# Elliptic Curves:
# Number Theory and Cryptography

Kethari Narasimha Vardhan
Tata Sai Manoj
Velagala Krishna Sai Deepak Reddy

Group Project

February 12, 2022

# 1 Chapter 1

# Introduction

## 1.1 Pyramid of Cannonballs

Let us take a scenario where we put 1 ball at the first layer, 4 balls at the second layer, 9 balls at the third layer and so on ... Now, is it possible to arrange a total of n balls in a similar pattern such that all these balls can be fitted into a square array?

Mathematically,

Sum of all the balls would be;

$$1 + 2^2 + 3^2 + \ldots + n^2 = \frac{(n)(n+1)(2n+1)}{6}$$

The above expression should be a perfect square.

$$\Rightarrow y^2 = \frac{(n)(n+1)(2n+1)}{6}$$

An equation of the above form is called an **Elliptic Curve**.

## 1.2 Elliptic Curve

In mathematics, an elliptic curve is an equation of genus-1 surface. Genus, to simply put in, is the number of "holes" of a surface. Elliptic Curves are important in Number Theory aspects and find applications in Elliptic Curve Cryptography (ECC). These are used in encryptions, digital signatures, pseudo-random number generators and few other areas.

The general equation of an elliptic curve $E$ is:

$$y^2 = x^3 + Ax + B,$$

where $A$ and $B$ are constants.

## Examples:

(i) Pyramid of Cannonballs

- The above mentioned example when put in mathematical terms, yeilds an Elliptic Curve $y^2 = \dfrac{(x)(x+1)(2x+1)}{6}$

(ii) A right angle triangle with area 5 and having rational side lengths.

- Let $a, b, c$ be the sides of the right angle triangle. Then, we need $a^2 + b^2 = c^2$, such that the area of the triangle is 5 and all the three sides must be rational.
- Now, let us assume $x = (c/2)^2$,
  So we have $x - 5 = ((a-b)/2)^2$,
  and $x + 5 = ((a+b)/2)^2$.
- We are looking for a rational number $x$, such that $x-5$, $x$, $x+5$ are simultaneously squares of rational numbers. So the product, $(x-5)(x)(x+5)$ should also be a perfect square.

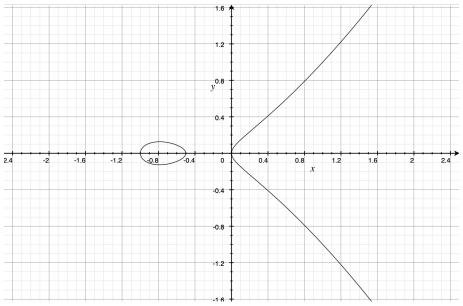
  $$\Rightarrow y^2 = x^3 - 25x$$

  This equation is an elliptic curve.
- The above equation has infinitely many solutions.

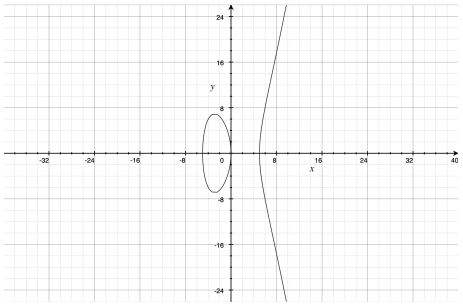
A more general case is, a right angle triangle with area $N$ and having rational sides. The elliptic curve in such scenario would be;

$$y^2 = (x-N)(x)(x+N)$$

$$\Rightarrow y^2 = x^3 - N^2x$$



(a) $y^2 = \frac{(x)(x+1)(2x+1)}{6}$



(b) $y^2 = x^3 - 25x$

Figure 1: Elliptic Curves of (i) and (ii)

The integer $N$ which can occur as an area of a right angle triangle can be seen as *Congruent Number Problem*. Tunnel's theorem relates this to the number of integral solutions of a few fairly simple *Diophantine Equations*. But Tunnel Theorem gives only partial resolution to the Congruent Number Problem.

**Diophantine Equation:** Finding all the right angle triangles with integer solutions is equivalent to solving the Diophantine equation $a^2 + b^2 = c^2$

**Conjecture:** Let $n$ be an odd, squarefree, positive integer. Then $n$ can be expressed as the area of a right angle triangle if and only if, the number of integer solutions of

$$4x^2 + y^2 + 8z^2 = n$$

when $z$ is even is equal to number of solutions when $z$ is odd.

# 2 Chapter 2

# The Basic Theory

## 2.1 Weierstrass Equation

As seen earlier, an elliptic curve $E$ is a graph with general equation

$$y^2 = x^3 + Ax + B,$$

where $A$ and $B$ are constants. The above equation is known as **Weierstrass Equation** for an elliptic curve. It is important to note as in what set $A, B, x,$ and $y$ belong to. Generally, these are the elements taken from a field.

**Field:** In mathematics, a field is a set on which basic mathematical operations are defined and behave as corresponding operations on rational and real numbers do. Such as addition, multiplication, subtraction, and division. A field is an *algebraic structure* that is widely used in algebra, number theory.

Few examples of fields are the field of rational numbers, the field of real numbers, the field of complex numbers. Finite Fields (fields with finitely many elements) are mostly used in cryptographic protocols.

**Algebraic Structure:** An algebraic structure consists of a nonempty set $A$, a collection of operations on $A$, in general binary operations $*$, and finite set of identities that these operations must satisfy.

A group is an example of examples of algebraic structures. The various types of algebraic structures are:

- Semigroup
- Monoid
- Group
- Abelian Group

Let us take an algebraic structure $(\mathbb{Z}, +)$. This is also an example of a group, that satisfies all the conditions of a group, *i.e.,* Closure, Associative, Identity Element, and Inverse Element.

Here, set $A$ is set of all integers $\mathbb{Z}$, and

the binary operation $*$ is addition $(+)$

Now, let us take $K$, that is a field with $A, B \in K$, then we say that the elliptic curve $E$ **is defined over** $K$. If we want to consider points with coordinates in a field $L$ which is a superset of $K$ $(L \supseteq K)$, then $E(L)$ is defined as

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}.$$

This set $E(L)$ always contains the point $\infty$ in it.

If the roots of the cubic equation are $r_1, r_2, r_3$, then it can be proved that the discriminant of the cubic equation is

$$((r_1 - r_2)(r_2 - r_3)(r_3 - r_1))^2 = -(4A^3 + 27B^2).$$

Therefore, we keep the roots of the cubic to be distinct. However, there are cases where the roots are not distinct. Thus, a more generalized equations are of the form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, \ldots, a_6$ are constants. The above equation is called **Generalized Weierstrass Equation**. These equations are useful when the fields have characteristic 2 or 3.

