Rational Points on Elliptic Curves

Shubham Mishra

A Thesis Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of Science

Department of Mathematics

May 2018

Declaration

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.

Shubham

(Signature)

SHUBHAM MISHRA

(Shubham Mishra)

MA16MSCST11016

(Roll No.)

Approval Sheet

This Thesis entitled Rational Points on Elliptic Curves by Shubham Mishra is approved for the degree of Master of Science from IIT Hyderabad

Ch.V.G.N. Kumar 09/05/18

(Dr. Narasimha Kumar) Adviser
Dept. of Mathematics
IITH

9/5/18

(Dr. C S Sastry) Faculty Adviser
Dept. of Mathematics
IITH

(Dr. J Balasubramaniam) H.O.D
Dept. of Mathematics
IITH

Acknowledgements

First of all i would like to thank my thesis advisor Dr. Ch VG Narasimha Kumar for guiding me throughout the project on "".He has been a constant source of inspiration and help.

Secondly I would like to thank my classmates and my seniors who have always been there for me whenever I had any doubts or other problems

Last but not least I would like to thank my parents who have guided me throughout my life and are my greatest source of motivation.

Abstract

The aim of this thesis is to define the Elliptic Curves and some of intresting properties of a special class of terms,namely,rational point of elliptic curve ,The properties of the rational pooint of curve is airthmetic ,and rational point on elliptic curve forms a finitely generated group structure group it will be done by using the chord-tangent group law of composition.After completing the the abelian group structure,so we look some elementary properties like for a given elliptic curve we find the torsion subgroup of that elliptic curves.and finally done the elliptic curve and their isomorphism.

Further, we study different families of elliptic curves which depend on different parameters. Moreover, we look at the reduction modulo p of an elliptic curve and infer the meaning of good and bad reduction of an elliptic curve. Lastly, the statement and proof of Mordell-Weil theorem is given.

The topics of the thesis are based on the book **Elliptic Curves** by **Dale Husemöller**. I have not added anything new, except making a few observations of my own.

This thesis may contain many errors. I am responsible for these errors as I did not get the thesis corrected on time.

Contents

Chapter 1

Rational Plane Curves

In this chapter, we describe the basics of rational plane curve and rational point on lines, conics and cubics viewed as a rational plane curves. We also study some intersection properties of a curve with tangents and after that we will define the projective plane.
Further, we define the set of rational points on cubic curves and the structure of this set aided by the Mordell's theorem which allow us to visualize the structure of the elliptic curves. Finally we discuss the curves of degree more than 3 and the real and complex points on elliptic curves.

1.1 Rational Lines in the Projective Plane

Definition 1.1.1. *An elliptic curve is viewed as a plane curve given by a non-singular cubic equation.*

In the case of rational plane curve C_f we have rational ,real and complex points $C_f(\mathbb{Q}) \subset C_f(\mathbb{R}) \subset C_f(\mathbb{C})$ or loci.

Definition 1.1.2. *The projective plane $\mathbb{P}_2$ is the set of all triples $w\colon x\colon y$,where w, x and y are not all the zero and the points $w\colon x\colon y = l\colon m\colon n$ provided there is a constant k with $l = kw$, $m = kx$, $n = ky$ as with the affine plane and plane curves we have three basic cases $\mathbb{P}_2(\mathbb{Q}) \subset \mathbb{P}_2(\mathbb{R}) \subset \mathbb{P}_2(\mathbb{C})$ Consisting of all triples proportional to $w\colon x\colon y$, where $x, y, w \in \mathbb{Q}$ for $\mathbb{P}_2(\mathbb{Q})$ similarly for $\mathbb{R}$ and $\mathbb{C}$*

Remark 1.1.3. *A line C_f in $\mathbb{P}_2$ locus of all the $w\colon x\colon y$ satisfying the equation $F(w, x, y) = aw + bx + cy = 0$.The line at infinity L_∞ is given by the the equation w=0.*

Remark 1.1.4. *Two distinct point P and Q in $\mathbb{P}_2(\mathbb{C})$ lie on a unique line L in the projective plane,and, further ,if P and Q are the rational points, then the line L is rational. Two distinct lines L and Q in $\mathbb{P}_2(\mathbb{C})$ intersects at a unique point P, and , further,if L and Q are the rational lines, then the intersection point P is the rational.*

Definition 1.1.5. *A rational plane curve in $\mathbb{P}_2$ is of the form*

$$C_F = \{(w\colon x\colon y) \in \mathbb{P}_2 | F(w, x, y) = 0\}$$

F is a polynomial with rational coefficient and we have

$$C_f(\mathbb{Q}) \subset C_f(\mathbb{R}) \subset C_f(\mathbb{C})$$

1.2 Rational Points on Conics

Now here the rational point of plane curve of degree 2 which in x, y- coordinates are given by the equation

$$0 = f(x, y) = a + bx + cy + dx^2 + exy + fy^2$$

and in the homogeneous form in projective space as

$$0 = F(w, x, y) = aw^2 + bwx + cwy + dx^2 + exy + fy^2$$

and we observe that the these two polynomials are related by

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

and

$$F(w, x, y) = w^2 f(\frac{x}{w}, \frac{y}{w})$$

generally , if $f(x, y)$ has degree d then

$$F(w, x, y) = w^d f(\frac{x}{w}, \frac{y}{w})$$

i.e we divide w^2 in the homogeneous form of the equation then we get

$$0 = F(w, x, y) = w^2(a + b(\frac{x}{w}) + c(\frac{y}{w}) + d(\frac{x}{w})^2 + e(\frac{x}{w}\frac{y}{w}) + f(\frac{y}{w})^2)$$

implies that

$$w^2(a + bX + cY + dX^2 + eXY + fY^2) = 0$$

where $X = \dfrac{x}{w}$ and $Y = \dfrac{y}{w}$ $w^2 f(X, Y) = F(w, x, y)$

$$w^2 f(\frac{x}{w}, \frac{y}{w}) = F(w, x, y)$$

and in the general

$$F(w, x, y) = w^d f(\frac{x}{w}, \frac{y}{w})$$

Theorem 1.2.1 (Legendre's Theorem)**.** *For a conic $ax^2 + by^2 = w^2$ there exist $m \in \mathbb{N}$ such that*

$$ax^2 + by^2 = w^2$$

has an integral solution if and only if the congruence

$$ax^2 + by^2 \equiv w^2 \pmod{m}$$

has a solution in the integer modulo m.

Theorem 1.2.2 (Hasse-Minkowski Theorem)**.** *A homogeneous quadratic equation in several variables is solvable by rational numbers, not all zeros, if and only if it is solvable in p-adic numbers for each prime p including the infinite prime. the p-adic numbers at the infinite primes are the real numbers.*

1.3 Pythagoras,Diophantus,and Fermat

The triples of whole numbers (a, b, c) satisfying the relation

$$c^2 = a^2 + b^2$$

are called the Pythagorean triples
if (a, b, c) is a Pythagorean triple, then any scalar multiple (ka, kb, kc) is also a Pythagorean triples
A pythagorean triples (a, b, c) is primitive Pythagorean triples if $\gcd(a, b, c) = 1$

Theorem 1.3.1. *Let m and n be two relatively prime natural numbers such that $n - m$ is positive and odd, then $(n^2 - m^2, 2mn, n^2 + m^2)$ is a primitive Pythagorean triple,further, each primitive Pythagorean triples is of the form some $m, n \in \mathbb{N}$.*

Proof. Consider the conic $x^2 + y^2 = 1$. Let $O = (-1, 0)$ and take any line which is not a tangent to the circle at O passing through O. suppose this line intersects the $y - axis$ at $(0, t)$ and the circle at (x_t, y_t). Equation of L_t, the line passing through $(-1, 0)$ and $(0, t)$ is $y = t(x + 1)$. Now, this line intersects the conic at (x_t, y_t). We get, $x_t^2 + y_t^2 = 1$. Substituting the value of y, we have, $x_t^2 + t^2(x_t + 1)^2 = 1$. By solving the quadratic equation in x_t gives the value of x_t as $\frac{1-t^2}{1+t^2}$. Thus, $y_t = \frac{2t}{1+t^2}$. Thus if t is rational, then (x_t, y_t) is also rational.

let $(a : b : c)$ be a Pythagorean triples.and then we show that there exists m, n such that $n - m > 0$ and m, n are relatively prime, satisfying

$$a = n^2 - m^2$$
$$b = 2mn$$
$$c = m^2 + n^2$$

Since $t \leq 1$, for any $n > m$, where m, n are relatively prime, $\frac{m}{n} < 1$.
Choose $t = \frac{m}{n}$,then we get a point (x_t, y_t) on the circle, which is as,

$$x_t = \frac{1 - \frac{m^2}{n^2}}{1 + \frac{m^2}{n^2}} = \frac{n^2 - m^2}{n^2 + m^2}$$

and

$$y_t = \frac{2(\frac{m}{n})}{1+\frac{m^2}{n^2}} = \frac{2mn}{n^2+m^2}$$

So (a, b, c) is a Pythagorean triple, we have, $a^2 + b^2 = c^2$. Dividing by c^2 on both sides, then we get $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$. Note that any for any Pythagorean triple, we can divide it by c^2 so that the point $(\frac{a}{c}, \frac{b}{c})$ lies on the circle $x^2 + y^2 = 1$. Thus the point $(\frac{a}{c}, \frac{b}{c})$ lies on the circle $x^2 + y^2 = 1$. Since every point on the circle is of the form (x_t, y_t), comparing (x_t, y_t) with $(\frac{a}{c}, \frac{b}{c})$, we get,

$$a = n^2 - m^2$$
$$b = 2mn$$
$$c = n^2 + m^2$$

and each Pythagorean triple can be obtained using these values of m and n.

□

Definition 1.3.2 (Fermat's curve $\mathbb{F}_n$ of order n)**.** *The Fermat's curve of order n is given by the equation in x,y- coordinates*

$$x^n + y^n = 1$$

,
or in the projective coordinates by

$$x^n + y^n = w^n.$$

1.4 Fermat's Last Theorem

The only rational points on $\mathbb{F}_n$ lie on the x-axis and y-axis for $n \geqslant 3$
For $n = 2$, the number of rational points on
F_2 are infinitely many. i.e it is of the form $(\frac{a}{c}, \frac{b}{c})$, where the a, b, c forms a Pythagorean triples.

Proposition

For a square-free integers $\mathbb{K}$ there is a bijective correspondence between the following three sets.

1. $A = \{(a, b, c) \quad | \quad a^2 + b^2 = c^2, a < b < c, \mathbb{K} = \frac{1}{2}ab\}$
2. Rational number x, where x+$\mathbb{K}$ and x-$\mathbb{K}$ are squares
3. rational points (x, y) on the cubic $y^2 = x^3 - \mathbb{K}^2 x$ such that x is a square of rational number and denominator of x is even.

