer B around 10^8 and compute $(B!)P_i$ on E_i for each i.

(3) If (2) fails because the slope does not exist modulo n, then we have found a factor of n.

(4) If (2) succeeds, increase B or choose new random curves E_i and points P_i and start over.

Example 6.1.2. Suppose that we are interested in factoring 4453. Rather than using the classical method, we use the elliptic curve factorization method. Let E be an elliptic curve $y^2 = (x^3 + 10x - 2) \pmod{4453}$ and let $P = (1, 3)$.
We choose $B = 3$ and compute $(3!)P = 6P$. Thus, we begin by computing $2P$. The slope of the tangent line at P is given by

$$m = \frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}. \tag{6.6}$$

Here we found $6^{-1} \equiv 3711 \pmod{4453}$, since $\gcd(6, 4453) = 1$. Using this slope, we find that $2P = (4332, 3230)$.

Now we compute $4P = 2(2P) = (1648, 4212)$ using the same method as above. To compute $6P$, we add $2P$ and $4P$. The slope is given as

$$m = \frac{4212 - 3230}{1648 - 4332} = \frac{982}{1769}. \tag{6.7}$$

However, $\gcd(1769, 4453) = 61 \neq 1$, so that 1769^{-1} does not exist and we cannot evaluate the slope. Thus, we have found a factor of 4453, namely $4453 = 61 \cdot 73$.

This elliptic curve factorization method is very successful in finding a prime factor p of n when $p < 10^{40}$. Suppose we are given a random composite integer n that is around 100 decimal digits. If we are unable to find a small prime factor that is less than 10^7, then the elliptic curve method can be used to find a prime factor. However, in many cryptographic applications n is taken so that its prime factors p and q are such that $p, q < 10^{74}$. For such numbers, the quadratic sieve and the number field sieve factorization methods outperform the elliptic curve method.

6.2 Primality Testing

To prove that an integer is prime of several thousand decimal digits the most popular method currently in use involves elliptic curves. The elliptic curve primality test is an elliptic curve generalization of the classical Pockington-Lehmer primality test, which is stated as Proposition 7.1 in [7].

Proposition 6.2.1. *Let $n > 1$ be an integer and let $n - 1 = rs$, where $r \geq \sqrt{n}$. Suppose that for each prime $\ell | r$, there exists $a_\ell \in \mathbb{Z}$ such that*

$$a_\ell^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \gcd(a_\ell^{(n-1)/\ell} - 1, n) = 1, \tag{6.8}$$

then n is prime.

To illustrate the usefulness of the Pockington-Lehmer primality test, we consider the following example.

Example 6.2.2. Let $n = 153533$, then $n - 1 = 153532 = 2^2 \cdot 131 \cdot 293$. Let

$r = 2^2 \cdot 131$. The primes dividing r are $\ell = 2$ and $\ell = 131$. Therefore, we have

$$2^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \gcd(2^{(n-1)/2} - 1, n) = 1 \tag{6.9}$$

so we take $a_2 = 2$. Furthermore,

$$2^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \gcd(2^{(n-1)/131} - 1, n) = 1 \tag{6.10}$$

so that $a_{131} = 2$ as well. Therefore, by the Pockington-Lehmer primality test, 153533 is prime.

As in the classical factorization method, for composite integers that have are thousand digits, an elliptic curve analogue can be used. The following method is due to Goldwasser and Kilian and is Theorem 7.3 in [7].

Theorem 6.2.3. *Let $n > 1$ and let E be an elliptic curve modulo n. Suppose there exist distinct primes $\ell_1, \ell_2, \ldots, \ell_k$ and finite points $P_i \in E(\mathbb{Z}_n)$ such that*

(1) $\ell_i P_i = \infty$ *for* $1 \leq i \leq k$.

(2) $\prod_{i=1}^{k} \ell_i > (n^{1/4} + 1)^2$,

then n is prime.

Example 6.2.4. Let $n = 907$ and E be the elliptic curve given by

$$y^2 = (x^3 + 10x - 2) \pmod{907}. \tag{6.11}$$

Let $\ell = 71$, then

$$71 > \left(907^{1/4} + 1\right)^2 \approx 42.092. \tag{6.12}$$

Let $P = 13(1,3) = (819, 784)$, so that $|P| = 923 = 13 \cdot 71$. Thus, $71P = \infty$ and by Theorem 6.2.3, 907 is prime.

For large values of n, the most difficult part of using Theorem 6.2.3 is finding an elliptic curve E that has enough points. One method is to choose random elliptic curves modulo n and compute their orders, until an elliptic curve has order that has a suitable prime factor ℓ. In practice, the Goldwasser-Kilian method has been successful in proving the primality of integers of more than 1000 decimal digits.