**Characteristic:** Denoted by *char(.)*, is defined by the smallest number of times the multiplicative identiy is to be used to get the additive identity of a ring/group. If the sum never reaches the additive identity, we say that the characteristic of the ring/group is zero.

The characteristic of any field $F$ is either 0 or a prime number $p$.

## 2.2 The Group Law

Let $E$ be an elliptic curve defined as $y^2 = x^3 + Ax + B$. Let us take two distinct points on the curve E, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1, P_2 \neq \infty$. Let $L$ be a line through $P_1$ and $P_2$, and this line $L$ intersects the curve $E$ at $P_3'$. Now, take a reflection of $P_3'$ across the $x-$axis to get a new point $P_3 = (x_3, y_3)$.

Then, we define $P_1 + P_2 = P_3 = (x_3, y_3)$ as:

- If $x_1 \neq x_2$, then

  $x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \dfrac{y_2 - y_1}{x_2 - x_1}$

- If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$

  Since the line $L$ joining $P_1$ and $P_2$ would be a vertical line parallel to the $y-$axis. Thus, the line $L$ doesn't intersect the curve $E$ for any $P_3$.

- If $P_1 = P_2$ and $y_1 \neq 0$, then

  $x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \dfrac{3x_1^2 + A}{2y_1}$

- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$

  Since the line $L$ joining $P_1$ and $P_2$ would be a vertical line and a tangent line to the curve $E$.

### 2.2.1 Theorem

The points on the curve $E$ form an algebraic structure *i.e.*, they form a group. Moreover, they form an abelian group with $\infty$ as it's identity element.

- *Commutativity:* $P_1 + P_2 = P_2 + P_1, \ \forall\, P_1, P_2 \in E$.

- *Existence of Identity:* $P + \infty = P, \ \forall\, P \in E.$
- *Existence of Inverse:* Given $P \in E$, $\exists\, P' \in E$ such that $P + P' = \infty$. The point $P'$ is denoted by $-P$.
- *Associativity:* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3), \ \forall\, P_1, P_2, P_3 \in E.$

□

According to the 2.2.1 Theorem, it is said that the points on the elliptic curve $E$ form an abelian group.

1. An elliptic curve over a finite field has only finitely many points with coordinated in that finite field. Therefore, we obtaion finite abelian group in this case.
2. Let $E$ be an elliptic curve defined over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finite abelian group.

If $P$ is a point on the curve $E$, and let $k$ be any positive integer. Then $kP$ denotes, $P + P + \ldots + P$ ($k$ times). For large values of $k$, repeatedly adding $P$ to itself is computationally heavy task. The computation becomes much faster when *succcessive doubling* method is used.
Eg. Compute $19P$;

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P, \quad 16P = 8P + 8P,$$
$$\text{thus} \Rightarrow 19P = 16P + 2P + P.$$

### 2.2.2 Integer Times a Point

**NOTE:** If we are working over a large finite field and are given points $P$ and $kP$, it is computationally difficult to determine the value of $k$. This is known as the **Discrete Logarithm Problem** for elliptic curves and is the basis for the cryptographic applications.

Let us take $k$ to be any positive integer and let $P$ be a point on the elliptic curve $E$. Then, to compute $kP$:

1. Start with $a = k, B = \infty, C = P$.
2. If $a$ is even, then $a = a/2$, and $C = 2C$.
3. If $a$ is odd, then $a = a - 1$, and $B = B + C$.
4. If $a \neq 0$, repeat from step 2.
5. Output $B$.

```
import math

def isprime(N):
    flag = 1
    for i in range(2, int(math.sqrt(N)) + 1):
        if N % i == 0:
            flag = 0
            break
    else:
        return flag

try:
    a, b = input('Elliptic Curve equation coefficients - a, b: ').spli
    p = int(input('Finite Field EC over prime p: '))
    print(f'Elliptic Curve: y^2 = x^3 + {a}x + {b} (mod {p})')
    if isprime(p) != 1:
        print(f'Given number {p} is not a prime number')
        exit()
    x = int(input('x-coordinate on the curve: '))
    a = int(a)
    b = int(b)
    y = x**3 +a*x + b
    y = y % p
    print(f'Point P := ({x}, {y})')
    s = 3*x**2 + a
    s = s / (2*y)
    x2 = (s**2 - 2*x) % p
    y2 = (s*(x - x2) - y) % p
    print(f'Point 2P := ({x2}, {y2})')
except:
    print('Error while computing. Terminating Program')
    exit()
```

## 2.3 Projective Space and the Point at Infinity

Projective Spaces allow us to interpret the point at infinity on an elliptic curve. Also, it says that parallel lines meet at infinity. In terms of Linear Algebra, a projective space of dimension $n$ is defined as the set of the **vector line** (a vector subspace of dimension 1) in vector space $V$ of $n+1$ dimension. A position vector describes the straight-line travel between a starting point

(usually the origin) and the location of a second point on a coordinate plane is called a vector line.

Let $K$ be a field. A 2-D **projective space** $P_K^2$ over $K$ is given by the equivalence classes of triples $(x, y, z)$ with $x, y, z \in K$. Two triples $(x_1, y_1, z_1)$ and $(x_2, y_2, z_2)$ are said to be **equivalent** if there exists a nonzero element $\lambda \in K$, such that

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$$

We write such a relation as $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. This class of triples depends on the ratios of $x$ to $y$ to $z$. Thus, the equivalence class is denoted by $(x : y : z)$.

We can write $(x : y : z)$ as $(x/z : y/z : 1)$ which represent "finite" points in $P_K^2$. And if $z = 0$, then the ratio becomes $(x : y : 0)$ which are called the **"points at infinity"** in $P_K^2$.

The two-dimensional **affine plane** over $K$ is denoted as:

$$\mathbb{A}_K^2 = \{(x, y) \in K \text{ x } K\}$$

**Affine Plane:** In geometry, an affine plane is a system of points and lines that satisfy the below conditions. Note that in an affine plane, two lines are called *parallel* if they are equal disjoint.

- Any two distinct points lie on a unique line.
- Each line has at least two points.
- Given a point and a line, there is a unique line which contains the point and is parallel to the line (From the Note point).
- There exist three non-collinear points.

Parallelism, the state of being parallel is an equivalence relation on the lines of an affine plane. *Euclidean Plane* is a familiar affine plane. There are also many finite and infinite affine planes.

**Finite Affine Plane:** If the number of points in an affine plane is finite, then if one line contains $n$ points, then:

- each line contains $n$ points.
- each point is contained in $n + 1$ lines.
- there are $n^2$ points in all.
- there is a total of $n^2 + n$ lines.