1.5 Rational Cubics

The cubics comes up two places first there is a Fermat's cubic $x^3 + y^3 = 1$ which Euler showed that it has only two rational points $(1, 0)$ and $(0, 1)$ and there is a cubic $y^2 = x^3 - \mathbb{K}^2 x$ whose rational

points tells about the existence of right rational triangles of area K.
The rational cubics in projective coordinates is given by

$$F(w,x,y) = c_1w^3 + c_2x^3 + c_3y^3 + c_4w^2x + c_5wx^2 + c_6x^2y + c_7xy^2 + c_8w^2y + c_9wy^2 + c_{10}wxy = 0$$

,
the coefficient are determined only up to a non zero constant multiple , and,hence, the cubic is given by

$$c_1 : c_2 : c_3 : c_4 : c_5 : c_6 : c_7 : c_8 : c_9 : c_{10}$$

.
a point in a nine dimensional projective space.
Intersection of line and the cubics.
Let C be a rational cubic and L be a rational line. if the line intersects the cubic at 3 points in which two of them are rational then third point of intersection is also a rational point.

Proof. Let

$$F(w,x,y) = 0.$$

be a rational cubics and the line

$$L(w,x,y) = aw + bx + cy = 0$$

. be a rational line for the line $aw + bx + cy = 0$ we eliminate the value of y.
so the value of $y = -\dfrac{aw+bx}{c}$.
substitute the value of y in the cubic then we get the equation in x and w.
for the line at infinity , $w = 0$, we get the cubic in x i.e cubic polynomial in x.
from this we get the value of x and put the value of x in the $y = -\dfrac{aw+bx}{c}$
and the line at infinity $w = 0$
then we get the (x, y).
thus (x, y) will be the rational point if and only if x is rational.
If two root of a cubic polynomial are rational then third one is also rational.

□

Remark 1.5.1. *If two of the three intersection point of a rational cubics with a rational line are the rational points, then the third point is rational.*

Definition 1.5.2 (Irreducible cubic)**.** *A irreducible cubic is one whose equation cannot be factored over the complex number.*

Definition 1.5.3 (Singular point on a cubic C)**.** *A point O on an irreducible cubic C is called a singular point provided each line through O intersects C at only one other point.*

Definition 1.5.4 (Nonsingular cubic)**.** *An irreducible cubic without a singular point is called Non-singular cubic curve.*

Definition 1.5.5 (Singular cubic)**.** *An irreducible cubic with a singular point is called a singular cubic curve.*

Rational points on cubics

We describe rational points on the reducible and singular cubics, which is same as to describe the rational point on the conics,and then, we describing the rational points on non-singular cubics.
Case 1-[Cubic is singular]
we consider the cubic with singular rational point O.
Let C be a singular cubic. and O be a singular point on the cubic C then each rational L through O cuts the cubic at any other point, say P, and P is rational because its x-coordinate is the solution of a cubic equation in x or in y with a double rational root corresponding to the x or y coordinate of O.
Case 2- [cubic is nonsingular]
we consider the cubic the cubic is non-singular
Let P and Q be any two rational point on the cubic. and let L be the line passing through P and Q clearly L is a rational line.
i.e if we draw the line connecting the two points P and Q. This is a rational line L since P and Q are rational, and this line meet the cubic at one more point, say PQ which must be rational by the intersection result of line and cubic.
even if we have only rational point say P. we can still find another and consider the line M tangent to that point i.e we join the point itself
Then tangent line M intersects the cubic "twice" at P and the intersection point is rational say "PP".

1.6 Primitive Form of Mordell's Theorem

For any nonsingular rational cubic curve C. there exist a finite set M of rational points on the curve C are generated using the iterates of the chord-tangent law of composition.
i.e if M is a finite set of rational points on the nonsingular rational cubic such that every rational point P can be decomposed in the form

$$P = (....((P_1P_2)P_3)...P_r)$$

where $P_1, ...P_r$ are in the finite set M.

Chord Tangent Composition Law

If P and Q be two rational points on the cubic. then the function that associates P and Q to the rational point PQ where PQ is the third intersection point of P and Q for the line and the cubic, is called as the chord tangent composition law.
Note− The chord-tangent composition law is not a group law, because, there is no identity element i.e an element 1 with $1P = P = P1$ for all P.and however it satisfy a commutative law property $PQ = QP$.

1.7 The Group Law on Cubic curves

The chord tangent composition law is not a group law because there is no identity element. but with a choice of rational point O as zero element (identity element O) we define the group law $P+Q$ by the relation.

$$P+Q=O(PQ)$$

it means $P+Q$ is the third intersection point of line through O and PQ.

(1)CLOSURE-

$$P+Q=O(PQ)$$

$P+Q$ is the third intersection point on the line through O and PQ meet the cubic which is again a rational point, thus, the group law is closed with respect to the addition

(2) EXISTENCE OF IDENTITY-

The point O is the identity on a rational point on the cubic, whose coordinates in projective planes is given by $(x,y,w)=(0,1,0)$, and its also called as point at infinity.

$$P+O=O(PO)=O+P=O(OP)=P$$

where P is the rational point on the cubic.

(3) EXISTENCE OF INVERSE-

To find $-P$ given P we use the tangent line to the cubic at O ant its third intersection point OO.

$$P+(-P)=O(OO)=O$$

(4) COMMUTATIVITY-

Line through P and Q is same as the line through Q and P .thus, the point of intersection of the line and the cubic is the same i.e we consider $O(PQ)$ and $O(QP)$ then we get

$$P+O=O(PO)=P$$

, and

$$O+P=O(OP)=P$$

Definition 1.7.1 (Elliptic curve over a field k)**.** *An elliptic curve E over the field k is a nonsingular cubic curve E over k together with a point O in $E(k)$.*
The group law on $E(k)$ is defined by O and the chord tangent law of composition PQ is defined by $P+Q=O(PQ)$

Theorem 1.7.2. ***(Mordell)***-
On a rational elliptic curve $E(Q)$ the group of rational point is a finitely generated abelian group.

Remark 1.7.3. *The structure theorem for finitely generated abelian group applied to $E(Q)$ to obtain a decomposition*

$$E(Q) = Z_g \oplus E(\mathbb{Q})_{tor}$$

where g is Natural number called the rank of E. and $E(\mathbb{Q})_{tor}$ is a finite abelian group consisting of all the element of the finite order in $E(Q)$.
Mazur proved that the torsion subgroup is either a cyclic group or a direct sum of a cyclic group. which is stated in following theorem.

Theorem 1.7.4 (Mazur)**.** *Let E be an elliptic defined over Q i.e $E(Q)$ and Tors $E(Q)$ be the group of all torsion points is isomorphic to either*

$$\mathbb{Z}/m\mathbb{Z} \qquad for \qquad m = 1, 2, 3, ..., 10, 12$$

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad for \qquad m = 2, 4, 6, or \quad 8$$

Remark 1.7.5. *Let E be an elliptic curve defined over the $\mathbb{Q}$ by the equation $y^2 = x^3 + ax + b$. there is no any way to to determine the rank of E by using these two coefficient a and b.in fact, there is no any other way to determining the whether or not $E(\mathbb{Q})$ is finite. and $E(\mathbb{Q})$ is finite if and only if the rank of g is zero.*

Theorem 1.7.6 (**Birch,Swinnerton-Dyer Conjecture**)**.** *The rank g of an elliptic curve E defined over the rational numbers $\mathbb{Q}$ is equal to the order of the zero of $L_E(s)$ at $s = 1$.*

1.8 Mordell Conjecture for plane curve

Let C be a smooth rational plane curve of degree strictly greater than 3. then the set $C(\mathbb{Q})$ of rational point on a cubic C is finite.

Genus of the curve

Let $X(\mathbb{C})$ be an algebraic curve defined over the complex number $\mathbb{C}$,topologically, $X(\mathbb{C})$ is a closed oriented surface with g holes.

Definition 1.8.1 (**Genus**)**.** *The invariant g is called the genus of the curve.*
Lines and Conic have genus $g = 0$
singular cubic have genus $g = 0$
Nonsingular cubic have genus $g = 1$

Note- A nonsingular plane curve of degree d has genus.

$$g = \frac{(d-2)(d-1)}{2}$$

Theorem 1.8.2 (**Siegel**). *The number of integral point on a nonsingular rational curve of genus strictly greater than 0 and is finite.*

Note- this applies to a nonsingular cubic curves, but not to the singular cubic
for eg. $y^2 = x^3$ it has infinitely many integral points of the form (n^2, n^3), where n is any integer.

1.9 Real and Complex Point on Elliptic Curve

Let E be an elliptic curve defined over the the real $\mathbb{R}$ or complex $\mathbb{C}$ numbers. the structure of $E(\mathbb{R})$ and $E(\mathbb{C})$ is continuous or Lie group structure.

Definition 1.9.1 (**Lie group**). *A lie group is a finite dimensional smooth manifold together with group structure on G such that the multiplication $G \times G \longrightarrow G$ and the attaching of an inverse $g \longrightarrow g^{-1}$ are the smooth maps.*
the product of twp lie group or a finite sequence of lie group is a lie group.

Note- An abelian, compact and connected Lie group is isomorphic to a product of circle.
COMPACTNESS
Consider the real projective projective plane $\mathbb{P}_2(\mathbb{R})$ then we have
(1)– $\mathbb{P}_2(\mathbb{R})$ is the quotient of two sphere S^2 in $\mathbb{R}^3$.
(2)– $\mathbb{P}_2(\mathbb{C})$ is the quotient of five sphere S^5 in $\mathbb{C}^3$.
CONNECTEDNESS
For an elliptic curve given by the equation in normal form.

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

right hand side is the cubic polynomial and it is denoted by $f(x)$

$$f(x) = x^3 + a_2x^2 + a_4x + a_6$$

is a cubic polynomial and so by completing the square

$$(y + \frac{a_1x + a_3}{2})^2 = f^*(x)$$

where $f^*(x)$ is another cubic polynomial, Now we see that the graph of this equation for real coefficient is symmetric around the line $2y + a_1x + a_3 = 0$ and for the real coefficient has two forms.
In the case of one real root, the group $E(\mathbb{R})$ has one connected component.
And in the case of three real root the group $E(\mathbb{R})$ has two connected component.

Proposition 1-
Let E be an elliptic curve defined by $(y + ax + b)^2 = g(x)$
where $g(x)$ is a cubic polynomial over $\mathbb{R}$,
(1)– If $g(x)$ has only one root then $E(\mathbb{R})$ is isomorphic to the circle.

(2)− if $g(x)$ has three real root then $E(\mathbb{R})$ is isomorphic to direct sum of circle and $\mathbb{Z}/2\mathbb{Z}$.