Appendix A

Projective Space and the Point at Infinity

Projective space allows us to make sense out of the statement that all parallel lines intersect at ∞ and also to interpret the point at infinity on an elliptic curve.

Definition A.1. *Let K be a field. The two-dimensional projective space $\mathbb{P}^2_K$ over K is given by equivalence classes of triples (x, y, z) with $x, y, z \in K$ and at least one of $x, y, z \neq 0$. The triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are equivalent if there exists a nonzero element $\lambda \in K$ such that*

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2). \tag{A.1}$$

In other words,

$$\mathbb{P}^2_K = (K^3 - \{0\})/\sim \quad \text{where } (x, y, z) \sim (\lambda x, \lambda y, \lambda z) \text{ if } \lambda \in K^\times. \tag{A.2}$$

The equivalence class of (x, y, z) is denoted $(x : y : z)$.

If $(x : y : z)$ is a point with $z \neq 0$, then $(x : y : z) = (x/z : y/z : 1)$, which are finite points in $\mathbb{P}^2_K$. If $z = 0$, however, the point at infinity is the point $(x : y : 0)$ in $\mathbb{P}^2_K$.

Definition A.2. *Let K be a field, the two-dimensional affine plane over K is often denoted*

$$\mathbb{A}^2_K = \{(x, y) \in K \times K\}, \tag{A.3}$$

so that we have the inclusion $\mathbb{A}^2_K \hookrightarrow \mathbb{P}^2_K$ by $(x, y) \mapsto (x : y : 1)$.

Hence, the affine plane is identified with the finite points in $\mathbb{P}^2_K$.

Definition A.3. *A polynomial is homogeneous of degree n if it is the sum of terms $ax^iy^jz^k$ with $a \in K$ and $i + j + k = n$. Note that if F is a polynomial that is homogeneous of degree n, then $F(\lambda x, \lambda y, \lambda z) = \lambda^{i+j+k}F(x, y, z) = \lambda^n F(x, y, z)$ for all $\lambda \in K$.*

To obtain a homogeneous polynomial from a polynomial, we multiply by an appropriate power of z to individual terms. For example, if $f(x, y) = y^2 - x^3 - ax - b$, then $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$ is a homogeneous polynomial of degree 3. Thus, if F is homogeneous of degree n then $F(x, y, z) = z^n f(x/z, y/z)$ and $f(x, y) = F(x, y, 1)$.

Therefore, when two parallel lines meet at infinity we mean the following. Let $y = mx + b_1$ and $y = mx + b_2$ be a set of non-vertical parallel lines, so that $b_1 \neq b_2$. Then they have corresponding homogeneous forms;

$$y = mx + b_1 z \quad \text{and} \quad y = mx + b_2 z. \tag{A.4}$$

Thus, by solving we get that

$$mx + b_1 z = mx + b_2 z \implies (b_1 - b_2)z = 0 \implies z = 0 \tag{A.5}$$

so that $y = mx$. Since all x, y, z cannot be zero, we must have $x \neq 0$. Therefore, we can rescale by dividing by x and find the intersection of the two lines as

$$(x : mx : 0) = x(1 : m : 0) = (1 : m : 0). \tag{A.6}$$

On the other hand, if $x = c_1$ and $x = c_2$ are a pair of vertical lines then they will intersect at the point $(0 : 1 : 0)$.

Example A.4. Given an elliptic curve E defined by $y^2 = x^3 + ax + b$, its homogeneous form is $y^2z = x^3 + axz^2 + bz^3$. The points $(x, y) \in E$ correspond to $(x : y : 1)$. If we set $z = 0$, then we obtain $x^3 = 0$ and so $x = 0$. By rescaling we see that $(0 : y : 0) = (0 : 1 : 0)$ is the only point at infinity on E. Moreover, since $(0 : 1 : 0) = (0 : -1 : 0)$ we see that the "top" and "bottom" of the y-axis are the same.

Bibliography

[1] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[2] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301−304, 1987.

[3] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483−494, 1985.

[4] D. Shanks. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, NY, 1969)*, pages 415−440. Amer. Math. Soc., Providence, RI, 1971.

[5] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[6] W. Trappe and L.Washington. *Introduction to cryptography with coding theory, (2nd ed.)*. Prentice Hall, Upper Saddle River, NJ, 2006.

[7] L. C. Washington. *Elliptic curves. Number theory and cryptography, (2nd ed.)*. Chapman & Hall/CRC, New York, NY, 2008.

[8] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521−560, 1969.