Here, the number $n$ is called the *order* of the affine plane. All knows finite affine planes have order as either a prime number or prime power integer.

Now, let us take an inclusion,

$$A_K^2 \hookrightarrow P_K^2$$

given by

$$(x, y) \mapsto (x : y : 1)$$

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

If $f(x, y)$ is a polynomial in $x$ and $y$, then we can make it homogeneous by inserting appropriate powers of $z$. Let us take A$f(x, y) = y^2 - x^3 - Ax - B$, then we obtain the homogeneous polynomial $F(x, y, z) = y^2z - x^3 - Axz^2 - bz^3$. If $F$ is homogeneous of degree $n$, then:

$$F(x, y, z) = z^n f(\frac{x}{z}, \frac{y}{z}) \text{ and } f(x, y) = F(x, y, 1)$$

Now, let us take an Elliptic Curve $E$ defined as $y^2 = x^3 + Ax + B$. The homogeneous form of this curve $E$ would be $y^2z = x^3 + Axz^2 + Bz^3$. The points $(x, y)$ on the original curve correspond to the points $(x : y : 1)$ in this new projective version. To see what points on $E$ lie at infinity, set $z = 0$ and obtain $0 = x^3$. Thus, $x = 0$, and $y$ can be any nonzero number (NOTE: $(0 : 0 : 0)$ is not allowed). Rescaling $y$ as, $(0 : y : 0) = (0 : 1 : 0)$ is the point at infinity on $E$. Moreover, since $(0 : 1 : 0) = (0 : -1 : 0)$, the "top" and the "bottom" of the $y-$axis are the same.

There are situations where using projective coordinates sppeds up the computational aspects on elliptic curves.

## 2.4 Proof of Associativity

Associativity of addition of points on an elliptic curves. Two most important theorems that are not about elliptic curves but are quite fascinating here are Pappus and Pascal.

### 2.4.1 Lemma:

Let $G(u, v)$ be a nonzero homogeneous polynomial and let $(u_0 : v_0) \in \mathbb{P}_K^1$. Then there exists an integer $k \geq 0$ and a polynomial $H(u, v)$ with $H(u_0, v_0) \neq 0$ such that

$$G(u, v) = (v_0u - u_0v)^k H(u, v)$$

□

Let $f(x, y) = 0$ be a polynomial describing a curve $C$ in the affine plane and let

$$x = a_1t + b_1,\ y = a_2t + b_2$$

be a line $L$ written in terms of the parameter $t$. And let,

$$\tilde{f}(t) = f(a_1t + b_1, a_2t + b_2).$$

The line $L$ intersects the curve $C$ at suppose $t = t_0$ if $\tilde{f}(t_0) = 0$. If $(t - t_0)^2$ divides $\tilde{f}(t)$, the $L$ is a tangent to $C$. To keep it more general, we say that $L$ intersects $C$ to order $n$ at the point $(x, y)$ corresponding to $t = t_0$ if $(t - t_0)^n$ is the highest power of $(t - t_0)$ that divides $\tilde{f}(t)$.

The homogeneous polynomial of the above can be described as

$$\tilde{F}(u, v) = F(a_1u + b_1v, a_2u + b_2v, a_3u + b_3v)$$

Here, we say that $L$ intersects $C$ to order $n$ at the point $P = (x_0 : y_0 : z_0)$ corresponding to $(u : v) = (u_0 : v_0)$ if $(v_0u - u_0v)^n$ is the highest power of $(v_0u - u_0v)$ dividing $\tilde{F}(u, v)$. We denote this by

$$ord_{L,P}(F) = n$$

If $\tilde{F}$ is identically 0, then we let $ord_{L,P}(F) = \infty$. The major advantage of the homogeneous formulation is that it allows us to treat the points at infiinty along with the finite points in a uniform manner.

### 2.4.2 Lemma:

Let $L_1$ and $L_2$ be lines intersecting in a point $P$, and, for $i = 1, 2$, let $L_i(x, y, z)$ be a linear polynomial defining $L_i$. Then $ord_{L_1,P}(L_2) = 1$ unless $L_1(x, y, z) = \alpha L_2(x, y, z)$ for some constant $\alpha$, in which case $ord_{L_1,P}(L_2) = \infty$.

### 2.4.3 Definition:

A curve in $\mathbb{P}^2_K$ defined by $F(x, y, z) = 0$ is said to be **non-singular** at a point $P$ if at least one of the partial derivatives $F_x, F_y, F_z$ is nonzero at $P$.

Let us take an Elliptic Curve $F(x, y, z) = y^2z - x^3 - Axz^2Bz^3 = 0$, and let us assume the characteristic of our field $K$ is not 2 or 3. Now, we have

$$F_x = -3x^2 - Az^2$$

$$F_y = 2yz$$

$$F_z = y^2 - 2Axz - 3Bz^2$$

Suppose $P = (x : y : z)$ is a singular point. It can be easily shown that for any values of $x, y, z$, there occurs a contradiction for Elliptic Curves. Therefore, **an elliptic curve has no singular points**.
NOTE: This is true even if we consider points with coordinates in $\overline{K}$ (= algebraic closure of $K$). In general, by a **non-singular curve**, we mean a curve with no singular points in $\overline{K}$. $\square$
If $P$ is a nonsingular point of a curve $F(x, y, z) = 0$, then the tangent line at $P$ is

$$F_x(P)x + F_y(P)y + F_z(P)z = 0$$

The above equation leads us to the fact that $\infty + \infty = \infty$ on an elliptic curve.

### 2.4.4 Lemma:

Let $F(x, y, z) = 0$ define a curve $C$. If $P$ is a nonsingular point of $C$, then there is exactly one line in $\mathbb{P}^2_K$ that intersects $C$ to order at least 2, and it is the tangent to $C$ at $P$.

Didn't understand this proof. $\square$

### 2.4.5 Theorem:

Let $C(x, y, z)$ be a homogeneous cubic polynomial, and let $C$ in $\mathbb{P}^2_K$ described by $C(x, y, z) = 0$. Let $l_1, l_2, l_3$ and $m_1, m_2, m_3$ be lines in $\mathbb{P}^2_K$ such that $l_i \neq m_j$ for all $i, j$. Let $P_{ij}$ be the point of intersection of $l_i$ and $m_j$. Suppose $P_{ij}$ is a nonsingular point on the curve $C$ for all $(i, j) \neq (3, 3)$.
In Addition, we require that if, for some $i$, there are $k \geq 2$ of the points $P_{i1}, P_{i2}, P_{i3}$ equal to the same point, then $l_i$ intersects $C$ to order at least $k$ at this point. Also, if, for some $j$, there are $k \geq 2$ of the points $P_{j1}, P_{j2}, P_{j3}$ equal to the same point, then $m_j$ intersects $C$ to order at least $k$ at this point. Then $P_{33}$ also lies on the curve $C$.