Proposition 2-
Let E be an elliptic curve defined by $(y + ax + b)^2 = g(x)$.
where $g(x)$ is a cubic polynomial over $\mathbb{C}$, then $E(\mathbb{C})$ is isomorphic to the direct sum of two circles.

Remark 1.9.2. *The finite subgroup of $E(R)$ are of the form a cyclic group or a cyclic group direct sum with he group of order 2.*

$$E(\mathbb{R}) \cong \mathbb{Z}/n\mathbb{Z}$$

$$E(R) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Chapter 2

Chord-tangent Computational Method on Normal Cubic Curve

In this chapter we show how, by using simple analytic geometry, and a large number of numerical calculation are possible with the group law on cubic curve.we define the normal form of cubic curve without the terms x^2y , xy^2, or y^3. and defining the sum of the two rational points by using the group law.and finally we define the group law on singular cubics.

2.1 Computation on Normal Cubic Curve

A cubic equation in normal form, or general Weierstrass form, is an expression

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

where the coefficients $a_i$are in the in the fields $\mathbb{K}$.
So term of y^3 in the above equation,a vertical line $x = x_0$ intersects the the locus of the normal cubic at two points (x_0, y_1) and (x_0, y_2), where y_1 and y_2 are the roots of the quadratic equation.

$$y^2 + a_1x_0y + a_3y - x_0^3 - a_2x_0^4 - a_4x_0 - a_6 = 0$$

we can write the above equation

$$y^2 + (a_1x_0 + a_3)y - (x_0^3 + a_2x_0^4 + a_4x_0 + a_6) = 0$$

in the completed plane,that is, the projective plane, we see that the equation in normal form has one more solution at infinity which we call as O, and the O is the third intersection point of the locus of the vertical line with the locus of the cubic equation in normal form in projective plane.

Definition 2.1.1. *The elliptic curve for the cubic equation in normal form is the locus of all solution $(x, y) \in k^2$ of the equation*

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

with the point O which is on every vertical line.

Remark 2.1.2. *Let E be an elliptic curve defined by an equation in normal form. if $P = (x, y)$ is a point on a curve then the negative $-P$ is $(x, y*)$,where*

$$y + y* = -a_1x - a_3$$

or, we can say that,

$$-(x, y) = (x, -y - a_1x - a_3)$$

Observe that the point O , (x, y) ,and $(x, y*)$ are the points of intersection of the vertical line through $(x, 0)$ with the curve E over the field k i.e $E(k)$
so for the equation

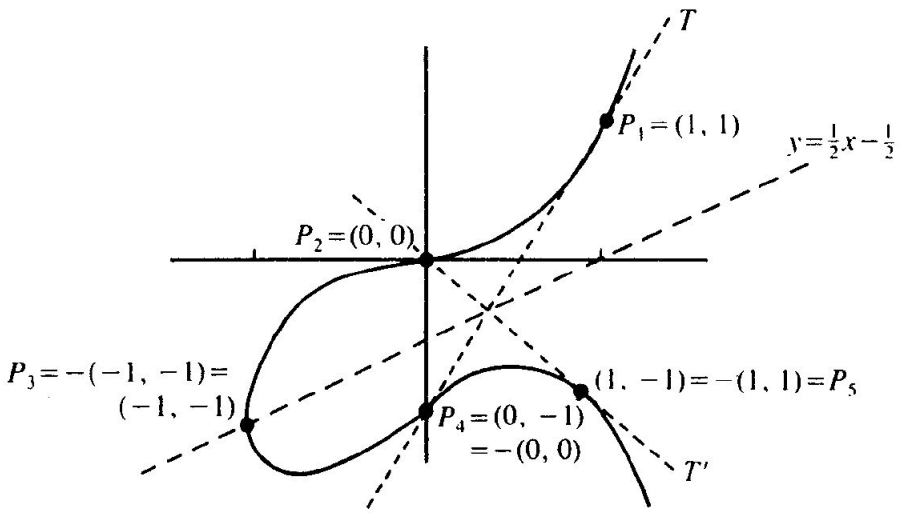
$$y^2 + (a_1x_0 + a_3)y - (x_0^3 + a_2x_0^4 + a_4x_0 + a_6) = 0$$

. y and $y*$ are the two roots of the quadratic equation over k. Where the sum of the roots are $-(a_1x + a_3)$ in k and so, if y is in k, then $y*$ is also is in the k.
and the curve has a reflection symmetry with respect to the line $y = \dfrac{-a_1x + a_3}{2}$ in the plane.

Example-1: For E given by the equation

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

we have $-(x, y) = (x, -y - 1 + x)$ and the curve is vertically symmetric about the line $y = \dfrac{x - 1}{2}$



In the curve the two tangent line to the curve T at $(1, 1)$ and and T' at $(1, -1)$ which have slopes coming from the implicit differentiation of the equation of the curve.
i.e

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

,
differentiating both side we get

$$2yy' + y' - xy' - y = 3x^2$$

$$(2y + 1 - x)y' = 3x^2 + y$$

,
Note- let E be an elliptic curve defined by the equation in normal form.

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

.
if we add two point $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. we first draw the line through P_1 and P_2 and the third intersection point is $P_1P_2 = (x_3, y_3)$ and

$$P_1 + P_2 = -P_1P_2$$

.
Case 1- if $x_1 \neq x_2$, so that $P_1 \neq P_2$ then the line through P_1 and P_2 has an equation $y = \lambda x + \beta$ where

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

Case 2- if $x_1 = x_2$ but $P_1 \neq P_2$ then the line through P_1 and P_2 is the vertical line $x = x_1$ and $P_2 = -P_1$
Case 3- if $P_1 = P_2$ then the tangent line through P_1 has the equation $y = \lambda x + \beta$ where

$$\lambda = \frac{f'(x_1) - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

since $(2y + a_1x + a_3)y' = f'(x) - a_1y$
we put the value of y into the normal form of the cubic equation then we get

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

the three root of this cubic are x_1, x_2,and x_3
the x coordinate of the three intersection point is either P_1 , P_2 and P_1P_2 for the Case1 and P_1 , P_1 and P_1P_1 for the Case3
Now the sum of the root of the cubic equation is

$$x_1 + x_2 + x_3 = -\frac{\text{coefficient of } x^2}{\text{coefficient of } x^3}$$

so

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

for the case 1.

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

for the case 3. finally,

$$(x_1, y_1) + (x_2, y_2) = (x_3, -y_3 - a_1 x_3 - a_3)$$

for the case 1. and

$$2(x_1, y_1) = (x_3, -y_3 - a_1 x_3 - a_3)$$

for the case 3.

Example-2: The Elliptic curve E: $y^2 + y - xy = x^3$ find $-P$. for any P=(x, y)

let P=(x, y) be any point of the elliptic curve E then we have to find the -P of that curve
$-P = (x, -y - a_1 x - a_3)$
for the given Elliptic curve the coefficient $a_1 = -1$ and $a_3 = 1$ then $-P = (x, -y + x + 1)$.

Example-3: The elliptic curve E: $y^2 + y - xy = x^3$ find the group generated by the point $P = (1, 1)$
given $P = (1, 1)$

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

$$2yy' + y' - xy' - y = 3x^2$$

$$(2y + 1 - x)y' = 3x^2 + y$$

$$y' = \frac{3x^2 + y}{2y + 1 - x}$$

where y' is the slope of the tangent.
at the point $(1, 1)$ the value of y' is 2, and the equation of the tangent at the point $(1, !)$ is

$$y - 1 = 2(x - 1)$$

i.e $y = 2x - 1$
Put the value of y in the equation of the elliptic curve then we get

$$(2x - 1)^2 + (2x - 1) - x(2x - 1) = x^3$$

$$x(x - 1)^2 = 0$$

$x = 0$ or $x = 1$ and $y = -1$ or $y = 1$
so we get the two points $(1, 1)$ and $(0, -1)$, the point $(1, 1)$ is the same as the point P then we take the point $(0, -1)$,
since $PP = (0, -1)$
and $P + P = -PP$ or $2P = -PP$

and $-PP = -(0,-1) = (0,0)$
$2P = (0,0)$. Now , $3P = P + 2P = -(2P)P$
The equation of the line through P and $2P$ is $y = x$. Put the value of the y in the equation of the elliptic curve to get

$$x(x^2 - 1) = 0$$

Where $x = 0, 1, -1$ and $y = 0, 1, -1$. So we have three points which are $(0,0)$, $(1,1)$ and $(-1,-1)$. So the points $(0,0)$ and $(1,1)$ are same as the points P and 2P .We consider the third point $(-1,-1)$.
$(2P)P = (-1,-1)$ and $3P = P + 2P = -(2P)P = -(-1,-1) = (-1,-1)$
$3P = (-1,-1)$
Consider tangent at 3P.
$y' = 0$,there is a vertical tangent at 3P
$\implies 3P + 3P = O$
$\implies 2(3P) = O$
$\implies 6P = O$
here the point O is the point is the point at infinity and the identity of the Group $E(Q)$ so P is the point of order 6
In, particular $4P + 2P = O$

$$4P = -2P = -(0,0) = (0,-1)$$

and,

$$5P = -P = -(1,1) = (1,-1)$$

so the $\{P, 2P, 3P, 4P, 5P, 6P = 0\}$ forms a cyclic subgroup of order 6 in $E(Q)$.

2.2 Illustration of the elliptic curve group law

if $2 \neq 0$ in the field k i.e the characteristic of k is different from 2 then in the normal form.

$$y^2 + y(a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6$$

. We can complete the square on the left-hand side

$$y^2 + y(a_1x + a_3) + \frac{(a_1x + a_3)^2}{4} = (y + \frac{a_1x + a_3}{2})^2$$

Remark 2.2.1. *if the equation for E is $y^2 = f(x)$ is cubic polynomial then the negative of an element is given by $-(x,y) = (x,-y)$. furthermore the cubic will be non-singular if and only if $f(x)$ has no repeated root.*

Remark 2.2.2. *The point $(0,0)$ is on the curve $y^2 = f(x)$ if and only if equation has the form $y^2 = x^3 + ax^2 + bx$. if we take r is the root of $f(x)$ then $y^2 = f(x) + r$ as this form and we will use the equation of elliptic curve in this form. If the characteristic of k from 3, then in the special normal form $y^2 = f(x)$. we can complete the cube in right in the side and after translation of x by*

a constant. We have Weierstrass of the cubic

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

.

2.3 The curves with equation $y^2 = x^3 + ax$ and $y^2 = x^3 + a$

Torsion subgroup of $y^2 = x^3 + ax$

If we substitute u^2x for x and u^3y for y in the equation then we get
$(u^3y)^2 = (u^2x)^3 + a(u^2x)$
$u^6x^2 = u^6x^3 + au^2x$
$u^6x^2 = u^6(x^3 + \frac{ax}{u^4})$
So we conclude that a is non zero integer which is free of any fourth-power factor i.e a is fourth power free.

Theorem 2.3.1. *The torsion subgroup of $E(Q)$ is*

$$TorsE(Q) = \begin{cases} \frac{Z}{4Z} & a = 4 \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} & -a \text{ is a square} \\ \frac{\mathbb{Z}}{2\mathbb{Z}} & -a \text{ is not a square} \end{cases}$$

Proof. -Any point of order two has the form $(x, 0)$.
Slope of the tangent is $y' = \dfrac{3x^2 + a}{2y}$
Case 1-
Point of order two when a is a square
x-coordinate is the root of the cubic equation $0 = x^3 + ax$
From here we get $x(x^2 + a) = 0$ i.e $x = 0$ or $x^2 = -a$
in particular, there are three point of order two if and only if -a is a square say, $(0, 0)$ and
and which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
Case 2- Point of order 4
Consider the equation $2(x, y) = (0, 0)$ on $E(Q)$ then (x, y) is a point of order 4.
For such a point there would be a line L i.e $y = \lambda x$ through $(0, 0)$ and tangent to E at (x, y) Thus.

$$(\lambda x^2) = x^3 + ax$$

$x(x^2 - \lambda^2 x + a) = 0$
$x = 0, x^2 - \lambda^2 x + a = 0$
$x = 0$ and $y = 0$ is a point of P so we consider the quadratic equation
$x^2 - \lambda^2 x + a = 0$ the discriminant of the quadratic equation is $D = \lambda^4 - 4a$ for the solution to exist, $D \geq 0$.
Since $y = \lambda x$ is tangent to E at (x, y) , D=0
$\lambda^4 = 4a$

But we know that a is fourth power free.
$\lambda \iff a = 4 \iff \lambda = \pm 2$

Substitute the value of a and λ in the above quadratic equation,
$\implies (x-2)^2 = 0$
$\implies x = 2$
And $y = \lambda x = \pm 4$
in this case the points (x, y) satisfying $2(x, y) = 0$ are $(2, 4)$ and $(2, -4)$
The point of finite order forms the subgroup $O, (0, 0), (2, 4), (2, -4)$,which makes the torsion subgroup is isomorphic $\mathbb{Z}/4\mathbb{Z}$.

Case 3- When -a is not a square or $a \neq 4$ then the only solution to the quadratic equation is $x = 0$ and hence $y = 0$
So the torsion subgroup formed is $O, (0, 0)$ and which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$
Claim-we will show that there is no 3-torsion,
If there were such a point P, on $E(Q)$
$\implies 2P = -P$
So the tangent line $y = \lambda x + \beta$ to E at P when substituted into

$$(\lambda x + \beta)^2 = x^3 + ax$$

or

$$x^3 - \lambda^2 x^2 + (a - 2\beta\lambda)x - \beta^2 = 0$$

would be a perfect cube $(x - r)^3 = 0$ with r is the x-coordinate of P this would means that

$$3r = \lambda^2$$

$$r^3 = \beta^2$$

$$3r^2 = a - 2\beta\lambda$$

so we get the value of r and λ and finally

$$3(\frac{\lambda^4}{9}) = a - 2(\frac{\lambda^4}{3\sqrt{3}})$$

Which is impossible for a and λ are the rational numbers since $\sqrt{3}$ is irrational, which is a contradiction.
since there is no three torsion.

□

Torsion Subgroup for $y^2 = x^3 + a$

we substitute u^2x for x and u^3y for y in the equation then we get
$\implies (u^3y)^2 = (u^2x)^3 + a$
$\implies u^6x^2 = u^6x^3 + a$
$\implies u^6x^2 = u^6(x^3 + \frac{a}{u^6})$
so we conclude that a is non zero integer which is free of any six-power factor i.e a is six power free.

Theorem 2.3.2. *The torsion subgroup of $E(Q)$ is*

$$TorsE(Q) = \begin{cases} \frac{Z}{6Z} & a = 1 \\ \frac{\mathbb{Z}}{3\mathbb{Z}} & a \neq 1, \ a \text{ is a square or } a = -432 \\ \frac{\mathbb{Z}}{2\mathbb{Z}} & a \neq 1, \ a \text{ is not a square and } a \text{ is a cube} \\ O & a \neq 1, \ a \text{ is not a square, not a cube and } \neq -432 \end{cases}$$

Proof-
Case 1- A point of order 2.
A point of order 2 has the form $(x, 0)$.
Substituting $y = 0$ in the equation we get $x^3 + a = 0 \implies x^3 = -a$
This exist on E iff a is a cube of c^3 of some integer c .
$\implies a = c^3 \implies x = -a$
then $(-c, 0)$ is the point of order two
thus we get the torsion subgroup $O, (-c, 0)$, which is isomorphic to $\frac{Z}{2Z}$
we show that there is no point of order 4
Let if possible (x, y) is a point of order 4
$\implies 2(x, y) = (-c, 0)$
consider the tangent line $y = \lambda x + c$ through $(-c, 0)$ when substitute into the equation of the curve

$$\lambda^2(x + c)^2 = x^3 + c^3$$

or $\lambda^2(x + c) = x^2 - cx + c^2$
the line through $(-c, 0)$ is the tangent at another point (x, y) on E iff the quadratic equation has a double root

$$x^2 - (\lambda^2 + c)x + c(c - \lambda^2) = 0$$

that is the discriminant $D = 0$
$D = \lambda^4 + 2\lambda^2c + c^2 - 4c(c - \lambda^2) = 0$, After completing the square in this equation we get

$$(\lambda^2 + 3c)^2 = 12c^2$$

$$(\lambda^2 + 3c) = \pm 2\sqrt{3c}$$

There is no rational solutions of this equation because 12 is not a square but λ and c are rational.

Thus we get a contradiction.
Since there is no point of order 4 in E.

Case 2- Point of order 3 .
A point (x, y) of order 3 i.e, $2(x, y) = -(x, y)$ iff there is a line $y = \lambda x + \beta$ through (x, y) such that

$$(\lambda x + \beta)^2 = x^3 + a$$

is a perfect cube

$$(x - r)^3 = x^3 - \lambda^2 x^2 - 2\lambda\beta x + (a - \beta^2)$$

comparing the coefficient we get,

$$-3r = -\lambda^2$$

$$3r^2 = -2\lambda\beta$$

and

$$a - \beta^2 = -r^3$$

$\implies r = \dfrac{\lambda^2}{3}$ and $\lambda^4 = -6\lambda\beta$
$\implies \lambda(\lambda^3 + 6\beta) = 0$

if $\lambda = 0$
$a - \beta^2 = -r^3 = \dfrac{-\lambda^6}{27} = 0 \implies a = \beta^2$

Then $(0, \beta)$ and $(0, -\beta)$ are the two point of order 3.

if $\lambda \neq 0$
we get $\lambda^3 + 6\beta = 0$
Substituting $\lambda = \dfrac{3r^2}{-2\beta}$
we derive the relation $r^6 3^2 = 2^4\beta^4$.
This relation is satisfied only in case $\beta = 2^2 3^2 m^3$ and $r = 2^3 3m$ in this we calculate $a = \beta^2 - r^3 = -432m^6$.
where $m = 1$ since a is a sixth power free.
Thus if $a = -432$ or $a = \beta^2$ we get the torsion subgroup which is isomorphic to $\dfrac{Z}{3Z}$.

2.4 Multiplication by two on an Elliptic Curve

Theorem 2.4.1. *Let E be an elliptic curve defined over the field k by the equation*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma) = x^3 + ax^2 + bx + c$$

For $Q = (x', y') \in E(k)$ there exist $P = (x, y) \in E(k)$ with $2P = Q$ if and only if $x' - \alpha$,$x' - \beta$, and $x' - \gamma$ are the squares.

Proof- The equation $2(x, y) = (x', y')$ has a solution on $E(k)$ if and only if the the related equation $2(x, y) = (0, y')$ has a solution on the curve defined by the normal cubics

$$y^2 = (x + x' - \alpha)(x + x' - \beta)(x + x' - \gamma)$$

Hence we reduced to proving the statement for the point $(0, y')$. in this case $y'^2 = c$
For $2(x, y) = (0, y')$ the equation of the tangent line $y = \lambda x+\delta$ is tangent to E at (x, y) substitute the value of y in the cubic equation then we get $(\lambda x+\delta)^2 = x^3+ax^2+bx+c\ x(x^2+(a-\lambda^2)x+(b-2\lambda\delta)) = 0$,
$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\delta)x + c - \delta^2 = 0$
Since $(0, y')$ is the point of intersection of this tangent to E then we get $\delta^2 = c = y'^2$
$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\delta)x = 0$
$x(x^2 + (a - \lambda^2)x + (b - 2\lambda\delta)) = 0$
Since $y = \lambda x + \delta$ is the tangent, this quadratic equation in x must have a repeated root i.e $D = 0$
Thus we have
$(\lambda^2 - a)^2 = 4(b - 2y'\lambda)$
implies that $(\lambda^2 - a + u)^2 = 2u\lambda^2 - 8\lambda y' + (u^2 + 4b - 2ua)$
The right hand side of the quadratic term is a perfect square if and only if the discriminant is zero i.e
$(-8y')^2 - 8u(u^2 + 4b + 2ua) = 0$
$64c - 8u^3 - 32ub + 16u^2a = 0$
$u^3 - 2au^2 + 4ub - 8c = 0$
substitute $u = -2v$ the above equation becomes
$(-8)(v^3 + av^2 + bv + c) = 0$
This the cubic term in the equation of the curve, and, hence, the roots are $v = \alpha, \beta, \gamma$ so that $u = 2\alpha, 2\beta, 2\gamma$
Now substituting $u = -2\alpha$ in $(\lambda^2 - a + u)^2 = 2u\lambda^2 - 8\lambda y' + (u^2 + 4b - 2ua)$
implies that $(\lambda^2 - a + (-2\alpha))^2 = 2(-2\alpha)\lambda^2 - 8\lambda y' + ((-2\alpha)^2 + 4b - 2(-2\alpha)a)$
$(\lambda^2 - a - 2\alpha)^2 = 2(-2\alpha)\lambda^2 - 8\lambda y' + (4\alpha^2 + 4b + 4a\alpha)$
Now,

$$\alpha + \beta + \gamma = -a$$

$$(\alpha\beta + \beta\gamma + \gamma\alpha) = b$$

$$\alpha\beta\gamma = c$$

Thus the equation for λ becomes
$(\lambda^2 + \alpha + \beta + \gamma - 2\alpha)^2 = -4\alpha\lambda^2 - 8y'\lambda + (4a^2 + 4(\alpha\beta + \beta\gamma + \gamma\alpha) - 4\alpha(\alpha + \beta + \gamma))$ or
$(\lambda^2 + \alpha + \beta + \gamma)^2 = -4\alpha\lambda^2 - 8y'\lambda + 4\beta\gamma = 4(\alpha'\lambda - \beta'\gamma')^2$,
Taking $\alpha'^2 = -\alpha$ $\beta'^2 = -\beta$ $\gamma'^2 = -\gamma$ and taking the square root on both the side we get ,
$\lambda^2 + \beta + \gamma - \alpha = \pm 2(\alpha'\lambda - \beta'\gamma')$

in this equation we complete the square to get
$(\lambda^2 \mp 2\alpha'\lambda - \alpha) = -\beta \mp 2\beta'\gamma' - \gamma$ or
$(\lambda \mp \alpha')^2 = (\beta' \mp \gamma')^2$
Taking the square root of both side of the equation,we find four solution for λ proving the existence of λ in hence also of the point (x, y) since

$$x = \frac{\lambda^2 + \alpha + \beta + \gamma}{2}$$

and

$$y = \lambda x + \delta$$

This proves the theorem i.e the point P exist.