**Proof:** Express $l_1$ in the parametric form. Then $C(x, y, z)$ becomes $\tilde{C}(u, v)$. The line $l_1$ passes through $P_{11}, P_{12}, P_{13}$. Let $(u_1 : v_1), (u_2 : v_2), (u_3 : v_3)$ be the parameters on $l_1$ for these points. Since these points lie on $C$, we have $\tilde{C}(u_i, v_i) = 0$ for $i = 1, 2, 3$.

Let $m_j$ have equation $m_j(x, y, z) = a_j x + b_j y + c_j z = 0$. Substituting the parameterization for $l_1$ yields $\tilde{m}_j(u, v)$. Since $P_{ij}$ lies on $m_j$, we have $\tilde{m}_j(u_j, v_j) = 0$ for $j = 1, 2, 3$.

Since $l_1 \neq m_j$ and since the zeros of $\tilde{m}_j$ yield the intersections of $l_1$ and $m_j$ , the function $\tilde{m}_j(u, v)$ vanishes only at $P_{1j}$, so the linear form $\tilde{m}_j$ is nonzero. Therefore, the product $\tilde{m}_1(u, v)\tilde{m}_2(u, v)\tilde{m}_3(u, v)$ is a nonzero cubic homogeneous polynomial. We need to relate this product to $\tilde{C}$.■

## 2.5 Other Equations for Elliptic Curves

Generally, we are mainly dealing with Weierstrass Equation of Elliptic Curves. However, elliptic curves arise in various other guises.

### 2.5.1 Legendre Equation

This is a variant on the Weierstrass Equation. It's advantage is that it allows us to express all elliptic curves over an algebraically closed field (characteristic $\neq 2$) in terms of one parameter.

Let $K$ be a field of characteristic not 2 and let

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$$

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

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

Then $\lambda \neq 0, 1$ and,

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda).$$

This equation has three singular points, $\lambda = 0, 1, \infty$.

### 2.5.2 Cubic Equations

Let us consider a cubic Fermat equation $x^3 + y^3 + z^3 = 0$.
This equatoin has no rational solutions with $xyz \neq 0$ was a conjecture and represents a special case of Fermat's Last Theroem, which asssets that the sum of two nonzero $n$th powers of integers cannot be a nonzer $n$th power when $n \geq 3$.

It is possible to start with a cubic equation $C(x, y) = 0$, over a field $K$ of characteristics not 2 or 3, that has a point with $x, y \in K$ and find an invertible change of variables that transforms the equation to Weierstrass form.

### 2.5.3 Quartic Equations

Sometimes, we might come across few curves defined by the equation of the form

$$v^2 = au^4 + bu^3 + cu^2 + du + e,$$

with $a \neq 0$. If we have a point $(p, q)$ lying on the curve with $p, q \in K$, then the equation can be transformed into a Weierstrass Equatoin by an invertible change of variables that uses rational functions wiht coefficients in the field $K$.
NOTE: If we are going to transform a curve $C$ into Weierstrass form in such a way that all coefficients of the rational functions describing the transformation lie in $K$, then we need to start with a point on $C$ that has coordinates in $K$.

Suppose we have a curve defined by the above equation and suppose we have a point $(p, q)$ lying on the curve. By changing $u$ to $u + p$, we may assume $p = 0$, so the point has the form $(0, q)$.

$$(\frac{v}{u^2})^2 = d(\frac{1}{u})^3 + c(\frac{1}{u})^2 + b(\frac{1}{u}) + a.$$

This can be easily transformed into a Weierstrass Equation in $d/u$ and $dv/u^2$.

**Theorem:**

Let $K$ be a field of characteristic not 2. Consider the equation

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2$$

with $a, b, c, d, q \in K$. Let,

$$x = \frac{2q(v + q) + du}{u^2}, \quad y = \frac{4q^2(v + q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3}.$$

Now, define

$$a_1 = d/q, \;\; a_2 = c - (d^2/4q^2), \;\; a_3 = 2qb, \;\; a_4 = -4q^2a, \;\; a_6 = a_2a_4$$

Then,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The inverse transformation is

$$u = \frac{2q(x + c) - (d^2/2q)}{y}, \;\; v = -q + \frac{u(ux - d)}{2q}.$$

The point $(u, v) = (0, q)$ corresponds to the point $(x, y) = \infty$ and $(u, v) = (0, -q)$ corresponds to $(x, y) = (-a_2, a_1a_2 - a_3)$.

### 2.5.4 Intersection of Two Quadractic Surfaces

The intersection of two quadractic surfaces in three-dimensional space, along with a point on this intersection, is usually an elliptic curve. DOUBT HEREEEEEE

Let us consider pairs of equations of the form

$$au^2 + bv^2 = 3, \quad cu^2 + dw^2 = f,$$

where $a, b, c, d, e, f$ are nonzero elements of a field $K$ of characteristic not 2. Each separeate equation may be regarded as a surface in $uvw$-space, and they intersect in a curve. Let's take $P = (u_0, v_0)$ be a point on $C$, where $C$ is a curve in the $uv$-plane. Let $L$ be the line through $P$ with slope $m$,

$$u = u_0 + t, \quad v = v_0 + t.$$

We want to find another point $(u, v)$ which is formed at the second intersection point of line $L$ and curve $C$. The new point $(u, v)$ can be given by,

$$u = u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}, \quad v = v_0 - \frac{2amu_0 + 2bv_0m^2}{a + bm^2}.$$

To derive the above values of $u$ and $v$, we use the fact that $au_0^2 + bv_0^2 = e$.

We now want to intersect $C$, regarded as a "cylinder" in $uvw$-space, with the surface $cu^2 + dw^2 = f$.

$$dw^2 = f - c\left(u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}\right)^2$$

This above equation can be changed to Weierstrass from. If $w_0 = 0$, then fourth degree polynomial becomes a cubic polynomial, so the equation just obtained is easily put into Weierstrass form. The procedure of changing "square = degree four polynomial" into Weierstrass form requires a point satisfying thie equation.