2.5 Corollary

For an elliptic curve E defined over an algebraically closed field the group homomorphism

$$\psi \colon E(k) \xrightarrow{2} E(k)$$

is surjective, that is, the group $E(k)$ is 2 divisible.
this corollary gives an exact sequence.

$$0 \xrightarrow{2} E(k) = (\frac{Z}{2Z})^2 \longrightarrow E(k) \xrightarrow{2} E(k) \longrightarrow 0$$

we can generalized for prime n.

$$0 \longrightarrow E(k) = (\frac{Z}{nZ})^2 \longrightarrow E(k) \xrightarrow{n} E(k) \longrightarrow 0$$

2.6 Remarks on the Group Law on the Singular Cubics

The two basic example of singular point on cubic curve are

(1)− A double point $(0, 0)$ on $y^2 = x^2(x + a)$
(2)− A cusp $(0, 0)$ on $y^2 = x^3$
For a cubic in normal form

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

the derivative of y' is

$$(2y + a_3 + a_3x)y' = 3x^2 + 2a_2x + a_4$$

at the point $(0, 0)$

$$a_3y' = a_4$$

the has a curve at singularity $(0, 0)$ if and only if $a_3 = a_4 = 0$
We consider the cubic A $y = x^3 + ax + b$ which is not in the normal form because there is no term of y^2.
if (x_1, y_1), (x_2, y_2) and (x_3, y_3) are the three points on the cubic A and on a line $y = \lambda x + \beta$ then
$\lambda x + \beta = x^3 + ax + b$
and $x_1 + x_2 + x_3 = 0$
so the set $A(k)$ has the structure of the group where $(0, b) = 0$ and $-(x, y) = -(x, x^3 + ax + b) = (-x, (-x)^3 - ax + b)$.

Remark 2.6.1. *The function $f(t) = (t, t^3 + at + b)$ is an isomorphism $f\colon k \longrightarrow A(k)$ of the additive group of the line k onto $A(k)$.*

Chapter 3

Elliptic Curve and Their Isomorphism

3.1 The Group Law on a Nonsingular Cubic

Remark 3.1.1. *Suppose L be a line and C be the cubic curve and both of them are defined over the field k. and k' be an algebraically closed extension of k.*
so the different case holds for the $L(k') \cap C(k')$.

(1)- *If $L(k') \cap C(k') = P_1, P_2, P_3$, and the multiplicity $i(P; L, C) = 1$ for $i = 1, 2, 3$*
and the composition is as $P_i P_j = P_k$, and if P_i and P_j are the rational then P_k is also rational over k for $i, j, k = 1, 2, 3$.

(2)- *If $L(k') \cap C(k') = P, P'$, and the multiplicity $i(P; L, C) = 2$,and $i(P; L, C) = 1$ thus here Line L is tangent to cubic C at P or we can say that the point P is a singular point on the cubic C, and the composition is $PP = P'$ and if P is rational over the field k, then P' is also rational .*

(2)- *if $L(k') \cap C(k') = P$, one point, and the multiplicity $i(P; L, C) = 3$*
and the composition is $PP = P'$ and the point P is a singular point.

3.2 Normal Form of Elliptic curve

Definition 3.2.1. *(Invariant differential) Let E be an elliptic curve in normal form.*
E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
then the invariant differential is is given by

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dx}{f_y} = \frac{-dy}{f_x} = \frac{dy}{3x^2 + 2a_2x - a_4 - a_1y}$$

.

Definition 3.2.2. *(Admissible change of variable) An admissible change of variable is one of the form*

$$x = u^2\overline{x} + r$$

and

$$y = u^3\overline{y} + su^2\overline{x} + r$$

where the u,r,s,t are in k with u invertible . if we substitute the value of x and y in the normal form of the equation then we get the new form of the equation in term of variables $\overline{x}$ *and* $\overline{y}$*:*

$$\overline{y}^2 + \overline{a}_1\overline{x}\overline{y} + \overline{a}_3\overline{y} = \overline{x}^3 + \overline{a}_2\overline{x}^2 + \overline{a}_4\overline{x} + \overline{a}_6$$

and the coefficient is

$$u\overline{a}_1 = a_1 + 2s,$$

$$u^2\overline{a}_2 = a_2 - sa_1 + 3r - s^2,$$

$$u^3\overline{a}_3 = a_3 + ra_1 + 2t = f_y(r,t)$$

$$u^4\overline{a}_4 = a_4 - sa_3 + 2ra_2 - (t - rs)a_1 + 3r^2 - 2st = -f_x(r,t) - sf_y(r,t),$$

$$u^6\overline{a}_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2 = -f(r,t),$$

and

$$\overline{\omega} = u\omega$$

Remark 3.2.3. *if* $\psi\colon \overline{E} \longrightarrow E$ *is an isomorphism such that the function x,y on E composed with* ψ *are related to the function* $\overline{x}$ *,* $\overline{y}$ *on* $\overline{E}$ *by an admissible change of variable.*

$$x\psi = u^2\overline{x} + r,$$

and

$$y\psi = u^3\overline{y} + su^2\overline{x} + t$$

Definition 3.2.4 (Section)**.** *For any open subset U of X,*$O(U)$ *is termed as a section for U .*

Definition 3.2.5 (Presheaf)**.** *A presheaf O is is a collection of all abelian group on a ringed space X,where for every open subset U of X ,* $O(U)$ *is an abelian group , and between any two subset of X there is a morphism between* $O(U)$ *and* $O(V)$*.*

Definition 3.2.6 (Sheaf)**.** *A presheaf whose section are determined by local data such as continuity and differentiability is called a sheaf..*

Definition 3.2.7 (Germs of Regular Functions)**.** *Functions f and g define the same germ if for all x in X ,there is a neighbourhood U of X such that f and g are equal in U.*

Theorem 3.2.8 (Riemann-Roch for Curves of Genus 1)**.** *Suppose $\Theta_C(m.K)$ be the structure sheaf on the non-singular curve C of the germs of the regular function and having at most an mth order pole at K ,Then for the vector space of the section $\Gamma(\Theta_C(m.K))$ where C is the curve of genus 1. and we can find a basis for $\Gamma(\Theta_C(m.K))$ for small m and using the inclusions $\Gamma(\Theta_C(m.K)) \subset \Gamma(\Theta_C(m'.K))$ and $m \leqslant m'$.*

$$dim_k(\Gamma((\Theta_C(m.K))) = \begin{cases} m & m > 1 \\ 1 & m = 0 \end{cases}$$

$$\Gamma(\Theta_C(1.K)) = k.1,$$

$$\Gamma(\Theta_C(2.K)) = k.1 \oplus k.x,$$

$$\Gamma(\Theta_C(3.K)) = k.1 \oplus k.x \oplus k.y,$$

$$\Gamma(\Theta_C(4.K)) = k.1 \oplus k.x \oplus k.y \oplus k.x^2,$$

$$\Gamma(\Theta_C(5.K)) = k.1 \oplus k.x \oplus k.y \oplus k.x^2 \oplus k.xy,$$

Here 1 has a pole of order of 1 ,x has a pole of order 2 ,and y has a pole of order 3
In $\Gamma(\Theta_C(6.K))$ there are seven natural basis elements,
$\{1, x, y, x^2, xy, x^3, y^2\}$.

3.3 The Discriminant and the Invariant j

The cubic equation in normal form

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

the new coefficient b_i for $i = 2, 4, 6, 8$ and c_j for $j = 4, 6$ these two new coefficient originate first for completing the square and then completing the cube.
Notation-
$b_2 = a^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$ and
$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$ and these new coefficient are related by the $4b_8 = b_2b_6 - b_4^2$ and the discriminant in terms of the new coefficient for $b_i's$

$$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

with the help of the discriminant we say that when the cubic is non-singular, so the cubic is non-singular if and only if the $\triangle \neq 0$.

Remark 3.3.1. *Under an admissible change of variable we have the following relations*

$$u^2 b_2^{'} = b_2 + 12r,$$

$$u^4 b_4^{'} = b_4 + rb_2 + 6r^2,$$

$$u^6 b_6^{'} = b_6 + 2rb_4 + r^2 b_2 + 4r^3,$$

$$u^8 b_8^{'} = b_8 + 3rb_6 + 3r^2 b_4 + 3r^4,$$

and lastly

$$u^{12} \triangle^{'} = \triangle$$

Proposition 3.3.2. *If k is field of characteristic different from 2, then equation of normal form becomes*

$$(y')^2 = (x')^3 + \frac{b_2}{4}(x')^2 + \frac{b_4}{2}x' + \frac{b_6}{4}$$

Proof. First we substitute $y' = y + \dfrac{a_1 x + a_3}{2}$ and $x' = x$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

so k is a field which is differ from 2 then the equation becomes

$$y^2 + 2\frac{a_1 x + a_3}{2}y + (\frac{a_1 x + a_3}{2})^2 - (\frac{a_1 x + a_3}{2})^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

$$(y + \frac{a_1 x + a_3}{2})^2 = x^3 + a_2 x^2 + a_4 x + a_6 + \frac{1}{4}(a_1^2 x^2 + a_3^2 + 2a_1 a_3 x)$$

$$(y + \frac{a_1 x + a_3}{2})^2 = x^3 + x^2(\frac{a_1^2 + 4a_2}{4}) + (a_4 + \frac{1}{2}a_1 a_3) + (a_6 + \frac{a_3^2}{4})$$

Arranging the coefficient and then we get the equation in normal form for the characteristic different from 2.

$$(y')^2 = (x')^3 + \frac{b_2}{4}(x')^2 + \frac{b_4}{2}x' + \frac{b_6}{4}$$

□

Notation- Coefficient for c_j in term of $b_i' s$ are

$$c_4 = b_2^2 - 24b_4,$$

and

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

for the $\triangle$ then invariant j is,

$$j(E) = j = \frac{c_4^3}{\triangle}$$

and we have the following relation $12^3\triangle = c_4^3 - c_6^2$, so we get the invariant j ,

$$j = 12^3 \frac{c_4^3}{c_4^3 - c_6^2}$$

Remark 3.3.3. *Under an admissible change of variable we have*

$$u^4 c_4^{'} = c_4,$$

and

$$u^6 c_6^{'} = c_6$$

and $j^{'} = j$.
and if k is a field of characteristic different from 3 *then for* $y'' = y'$ *and* $x'' = x' + \frac{b_2}{12}$ *then equation of normal form become,*

$$(y'')^2 = (x'')^3 - x''(\frac{c_4}{48}) - \frac{c_6}{864}$$

and $\omega = \frac{dx''}{2y''}$ *,Now we have to consider a cubic polynomial,*

$$f(x) = x^3 + px + q$$

, the discriminant of the cubic polynomial become

$$D(f) = 27q^2 + 4p^3$$

.