Trying with an example, let us take

$$u^2 + v^2 = 2, \quad u^2 + 4w^2 = 5.$$

First, we parameterize the solutions of $u^2 + v^2 = 2$. Then, finding the values of $u, v$ in terms of slope $m$.
Substituting the values of $u, v$ in $u^2+4w^2 = 5$, with a little bit of manipulation, the formulas then change this curve to generalized Weierstrass equation

$$y^2 - xy + 2y = x^3 + \frac{7}{4}x^2 - 4x - 7.$$

## 2.6 The j-invariant

If we have 2 elliptic curves $E_1$ and $E_2$, we use the "j-invarinat" concept to check whether the 2 curves are isomorphic or not.
Let $E$ be the elliptic curve given by $y^2 = x^3+Ax+B$, where $A, B$ are elements of a filed $K$ of characteristic not 2 or 3. Let us consider

$$x_1 = \mu^2 x, \quad y_1 = \mu^2 y,$$

with $\mu \in \bar{K}^X$, then we obtain a new curve as

$$y_1^2 = x_1^3 + A_1 x_1 + B_1,$$

with

$$A_1 = \mu^4 A, \quad B_1 = \mu^6 B.$$

Now, we define the **j-invariant** of $E$ to be

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

We also define $\Delta$ as $\Delta = 4A^3 + 27B^2$. Thus, the j-invariant would be

$$j = j(E) = 1728\frac{4A^3}{\Delta}$$

### 2.6.1 Theorem

Let $y_1^2 = x_1^3 + A_1 x_1 + B_1$ and $y_2^2 = x_2^3 + A_2 x_2 + B_2$ be two elliptic curves with $j-$invariant $j_1$ and $j_2$, respectively. If $j_1 = j_2$, then there exists $\mu \neq 0$ in $\bar{K}$ (= algebraic closure of $K$) such that

$$A_2 = \mu^4 A_1, \quad B_2 = \mu^6 B_1$$

The transformation

$$x_2 = \mu^2 x_1, \quad y_2 = \mu^3 y_1$$

takes one equation to the other.

There are two special cases of $j$ that arise often:

- $j = 0$ : In this case, the elliptic curve $E$ has the form $y^2 = x^3 + B$.
- $j = 1728$ : In this case, the elliptic curve $E$ has the form $y^2 = x^3 + Ax$.

We say that the two elliptic curves $E_1$ and $E_2$ are isomorphic **iff** $j(E_1) = j(E_2)$

The j - invariant is a one dimensional space which parametrises Elliptic Curves. It is also called 'Coarse Moduli Space' of Elliptic Curves.

The curves with $j = 0$ and with $j = 1728$ have automorphisms (bijective group homomorphisms from the curve to itself). Note that the $j-$invariant tells us when two curves are isomorphic over an algebraically closed field. However, if working with a nonalgebraically closed field $K$, 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 $K$.

If two different elliptic curves defined over a field $K$ have the same $j-$invariant, then we say that the two curves are **twists** of each other. The $j$ is the $j-$invariant of

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}$$

when $j \neq 0, 1728$.

## 2.7 Elliptic Curves in Characteristic 2

Most of the time, we used the Weiertrass equation rather than the generalized Weierstrass equation. That is, all the given formulas given do not apply when the field $K$ has characteristic 2. For the generalized Weierstrass equation for an elliptic curve $E$:

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

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

$$x = a_1^2x_1 + (a_3/a_1), \quad y = a_1^3y_1 + a_1^{-3}(a_1^2a_4 + a_3^2)$$

changes the equation to the form

$$zy_1^2 + x_1y_1 = x_1^3 + a_2'x_1^2 + a_6'.$$

This above curve is nonsingular if and only if $a_6' \neq 0$. The $j-$invariant in this case is defined to be $1/a_6'$.

If $a_1 = 0$, we let $x = x_1 + a_2, y = y_2$ to obtain an equation of the form,

$$y_1^2 + a_3'y_1 = x_1^3 + a_4'x_1 + a_6'.$$

This above curve is nonsingular if and only if $a_3' \neq 0$. The $j-$invariant in this case is defined to be 0.

Making the equation homogeneous:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Now, set $z = 0$, therefore $\infty = (0 : 1 : 0)$ is the only poiny at infinity on $E$. A line $L$ through $(x_0, y_0)$ and $\infty$ is a vertical line $x = x_0$. If $(x_0, y_0)$ lies on $E$, then the other point of intersection of $L$ and $E$ is $x_0, -a_1x_0 - a_3 - y_0)$. Now we can descrive the addition of points.

## 2.8 Endomorphisms

By an **endomorphism** of $E$, we mean a homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$ 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 (quotients of polynomials) $R_1(x, y), R_2(x, y)$ with coefficients in $\bar{K}$ such that

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

for all $(x, y) \in E(\bar{K})$. Since $\alpha$ is a homomorphism, we have $\alpha(\infty) = \infty$.

We will also assume that $\alpha$ is nontrivial; that is, there exists some $(x, y)$ such that $\alpha(x, y) \neq \infty$. The trivial endomorphism that maps every point to $\infty$ will be denoted by 0.

**Example:**
Let $E$ be given by $y^2 = x^3 + Ax + B$ and let $\alpha(P) = 2P$. Then $\alpha$ is a homorphism and

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

where

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$
$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y.$$

Since $\alpha$ is a homomorphism given by rational functions it is an endomorphism of $E$. □

An endomorphism of a group, module, ring, vector space, etc. is a homomorphism from one object to itself (with surjectivity not required).

Let $R(x, y)$ be any ratioanl function. Since $y^2 = x^3 + Ax + B$ for all $(x, y) \in E(\bar{K})$, we can replace any even power of $y$ by a polynomial in $x$ and replace any odd power of $y$ by $y$ times a polynomial in $x$ and obtain a rational function that gives the same function as $R(x, y)$ on points on $E(\bar{K})$.

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

Also, we can rationalize the denominator with $p_3 - p_4 y$.

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

Consider an endomorphism given by

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)),$$

as above. Since $\alpha$ is a homomorphism,

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

This means that

$$R_1(x,-y) = R_1(x,y) \quad \text{and} \quad R_2(x,-y) = -R_2(x,y)$$

Therefore, we may assume that

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

with rational functions $r_1(x), r_2(x)$.

We write $r_1(x) = p(x)/q(x)$. 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; hence the rational functions defining $\alpha$ are defined.
We define the **degree** of $\alpha$ to be

$$\deg(\alpha) = \text{Max}\{\deg\, p(x), \deg\, q(x)\}$$

if $\alpha$ is nontrivial. 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. This is equivalent to saying that at least one of $p'(x)$ and $q'(x)$ is not identically zero.

**Example:**
Taking the same example as the previous one; where $\alpha(P) = 2P$. We have

$$R_1(x,y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$

after some algebraic manipulation, we get

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

here, $\deg(\alpha) = 4$. The polynomial $q'(x) = 4(3x^2 + A)$ is not zero (including in characteristic 3, since if $A = 0$, then $x^3 + B$ has multiple roots, contraty to assumption). Therefore $\alpha$ is separable. $\square$

An important example of an endomorphism is the **Frobenius map**.
Suppose $E$ is defined over the finite field $\mathbb{F}_q$. Let

$$\phi_q(x, y) = (x^q, y^q)$$

The Frobenius map $\phi_q$ plays a crucial role in the theory of elliptic curves over $\mathbb{F}_q$.

### 2.8.1 Lemma

Let $E$ be defined over $\mathbb{F}_q$. Then $\phi_q$ is an endomorphism of $E$ of degree $q$, and $\phi_q$ is not separable. $\square$

### 2.8.2 Proposition

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

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

Where $\mathrm{Ker}(\alpha)$ is the kernel of the homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$.
If $\alpha \neq$ is not separable, then

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

$\square$

### 2.8.3 Theorem

Let $E$ be an elliptic curve defined over a field $K$. Let $\alpha \neq 0$ be an endomorphism of $E$. Then $\alpha : E(\bar{K}) \to E(\bar{K})$ is surjective. $\square$

### 2.8.4 Lemma

Let $E$ be the elliptic curve $y^2 = x^3 + Ax + B$. Fix a point $(u, v)$ on $E$. Write

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

where $f(x, y)$ and $g(x, y)$ are rational functions of $x, y$ (coefficients depend on $(u, v)$) and $y$ is regarded as a function of $x$ satisfying $dy/dx = (3x^2 + A)/(2y)$. Then

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}.$$

. □

### 2.8.5 Lemma

Let $\alpha_1, \alpha_2, \alpha_3$ be nonzero endomorphism of an elliptic curve $E$ with $\alpha_1 + \alpha_2 = \alpha_3$. Write

$$\alpha_i(x,y) = (R_{\alpha_i(x)}, yS_{\alpha_i(x)}).$$

Suppose there are constants $c_{\alpha_1}, c_{\alpha_2}$ such that

$$\frac{R_{\alpha_1'(x)}}{S_{\alpha_1(x)}} = c_{\alpha_1}, \quad \frac{R_{\alpha_2'(x)}}{S_{\alpha_2(x)}} = c_{\alpha_2}.$$

Then,

$$\frac{R_{\alpha_3'(x)}}{S_{\alpha_3(x)}} = c_{\alpha_1} + c_{\alpha_2}.$$

□

### 2.8.6 Proposition

Let $E$ be an elliptic curve defined over a field $K$, and let $n$ be a nonzero integer. Suppose that multiplication by $n$ on $E$ is given by

$$n(x,y) = (R_n(x), yS_n(x))$$

for all $(x,y) \in E(\bar{K})$, where $R_n$ and $S_n$ are rational functions. Then,

$$\frac{R_n'(x)}{S_n'(x)} = n.$$

Therefore, multiplication by $n$ is separable if and only if $n$ is not a multiple of the characteristic $p$ of the field. □

### 2.8.7 Proposition

Let $E$ be an elliptic curve over $\mathbb{F}_q$, where $q$ is a power of the prime $p$. Let $r$ and $s$ be integers, both not 0. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid q$. □

## 2.9 Singular Curves

Till now, we have discussed elliptic curves of an equation $y^2 = x^3 + Ax + B$ under the assumption of distinct roots. But what if, they have multiple roots. It will turn out that elliptic curve addition becomes either addition of elements of $K$ or multiplication of elements in $K^X$ or in a quadratic extension of $K$. Also, singular curves arise naturally when elliptic curves defined over the integers are reduced modulo various primes.

**First**, let us take the case where $y^2 = x^3 + Ax + B$ has a triple root at $x = 0$, so the curve has the equation $y^2 = x^3$.

The point $(0, 0)$ is the only singular point on the curve. Since any line through this point intersects the curve in at most one other point, $(0, 0)$ causes problems if we try to include it in our group. Thus, we remove this point from our group and denote it with $E_{ns}(K)$, with the group law defined in the same manner as when the cubic has distinct roots.

The only thing that needs to be checked is that the sum of two points cannot be $(0, 0)$. But since a line through $(0, 0)$ has at most one other intersection point with the curve, a line through two nonsingular points cannot pass through $(0, 0)$).

### 2.9.1 Theorem

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

$$E_{ns}(K) \to K, \quad (x, y) \mapsto \frac{x}{y}, \quad \infty \mapsto 0.$$

is group isomorphism between $E_{ns}(K)$ and $K$, regarded as an additive group. □

**Second**, we now consider the case where $x^3 + Ax + B$ has a double root. Thus, the elliptic curve $E$ has the equation $y^2 = x^2(x + a)$, for some $a \neq 0$. The point $(0, 0)$ is the only singularity here as well. Let $E_{ns}(K)$ be the nonsingular points on $E$ with coordinates in $K$, including the point $\infty$. let $\alpha^2 = a$ (so $\alpha$ might lie in an extension of $K$).
The new equation can be rewritten as

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

When $x$ is near 0, the right side of this equation is approximately $a$. Therefore, $E$ is approximated by $(y/x)^2 = a$, or $y/x = \pm\alpha$ near $x = 0$.
This means that the two "tangents" to $E$ at $(0, 0)$ are

$$y = \alpha x \quad \text{and} \quad y = -\alpha x$$

### 2.9.2 Theorem

let $E$ be the curve $y^2 = x^2(x + a)$ with $0 \neq a \in K$. Let $E_{ns}(K)$ be the nonsingular points on $E$ with coordinates in $K$. Let $\alpha^2 = a$. Consider the map

$$\psi : (x, y) \mapsto \frac{y + \alpha x}{y - \alpha x}, \quad \infty \mapsto 1.$$

1. If $\alpha \in K$, then $\psi$ gives an isomorphism from $E_{ns}(K)$ to $K^X$, considered as a multiplicative group.
2. If $\alpha \notin K$, then $\psi$ gives as isomorphism

   $$E_{ns}(K) \simeq \{u + \alpha v \mid u, v \in K, u^2 - av^2 = 1\},$$

   where the right hand side is a group under multiplication.

□

There are few situations where the above singular curves arise naturally, it's when working with curves with integral coefficients and reducing modulo various primes. For example, let $E$ be $y^2 = x(x - 35)(x - 55)$. Then we have

$$E \bmod 5\text{: } y^2 \equiv x^3,$$
$$E \bmod 7\text{: } y^2 \equiv x^2(x + 1),$$
$$E \bmod 11\text{: } y^2 \equiv x^2(x + 2).$$

The first case is treated and called **additive reduction**. The second case is split multiplicative reduction. And in the third case, $\alpha \notin \mathbb{F}_{11}$, so we are in the situation of the last discussed theorem. This is called **nonsplit multiplicative reduction**. For all primes $p \geq 13$, the cubic polynomial has distinct roots mod $p$, so $E$ mod $p$ is nonsingular. This situation is called **good reduction**.