Remark 3.3.4. *The cubic polynomial* $f(x) = x^3 + px + q$ *has a repeated root in some extension field of k if and only if* $D(f) = 0$.
Equation

$$y^2 = x^3 - -x(\frac{c_4}{48}) - \frac{c_6}{864} = f(x),$$

where $p = \frac{c_4}{48}$ *and* $q = \frac{c_6}{864}$, $864 = 2^5.3^3$ *and* $48 = 2^4.3$ *then we have*

$$-2^4 D(f) == \frac{c_4^3 - c_6^2}{12^3} = \Delta$$

Proposition 3.3.5. *Over a field k of characteristic different from 2 and 3 the cubic equation*

$$y^2 = x^3 - -x(\frac{c_4}{48}) - \frac{c_6}{864}$$

represent an elliptic curve if and only if $\Delta \neq 0$ and $\omega = \frac{dx}{2y}$.

Remark 3.3.6. *For $j \neq 0$ or 12^3 the following cubic*

$$y^2 + xy = x^3 - x\frac{36}{1728} - \frac{1}{j - 1728}$$

defines the elliptic curve with j-invariant equals j over any field of k.
The elliptic curve with equation

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

has $j = 0$, and the elliptic curve with equation

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

has $j = 0 = 1728$.

3.4 Isomorphism classification for Characteristic $\neq 2, 3$

For the characteristic of the base field $\neq 2, 3$, an elliptic curve over k the Weierstrass model of the equation become.

$$y^2 = x^3 + a_4x + a_6,$$

$$\omega = \frac{dx}{2y},$$

$$c_4 = -48a_4,$$

$$c_6 = -864a_6,$$

and

$$\Delta = -16(4a_4^3 + 27a_6^2),$$

And the curve E is smooth or non-singular if and only if $\Delta \neq 0$

$$j = 12^3\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

3.5 Isomorphism between two elliptic curves with same j invariant

Isomorphism between two elliptic curve is of the form of an admissible change of variable, suppose the two elliptic curve E and $E^{'}$ defined over the field k such that $j = j(E) = j(E')$.

$E: y^2 = x^3 + a_4x + a_6$
$E^{'}: y^2 = x^3 + \overline{a}_4x + \overline{a}_6$
if

$$\psi: E \longrightarrow E^{'}$$

is an isomorphism, then

$$x\psi = u^2\overline{x}.$$

$$y\psi = u^3\overline{y}$$

$$a_4 = u^4\overline{a}_4$$

$$a_6 = u^6\overline{a}_6$$

we will consider these relation in three different cases for j.

Case 1- $j \neq 0$ or $j \neq 12^3$
if $j \neq 0$ then $a_4 \neq 0$ and $a_6 \neq 0 \Longrightarrow a_4a_6 \neq 0$ Then E and $E^{'}$ are isomorphic if and only if $\frac{a_4a_6^{'}}{a_4^{'}a_6} = \frac{a_4^{'}a_6^{'}u^4}{a_4^{'}a_6^{'}u^6} = u^{-2}$ is a square.
Hence E and $E^{'}$ are isomorphic over any field extension of k containing the square root of the quotient. To find the automorphism group of E then $E = E^{'}$, then we have $u^2 = 1$

$$Aut(E) = \{+1, -1\}$$

the group of square root of 1 .
Case 2- $j = 12^3$
if $j = 12^3$ then $a_6 = 0$
then E and $E^{'}$ are isomorphic if and only if the quotient
$\frac{a_4}{a_4^{'}}$ is a fourth power u^4
Hence E and $E^{'}$ are isomorphic over any field extension of k containing the fourth root of the quotient
$\frac{a_4}{a_4^{'}}$ is a fourth power u^4
to find the automorphism group of E then $E = E^{'}$ then we have $u^4 = 1$

$$Aut(E) = \{+1, -1, i, -i\}$$

the group of fourth root of unity.

Case 3- $j = 0$
if $j = 0$ then $a_4 = 0$
then E and $E^{'}$ are isomorphic if and only if the quotient
$\frac{a_6}{a_6^{'}}$ is a six power u^6
Hence E and $E^{'}$ are isomorphic over any field extension of k containing the six root of the quotient.
to find the automorphism group of E then $E = E^{'}$ then we have $u^6 = 1$

$$Aut(E) = \{+1, -1, \rho, -\rho, \rho^2, -\rho^2\}$$

the group of six root of unity where

$$\rho^2 + \rho + 1 = 0$$

At this point, the following two questions are
1-if $j(E) = j(E^{'}) \Longrightarrow E \cong E^{'}$
2-For all values in k besides 0 and 12^3, are j values of some elliptic curve.
The answer of both the question is yes
Consider E: $y^2 = x^3 + a_4x + a_6$
by rescaling the coefficient the Weierstrass equation has the form E: $y^2 = 4x^3 - cx - c$

$$j = j(E) = 12^3 \frac{c^3}{c^3 - 27c^2},$$

$$= 12^3 \frac{c}{c - 27},$$

$$= 12^3 J,$$

where

$$j = \frac{c}{c - 27} = \frac{j}{1728},$$

Thus,

$$c = 27\frac{J}{J - 1} = 27\frac{j}{j - 1728}^{'}$$

substituting the value of c in equation E: $y^2 = 4x^3 - cx - c$
we get

$$y^2 = 4x^3 - 27\frac{j}{j - 1728}x - 27\frac{j}{j - 1728}$$

and has j- invariant equal to the parameter j.

3.6 Isomorphism Classification in Characteristic = 3

For an elliptic curve E over the field k of characteristic 3 in normal form after completing the square the equation

$$E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

and

$$\omega = \frac{-dx}{y},$$

For E we have the following,

$$b_2 = a_2$$

$$b_4 = -a_4$$

$$b_6 = a_6,$$

$$b_8 = -a_4^2 + a_2a_6,$$

$$c_4 = a_2^2,$$

$$c_6 = -a_2^3,$$

$$\Delta = a_2^2a_4^2 - a_2^3a_6 - a_4^3,$$

$$j = \frac{c_4^3}{\Delta} = \frac{a_2^6}{a_2^2a_4^2 - a_2^3a_6 - a_4^3}$$

The curve E is non-singular ,$\Delta \neq 0$
We will find the condition for u,r,s,t for the isomorphism of E,
Consider the two elliptic curves defined over the field k.
$E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6$
$E^{'}: y^2 = x^3 + a_2^{'}x^2 + a_4^{'}x + a_6^{'}$

If

$$\psi\colon E \longrightarrow E^{'}$$

is an isomorphism, , then its form is determined by $j \neq 0$ or $j = 0$
Case 1- $j \neq 0$, then $a_2 \neq 0$ by completing the square in both Weierstrass equations in E,

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

$$= a_2(\frac{1}{a_2}x^3 + (x^2 + a_4x + (\frac{a_4}{2})^2) + a_6 - \frac{a_4^2}{4})$$

$$= a_2(\frac{1}{a_2}x^3 + (x + \frac{a_4}{2})^2 + \frac{4a_6 - a_4^2}{4})$$

$$= x^3 + a_2(x + \frac{a_4}{2})^2 + \frac{4a_2a_6 - a_4^2a_2}{4}$$

then we get $a_4 = a_4^{'} = 0$
Also, $j(E) = \frac{-a_2^3}{a_6}$ and $j(E^{'}) = \frac{-a_2^{'3}}{a_6^{'}}$
and the following holds

$$x\psi = u^2x^{'},$$

$$y\psi = u^3y^{'},$$

and

$$a_2 = u^2a_2^{'}$$

Hence E and $E^{'}$ are isomorphic over any field extension of k containing the square root of the quotient $\frac{a_2}{\bar{a}_2} = u^2$
To find the automorphism group of E then $E = E^{'}$ then we have $u^2 = 1$

$$Aut(E) = \{+1, -1\}$$

the group of square root of 1.

Case 2- $j = 0$ then $a_2 = 0$
Then $\Delta = a_4^3$ and $\omega = \frac{dy}{a_4}$
then we have the following change of variable,

$$x\psi = u^2x^{'} + r$$

$$y\psi = u^3y^{'}$$

$$u^4a_4^{'} = a_4$$

$$a_6 + ra_4 + r^3 = u^6a_6^{'}$$

Hence E and $E^{'}$ are isomorphic over any field where $\frac{a_4}{a_4^{'}}$ is a fourth power and there is a solution for cubic equation for r
if $E = E^{'}$
then automorphism are parametrized by u and r
if $u = 1, -1$
then

$$r^3 + a_4r = 0$$

if $u = i, -i$
then

$$r^3 + a_4 r + 2a_6 = 0$$

Automorphism group is a semidirect product ,
$\mathrm{Aut}(E) = \dfrac{\mathbb{Z}}{4} \times \dfrac{\mathbb{Z}}{3}$

For $j \neq 0 or 12^3$we had

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$

in Characteristic 3 the equation become

$$y^2 + xy = x^3 - \frac{1}{j}$$

where

$$j = \frac{1}{a_6}$$

via rescaling the coefficient using admissible change of variable 3

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

where

$$a_6 = \frac{-1}{j}$$

Proposition 3.6.1. *Curves with equation*

$$y^2 = x^3 + x^2 - \frac{1}{j},$$

and

$$y^2 + xy = x^3 - \frac{1}{j},$$

have j-invariant equal to the parameter j.