## 2.10 Elliptic Curves mod n

Sometimes, we need to work with elliptic curves mod $n$, where $n$ is composite. Sometimes, it also takes elliptic curves over $\mathbb{Q}$ and reduces them to mod $n$, where $n$ is an integer.

**Example**

Let $E$ be given by

$$y^2 = x^3 - x + 1 \pmod{5^2}.$$

Let us take that, we want to compute the sum of $(1,1)+(21,4)$. Now, we can see that the slope of the line passing through these 2 points is $3/20$. Here, the denominator is not zero mod 25, but it is also not invertible. Therefore, the slope is neither infinite nor finite mod 25. If we compute the sum using the formulas for the group law, the $x-$coordinate of the sum is

$$\left(\frac{3}{20}\right)^2 - 1 - 21 \equiv \pmod{25}.$$

But $(1,1)+(1,24)=\infty$, so we cannot also have $(1,1)+(21,4)=\infty$. □

**Example**

Let $E$ be given by

$$y^2 = x^3 - x + 1 \pmod{35}.$$

Let us take that, we want to compute the sum of $(1,1)+(26,24)$. Now, we can see that the slope of the line passing through these 2 points is $23/25$, which is infinite mod 5 but finite mod 7. Therefore, the formulas for the sum yield a point that is $\infty$ mod 5 but is finite mod 7. That is, the point is partially at $\infty$. It is not possible to express it in affine coordinates mod 35. Nevertheless, we can use CRT (Chinese Remainder Theorem) as a remedy for this.

$$E(\mathbb{Z}_{35}) = E(\mathbb{Z}_5) \oplus E(\mathbb{Z}_7)$$

and the work mod and mod 7 separately. This is one of the optimal way to proceed further in such cases. □

**Example**

Let $E$ be given by

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

over $\mathbb{Q}$ Suppose we want to compute

$$(1,1) + (\frac{571}{361}, \frac{16379}{6859}).$$

Since the two points are distinct, we compute the slope as usual. Now, consider $E$ mod 7. The two points are seen to be congruent mod 7, so the

line through them mod 7 is the tangent line. Therefore, the formula used to add the points mod 7 is different from the one used in $\mathbb{Q}$. Suppose we want to show that the reduction map from $E(\mathbb{Q})$ to $E(\mathbb{F}_7)$ is a homomorphism. At first, it would seem that it's obvious since we just take the formulas for the group law over $\mathbb{Q}$ and reduce them to mod 7. But the present example says that sometimes we are using different formulas over $\mathbb{Q}$ and mod 7. A careful analysis shows that this does not cause problems, but it should be clear that the reduction map is more subtle than one might guess. □

Thus, rings come to picture now.

### 2.10.1 Corollary

Let $n_1$ and $n_2$ be odd integers with $\gcd(n_1, n_2) = 1$. Let $E$ be an elliptic curve defined over $\mathbb{Z}_{n_1 n_2}$. Then there is a group isomorphism

$$E(\mathbb{Z}_{n_1 n_2}) \simeq E(\mathbb{Z}_{n_1}) \oplus E(\mathbb{Z}_{n_2}).$$

□

### 2.10.2 Corollary

Let $E$ be an elliptic curve over $\mathbb{Q}$ given by

$$y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$.
Let $n$ be a positive odd integer such that $\gcd(n, 4A^3 + 27B^2) = 1$. Represent the elements of $E(\mathbb{Q})$ as primitive triples $(x : y : z) \in \mathbf{P}^2(\mathbb{Z})$. The map

$$\begin{array}{rccc} \mathrm{red}_n : & E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Z}_n) \\ & (x : y : z) & \mapsto & (x : y : z) \pmod{n} \end{array}$$

is a group homomorphism. □

# 3 Chapter 3

# Torsion Points

The torsion points, namely those whose orders are finite, play an important role in the study of elliptic curves, One of the most important parts of this chapter is the Weil and Tate-Lichtenbaum pairings.

## 3.1 Torsion Points

Let $E$ be an elliptic curve defined over a field $K$. Let $n$ be a positive integer. Let us have

$$E[n] = \{P \in E(\bar{K}) \mid nP = \infty\}$$

Here, $\bar{K}$ is the algebraic closure of $K$. We emphasize that $E[n]$ contains points with coordinates in $\bar{K}$, not just in $K$.

We know that when the characteristic of $K$ is not 2, $E$ can be put in the form $y^2 =$ cubic, and it is easy to determine $E[2]$. Let us take $E$ as,

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with $e_1, e_2, e_3 \in \bar{K}$. A point $P$ satisfues $2P = \infty$ iff the tangent line at $P$ is vertical. Therefore,

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

As an abstract group, this is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

### 3.1.1 Proposition

Let $E$ be an elliptic curve over a field $K$. If the characteristic of $K$ is not 2, then

$$E[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

If the characteristic of $K$ is 2, then

$$E[2] \simeq 0 \text{ or } \mathbb{Z}_2.$$

□

Similarly, we can find $E[3], \ldots, E[n]$ as well. Generalizing this,

### 3.1.2 Theorem

Let $E$ be an elliptic curve over a field $K$ and let $n$ be a positive integer, If the characteristic of $K$ does not divide $n$, or is 0, then

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

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

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

□

An elliptic curve $E$ in characteristic $p$ is called ordinary if $E[p] \simeq \mathbb{Z}_p$. It is called supersingular if $E[p] \simeq 0$.

Each homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$ is represented by a $2 \times 2$ matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

**Example**

Let $E$ be the elliptic curve defined over $\mathbb{R}$ by $y^2 = x^3 - 2$, and let $n = 2$. Then,

$$E[2] = \{\infty, (2^{1/3}, 0), (\zeta 2^{1/3}, 0), (\zeta^2 2^{1/3}, 0)\},$$

where $\zeta$ is a nontrivial cube root of unity. Let

$$\beta_1 = (2^{1/3}, 0), \quad \beta_2 = (\zeta 2^{1/3}, 0).$$

Then we say that $\{\beta_1, \beta_2\}$ is a basis for $E[2]$, and $\beta_3 = (\zeta^2 2^{1/3}, 0) = \beta_1 + \beta_2$. Let $\alpha : E(C) \longrightarrow E(C)$ be complex conjugation: $\alpha(x, y) = (\bar{x}, \bar{y})$, where the bar denoted complex conjugation. It can be easily erified that $\alpha$ is a homomorphism. □

## 3.2 Division Polynomials

The main goal of this section is to prove the 3.1.2 Theorem, mathematically.