3.7 Isomorphism Classification in Characteristic 2

Consider the elliptic curve E over the field k of characteristic 2 and the invariant differential $\omega = \dfrac{dx}{2y + a_1 x + a_3} = \dfrac{dx}{a_1 x + a_3}$ so that $a_1 a_3 \neq 0$

$$b_2 = a_1^2,$$

$$b_4 = a_1 a_3,$$

$$b_6 = a_3^2,$$

$$c_4 = b_2^2,$$

$$c_6 = -b_2^3,$$

$$j = \frac{a_1^{12}}{\Delta}$$

For the different cases of j we get the different cubic equation in normal form .
Case 1- $j \neq 0$
if $j \neq 0 \Longrightarrow a_1 \neq 0$
change $x \longrightarrow x + c$ we get ,

$$y^2 + a_1xy + a_3 = y^2 + a_1xy + (a_1c + a_3)y$$

For $a_1 \neq 0$ so we can choose $a_3 = 0$
changing x to a_1^3x and y to a_1^3y we get,

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

and

$$\omega = \frac{dx}{x}$$

$$b_2 = 1$$

$$b_4 = 0 = b_6$$

$$b_8 = a_6$$

$$c_4 = 1$$

$$\Delta = a_6 = \frac{1}{j}$$

Case 2- $j = 0$
if $j = 0 \Longrightarrow a_1 = 0$
By completing the cube, the normal form of the cubic to be,

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

and

$$\omega = \frac{dx}{2y},$$

$$b_2 = 0,$$

$$b_4 = 0,$$

$$b_6 = a_3^2,$$

$$b_8 = a_4^2,$$

$$\Delta = a_3^4$$

In both the cases it follows that the curve is smooth if and only if $\Delta \neq 0$.
Suppose E and $E^{'}$ are the two elliptic curves defined over the field k such that $j(E) = j(E^{'}) = j$
We have,E: $y^2 = x^3 + a_4x + a_6$
$E^{'}$: $y^2 = x^3 + \overline{a}_4x + \overline{a}_6$

if

$$\psi \colon E \longrightarrow E^{'}$$

is an isomorphism, , then its form is determined by $j \neq 0$ or $j = 0$
Case a- $j \neq 0$
Then,

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

$$E^{'} : y^2 = x^3 + a_4^{'}x + a_6^{'}$$

the change of variable is

$$x\psi = x^{'},$$

$$y\psi = y^{'} + sx^{'},$$

$$a_2^{'} = a_2 + s^2 + s,$$

$$a_6^{'} = a_6$$

Then E and $E^{'}$ are isomorphic over any field extension of k containing a solution to the quadratic equation

$$s^2 + s = \overline{a}_2 - a_2$$

If $E = \overline{E}$ then $a_2 = a_2^{'}$ so we get $s^2 - s = 0$ i.e $s = 0, 1$

$$Aut(E) = \{0, 1\}$$

Case b- $j = 0$
Then,

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

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

the change of variable is

$$x\psi = u^2 x^{'}$$

$$y\psi = u^2 y^{'} + sa_3 + s^4,$$

$$a_3 = u^3 a_3^{'},$$

$$u^4 a_4^{'} = a_4 + sa_3 + s^4$$

$$u^6 a_6^{'} = a_6 + s^2 a_4 t a_3 + s^6 + t^2$$

Then E and $E^{'}$ are isomorphic if and only if
(1)– $\frac{a_3}{a_3^{'}} = u^3$

(2)– $s^4 + a_3 s + a_4 + u^4 a_4^{'} = 0$ has a solution in the field extension of k.

(3)– $t^2 + a_3 t + (s^6 + s^2 a_4 + a_6 + u^6 a_6^{'}) = 0$ as a quadratic equation in t has a solution in field extension of k.

Special case -
When $k = F_2$ so there are 5 elliptic curves up to isomorphism
If $j = 1$ then

$$y^2 + xy = x^3 + a_2 x^2 + 1$$

we have to take two different cases for a_2 i.e
If $a_2 = 0$ then

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

If $a_2 = 1$ then

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

If $j = 0$ then

$$y^2 + y = x^3 + a_4 x + a_6$$

we have to take three different cases for a_4 and a_6 i.e
if $a_4 = 0$, $a_6 = 1$ then

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

if $a_4 = 1$, $a_6 = 1$ then

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

if $a_4 = 1$, $a_6 = 0$ then

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

Proposition 3.7.1. *Up to isomorphism over F_2 there are 5 elliptic curves over the field F_2 i.e E*

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

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

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

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

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

3.8 Singular Cubic curves

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

consider tese cubic equation in normal form over the field k
suppose it has a singular point which is rational
This singular point can be transformed to origin using change of variable $(x, y, w) = (0, 0, 1)$
Observe that $(0, 0)$ is on the curve, i.e $F(0, 0) = 0$ if and only if $a_6 = 0$
Now we determine whether or not $(0, 0)$ is a singular point

$$F_x = a_1y - 3x^2 - 2a_2x - a_4$$

and

$$F_y = 2y + a_1x + a_3$$

Both partial derivative must be zero $\implies a_3 = -a_4 = 0$ we get

$$y^2 + a_1xy = x^3 + a_2x^2$$

For this

$$b_4 = b_6 = b_8 = 0$$

and

$$\Delta = 0$$

$b_2 = a_1^2 + 4a_2$
Substitute $t = \dfrac{-x}{y}$ and $s = \dfrac{-1}{y}$ i,e $x = \dfrac{t}{s}$
then the equation become

$$s = t^3 + a_1ts + a_2t^2s$$

and thus s is rational function of t,

$$s = \frac{t^3}{1 - a_1 t - a_2 t^2}$$

$$C_{ns} = (t, s) | s = \frac{t^3}{1 - a_1 t - a_2 t^2}, 1 - a_1 t - a_2 t^2 \neq 0$$

where C_{ns} is the set of all non-singular points.

Theorem 3.8.1. *Let E be a cubic curve over k with the equation* $y^2 + a_1 xy = x^3 + a_2 x^2$ *which we factor* $(y - \beta x)(y - \alpha x) = x^3$ *over the field* $k_1 = k(\alpha) = k(\beta)$

(1) $\alpha \neq \beta$ *(multiplicative case)*

$$\phi \colon E_{ns} \longrightarrow G_m$$

is homomorphism such that $(x, y) \longrightarrow \dfrac{y - \beta x}{y - \alpha x}$
(a) *if* $k = k_1$ *i.e* α *and* β *are in k, then the map*

$$\phi \colon E_{ns} \longrightarrow G_m = k^*$$

is an isomorphism onto the multiplicative group of k.
(b) *if* k_1 *is a quadratic extension of k, i.e,* α β *are not in k, then he map*

$$\phi \colon E_{ns} \longrightarrow ker(N_{\frac{k_1}{k}})$$

where

$$N_{\frac{k_1}{k}} : k_1^* \longrightarrow k^*$$

is the norm map and $ker(N_{\frac{k_1}{k}})$ *is the subgroup element in* k_1^* *with norm 1.*
(2) $\alpha = \beta$ *(additive case)*

$$E_{ns} \longrightarrow G_a$$

over k_1 *and*

$$(x, y) \longrightarrow \frac{x}{y - \alpha x}$$

is a homomorphism over k_1*. and the map*

$$E_{ns}(k_1) \longrightarrow G_a(k_1)$$

is an isomorphism onto the additive group of k_1*.(observe* $k = k(\alpha)$ *except possibly in characteristic 2).*

Proof. (1) Let $u = \dfrac{y - \beta x}{y - \alpha x}$ and $v = \dfrac{1}{y - \alpha x}$, $u = (y - \beta x)v$

$$(y - \beta x)(y - \alpha x) = x^3$$

using these relation we get

$$(u-1)^3 = (\alpha-\beta)^3 uv$$

Moreover, lines with x,y with equations $Ax + By + C = 0$ are transformed into lines in u,v with equations $A'u + B'v + C' = 0$
Let (u_1, v_1) (u_2, v_2) and (u_3, v_3) are the three points on the cubic E_{ns} which lie on the line $v = \lambda u + \delta$ then we get

$$(u-1)^3 - (\alpha-\beta)^3 u(\lambda u + \delta) = (u-u_1)(u-u_2)(u-u_3)$$

And $u_1u_2u_3 = 1$ (identity) it means the function

$$(x, y) \longrightarrow u$$

carries the group law on E_{ns} into the multiplicative group law on k_1^*.

$N_{\frac{k_1}{k}}(u) = uu' = \dfrac{y-\beta x}{y-\alpha x}.\dfrac{y-\alpha x}{y-\beta x} = 1$
Norm of u is 1 where $\alpha' = \beta$ and $\beta' = \alpha$
if z is in k_1 has norm 1
$\Longrightarrow c \in k_1$ such that $w = c + c'z \neq 0$
we have $w' = c' + z'c$
$\Longrightarrow zw' = zc' + zz'c = c + zc' = w$
Hence $z = \dfrac{w}{w'} = \dfrac{y-\beta x}{y-\alpha x}$ for x,y in k
(2) in case of additive we take

$$u = \frac{x}{y-\alpha x}$$

and

$$v = \frac{1}{y-\alpha x}$$

using the relation we get

$$(y-\alpha x)^3 u^3 = x^3$$

and lines in x-y transformed in lines in u-v as $v = u^3$
Let (u_1, v_1), (u_2, v_2) and (u_3, v_3) are the three points on the cubic E_{ns} which lie on a line $v = \lambda u + \delta$ then we get

$$u^3 - v = u^3 - (\lambda u + \delta) = (u-u_1)(u-u_2)(u-u_3) = 0$$

and hence the relation $u_1 + u_2 + u_3 = 0$ in the additive group.
$(x, y) \longrightarrow u$ carries group law on E_{ns}, into the additive group law on k_1, and $E_{ns} \longrightarrow k_1^+$ is an isomorphism of group.

□

Remark 3.8.2. *Consider*

$$x^3 = y^2 + a_1xy - a_2x^2$$
$$= (y - \alpha x)(y - \beta x)$$

the tangent line are given by $y = \alpha x$ *and* $y = \beta x$ *and the discriminant is* $D = a_1^2 + 4a_2 = b_2$
Two cases corresponds to two kinds of singularities

(1)-
$(0, 0)$ *is a node if and only if* $D = b_2 \neq 0$ *i.e* $\alpha \neq \beta$ *and observe that* $b_2 \neq 0$ $c_4 \neq 0$ *and* $c_6 \neq 0$ *so*

$$j = \frac{c_4^3}{\Delta} = \infty$$

where $\Delta = 0$ *The tangent are rational over* k *if and only if* b_2 *is a square in* k.