## 3.3 The Weil Pairing

The Weil Pairing on the $n$-torsion on an elliptic curve is a major tool in studying elliptic curves. It is also used to attack the discrete logarithm problem for elliptic curves.

Let $E$ be an elliptic curve over a field $K$ and let $n$ be an integer not divisible by the characteristic of $K$. Then $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Let

$$\mu_n = \{x \in \bar{K} \mid x^n = 1\}$$

be the group of $n$th roots of unity in $\bar{K}$. Since the characteristic of $K$ does not divide $n$, the equation $x^n = 1$ has no multiple roots, hence has $n$ roots in $\bar{K}$. Therefore, $\mu_n$ is a cyclic group of order $n$. And, any generator $\zeta$ of $\mu_n$ is called a **primitive $n$th root of unity**. This is equivalent to saying that $\zeta^k = 1$ iff $n$ divided $k$.

### 3.3.1 Theorem

Let $E$ be an elliptic curve defined over a field $K$ and let $n$ be a positive integer. Assume that the characteristic of $K$ doesn't divide $n$.

Then, there is a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

called the **Weil pairing**, that satisfies the following properties:

1. $e_n$ is bilinear is each variable
   (a function combining elements of two vector spaces to yield an element of a third vector space.

   $$e_n(S_1 + S_2, T) = e_n(S_1, T)e_N(S_2, T)$$

   and

   $$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. $e_n$ is nondegenerate in each variable.

   $$\text{if } e_n(S, T) = 1 \text{ for all } T \in E[n], \text{ then } S = \infty$$

   $$\text{and}$$

   $$\text{if } e_n(S, T) = 1 \text{ for all } S \in E[n], \text{ then } T = \infty$$

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

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

5. $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for all automorphisms $\sigma$ of $\bar{K}$ such that $\sigma$ is the identity map on the coefficients of $E$. (if $E$ is the Weierstrass form, then $\sigma(A) = A, \sigma(B) = B$.

6. $e_n(\alpha(S), \alpha(T)) = e_n(s, T)^{deg(\alpha)}$ for all separable endomorphisms $\alpha$ of $E$.

The proofs of all the above properties will be proved in the later sections. □

### 3.3.2 Corollary

Let $\{T_1, T_2\}$ be a basis of $E[n]$. Then $e_n(T_1, T_2)$ is a primitive $n$th root of unity. □

### 3.3.3 Corollary

If $E[n] \subseteq E(K)$, then $\mu_n \subset K$.
That is, points in $E[n]$ are allowed to have coordinates in $\bar{K}$. The hypotheses of the corollary is that these points all have coordinates in $K$.□

### 3.3.4 Corollary

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E[n] \nsubseteq E(\mathbb{Q})$ for $n \geq 3$.
That is, if $E[n] \subseteq E(\mathbb{Q})$, then $\mu_n \subset \mathbb{Q}$, which is not the case when $n \geq 3$. □
**Example**

When $n = 2$, it is possible to have $E[2] \subseteq E(\mathbb{Q})$. If $E$ is givenby $y^2 = x(x-1)(x+1)$, then

$$E[2] = \{\infty, (0,0), (1,0), (-1,0)\}.$$

If $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$, there are elliptic curves $E$ defined over $\mathbb{Q}$ that have points or order $n$ with rational coordinates. However, the corollary says that it is not possible for all points of order $n$ to have rational coordinates for these $n$.

### 3.3.5 Proposition

Let $\alpha$ be an edomorphism of an elliptic curve $E$ defined over a field $K$. Let $n$ be a positive integer not divisible by the characteristic of $K$. Then,

$$\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$$

□

Let $\alpha$ and $\beta$ be edomorphisms of $E$ and let $a, b$ be integers. The endomorphisms $a\alpha + b\beta$ is defined by

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Here, $a\alpha(P)$ means multiplication on $E$ of $\alpha(P)$ by the integer $a$. The result is added in $E$ to $b\beta(P)$. 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.

### 3.3.6 Proposition

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$$

□

## 3.4 The Tate-Lichtenbaum Pairing

From the Weil pairing, we can also defince a pairing that can be used in case where the full $n$-torsion is not avilable. Thus, cannpt apply the Weil pairing directly.

### 3.4.1 Theorem

Let $E$ be an elliptic curve over $\mathbb{F}_q$. Let $n$ be an integer such that $n \mid q-1$. Denote by $E(\mathbb{F}_q)[n]$ the elements of $E(\mathbb{F}_q)$ of order dividing $n$, and let $\mu_n = \{x \in \mathbb{F}_q \mid x^n = 1\}$. Let $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$ and choose $R \in E(\mathbb{F}_q)$ satisfying $nE = \mathbb{Q}$. Denote by $e_n$ the $n$th Weil pairing and by $\phi = \phi_q$ the $q$th power Frobenius endomorphism. Define

$$\tau(P, q) = e_n(P, R - \phi(R)).$$

Then

$$\tau_n : E(\mathbb{F}_q)]n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \longrightarrow \mu_n$$

is a well defined nondegenerate bilinear pairing. □

The pairing of the theorem is called the **modified Tate-Lichtenbaum pairing**. The original **Tate-Lichtenbaum pairing** is obtained by taking the $n$th root of $\tau_n$, thus obtaining a pairing,

$$\langle \cdot, \cdot \rangle : E(\mathbb{F}_q) \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \longrightarrow F_q^\times/(F_q^\times)^n.$$

The pairing $\tau_n$ is better suited for computations since it gives a definite answer, rather than a coset in $\mathbb{F}_q^\times$ mod $n$th powers. These pairings can be computed very fastly.

The term $\tau_n(P, q)$ should be written as $\tau_n(P, Q + nE(\mathbb{F}_q))$, since an element of $E(\mathbb{F}_q/nE(\mathbb{F}_q)$ has the form $Q + nE(\mathbb{F}_q)$.

The Tate-Lichtenbaum pairing can be used in some situations where the Weil pairing does not apply. The Weil pairing needs $E[n] \subseteq E(\mathbb{F}_q)$, that is, $\mu_n \subseteq F_q^\times$, by Corollary 3.3.3. The Tate-Lichtenbaum pairing required that $\mu_n \subseteq F_q^\times$, but only needs a point of order $n$, rather than all of $E[n]$, to be in $E(\mathbb{F}_q^\times)$.

# 4 Chapter 4

# Elliptic Curves over Finite Fields