(2)-
$(0, 0)$ *is a cusp if and only if* $D = b_2 = 0$ *i.e* $\alpha = \beta$ *and observe that* $b_2 = 0$ $c_4 = 0$ *and* $c_6 = 0$ *so all are equivalent in this case and* $j = \frac{0}{0}$ *is indeterminate.*

Chapter 4

Family of Elliptic Curves and their Geometric Properties

In the previous chapters, we saw that the basic properties of elliptic curves, defined Normal form of an elliptic curve and see how the two elliptic curve are isomorphic to each other over a field k. In this chapter we investigates some families of elliptic curves and know about torsion point on those kind of families of elliptic curves.Such families can be computed by a cubic in normal form and their coefficient depends upon the parameter.We close the chapter by defining with a dual isogeny or explicit isogeny, that is, a homomorphism of elliptic curves for particular curves and see their importance.

4.1 The Legendre Family

The Legendre family is one of the most important family of the elliptic curves.
Consider a cubic in normal form of an equation with $a_i(t) \in k[t]$

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

giving an elliptic curve E over $k(t)$, then we can substitute in any value for $t \in T$, the parameter space, and obtained a normal form of an cubic equation, and, hence, an elliptic curve E over $k(t)$ at all points T where $\triangle\ (E_t) \neq 0$. Now the Each point $P(t) = (x(t), y(t)) \in E(k(t))$ can be viewed as a mapping from T to E.such a map is called the cross- section.

Remark 4.1.1. *The group of points of E over $k(t)$ is the group of rational cross-section of the algebraic family of the elliptic curves E_t over k. and the one such cross-secion of the algebraic family of an elliptic curves is always the zero cross-section.*

Definition 4.1.2. *(Legendre Family) For the field of characteristic not equals to two, the Legendre family of an elliptic curves is defined as*

$$E_\lambda : y^2 = x(x-1)(x-\lambda).$$

From the definition, we observe that the curve E_λ is nonsingular for $\lambda \neq 0, 1$, so that over $k - 0, 1$, it is a family of nonsingular elliptic curves.

Remark 4.1.3. *The four basic cross-section for the nonsingular curve E_λ are $0(\lambda) = 0$, $e_1(\lambda) = (0, 0)$, $e_2(\lambda) = (1, 0)$, $e_3(\lambda) = (\lambda, 0)$. the value of these four cross section $E(\lambda)$ give the group of 2-division point on $E(\lambda)$. With the three nonzero cross-section, there are six possible ordering for the 2-division point on an the elliptic curve E, or equivalently, six possible bases (e_1, e_2) for the subgroup of the two division point on E_λ.*

Proposition 4.1.4. *The orbit of λ under G acting on $\mathbb{P}_1 - \{0, 1, \infty\}$ is*

$$\lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda - 1}{\lambda}, \frac{\lambda}{\lambda - 1}.$$

If s is an element in G, then $s(\lambda)$ is same as one the above terms. The curve E_λ and $E_{\lambda'}$ are isomorphic to each other, in the other words their expressions should be differ by a linear change of variable which conserves the group structure, if and only if there exists $s \in G$ with $s(\lambda) = \lambda'$.

Remark 4.1.5. *The j-invariant $j(E_\lambda)$ of E_λ: $y^2 = x(x-1)(x-\lambda)$ is the value.*

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

This $j-$ invariant is some kind of special case of the j- invariant of any cubic in normal form, and their normalization factor 2^8 arises naturally.

Proposition 4.1.6. *The j-invariant has one of the special property that $j(\lambda) = j(\lambda')$ if and only if E_λ and $E_{\lambda'}$ are isomorphic under change of variable preserving the group structure.*

Remark 4.1.7. *The orbit of $\lambda \in \mathbb{P}_1$ under G has six distinct elements λ, $1 - \lambda$, $\frac{1}{\lambda}$, $\frac{1}{1-\lambda}$, $\frac{\lambda - 1}{\lambda}$ and $\frac{\lambda}{\lambda - 1}$ except in three case :*
(1) *$j(\lambda) = \infty$ where orbit is $\{0, 1, \infty\}$.*
(2) *$j(\lambda) = 0$ where the orbit is $\{+\rho, -\rho^2\}$ for $\rho^2 + \rho + 1 = 0$,i.e.,ρ is the third primitive root of unity.*
(3) *$j(\lambda) = 12^3$ where the orbit is $\{\frac{1}{2}, -1, 2\}$.*

Now we put out few things about the few exceptional values $j = 12^3$ or $j = 0$.
(1) *For $j(\lambda) = 12^3$ take $\lambda = -1$, then the curve is the familiar*

$$y^2 = x(x-1)x(x+1) = x^3 - x$$

which is one of the family of the curve $y^2 = x^3 + ax$.
(2) *For $j(\lambda) = 0$ take $\lambda = -\rho$ then the curve has equation of the form,*

$$y^2 = x(x-1)x(x+\rho).$$

and make a change of variable $x + \frac{1-\rho}{3}$ for x. This gives the equation

$$y^2 = (x + \frac{1-\rho}{3})(x + \frac{-2-\rho}{3})(x + \frac{1+2\rho}{3}).$$

and this is just

$$y^2 = x^3 - \frac{i}{3\sqrt{3}}$$

and which is one of the the family of the curve $y^2 = x^3 + a$.
The discriminant for the family E_λ *is given by* $\Delta_\lambda = 2^4\lambda^2(\lambda - 1)^2$.

4.2 The Hessian Family

Consider the normal form of cubic,

$$E_0 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We observe that $(0, 0)$ is a point on the curve if and only if $a_6 = 0$.
Differentiating both sides of E_0 with respect to x we get,

$$(2y + a_1x + a_3)y' = 3x^2 + 2a_2x + a_4 - a_1y.$$

$$\implies y' = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1y + a_3}$$

slope of tangent at $(0, 0)$ is $y' = \frac{a_4}{a_3}$ on E_0.

Remark 4.2.1. *Now,* $(0, 0)$ *is singular point if and only if* $a_3 = a_4 = 0$ *on* E_0. *if* $a_3 = 0$ *and* $a_4 \neq 0$, *then we get a vertical tangent so* a_4 *should also be zero. The point* $(0, 0)$ *is a nonsingular point of order* 2 *in the group* E *if and only if* $a_3 = 0$ *and* $a_4 \neq 0$, *in this case the family of cubic reduces to* $E_{00} : y^2 + a_1xy = x^3 + a_2x^2 + a_4x$. *Now we assume that* $(0, 0)$ *is a nonsingular point which is not of order* 2. *by the change of variable of the form*

$$x' = x,$$

$$y = y' + (\frac{a_4}{a_3})x'.$$

The equation for E_0 *takes the form*

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2$$

Since $a_4 = 0$, $a_3 \neq 0$.
Slope of tangent at $(0, 0)$ *in* E' *is equals to zero (horizontal tangent).*

Remark 4.2.2. *The point* $(0, 0)$ *on* E' *has order* 3 *if and only if* $a_2 = 0$ *and* $a_3 \neq 0$. *In this case ,the family reduces to*

$$E(a_1, a_3) : y^2 + a_1xy + a_3y = x^3.$$

Thus, E' *have third-order intersection with the tangent line* $y = 0$ *at* $(0, 0)$.
For these curve some of the basic invariants are the following:
$b_2 = a_1^2$, $b_4 = a_1a_3$, $b_6 = a_3^2$, $b_8 = 0$, $\Delta = a_1^3a_3^3 - 27a_3^4$, $c_4 = a_1(a_1^3 - 24a_3)$ *and* $j = \frac{c_4^3}{\Delta}$.
We can normalize $a_3 = 1$ *to obtain Hessian family of elliptic curve which gives the point of order* 3.

Definition 4.2.3. *The Hessian family of elliptic curve $E_\alpha : y^2 + \alpha xy + y = x^3$. is defined for any field of characteristic different from 3, where j- invariant of E_α is given by :*

$$j(\alpha) = \alpha^3 \frac{(\alpha^3 - 24)^3}{\alpha^3 - 27}.$$

for nonsingularity $\alpha^3 \neq 27$, i.e $\alpha \neq 3, 3\omega, 3\omega^2$ over $k/\{3, 3\omega, 3\omega^2\}$.
E_α consist of elliptic curve with constant section $(0,0)$ of order 3 where $2(0,0) = (0,-1)$.

Remark 4.2.4. *At the point $3, 3\omega, 3\omega^2$, E_α has 3 singular fibres which are nodal cubics at the points where $1 + \omega + \omega^2 = 0$. Now consider the equation without normalizing $y^2 + a_1xy + a_3y = x^3$ suppose $y = 0$ intersects the cubic implies that $x^3 = 0$ i.e $x = 0$ implies triple intersection point $(0,0)$ is point of order 3.*
Suppose $y = x + u$ intersects the cubic such that it generates the the distinct subgroup of order 3. The line $y = x + u$ has a triple intersection point $(v.v + u)$ with the cubic iff
$x^3 - (x+u)^2 - (a_1x + a_3)(x+u) = (x-v)^3$
$\implies x^3 - (x^2 + u^2 + 2ux) - (a_1x^2 + a_1ux + a_3x + a_3u) = (x-v)^3$
comparing the coefficient of x^2, x, and x^0 yields the relations.

$$3v = a_1 + 1,$$

$$-3v^2 = 2v + a_1u + a_3,$$

$$v^3u^2 + a_3u$$

Multiply the second relation by u, we obtain

$$-3uv^2 = 2u^2 + a_1u^2 + a_3u.$$

And subtracting it from the third relation yields

$$v^3 + 3uv^2 = -u^2(1 + a_1).$$

from the first relation

$$v^3 + 3uv^2 = -3u^2v.$$

$\implies$

$$v^3 + 3uv^2 + 3u^2v + u^3 = u^3.$$

$\implies$

$$(u+v)^3 = u^3.$$

This means that the second point of order 3 has he form $(v, v+u)$ where $(u+v)^3 = u^3$. Since $v \neq 0$, we must have $v + u = \rho u$, where ρ is the third primitive root of unity. From the above relation we get $u = (\rho - 1)^{-1}v$.
Since $T^2 + T + 1 = (T - \rho)(T - \rho^2)$. Put $T = 1$
$\implies 3 = (1-\rho)(1-\rho^2)$,
$\implies (1-\rho)^{-1} = \frac{1}{3}(1-\rho^2)$,

We have

$$u = (\rho - 1)^{-1}v = \frac{1}{3}(\rho^2 - 1)v = -\frac{1}{3}(\rho + 2)v.$$

And

$$u + v = \frac{1}{3}(1 - \rho)v.$$

Other point of order 3 *can be generated by* $(0, 0)$ *and* $(v, v + u)$ *i.e* $(v, \frac{1}{3}(1 - \rho)v)$.
We can solve a_1 *and* a_3 *in terms of* v, *and thus obtain a one parameter family of curves with a basis.*

Remark 4.2.5. *The family of cubic curves*

$$E_\gamma = y^2 + a_1(\gamma)xy + a_3(\gamma)y = x^3,$$

where $a_1(\gamma) = 3\gamma - 1$, *and* $a_3(\gamma) = \gamma(\rho - 1)(\gamma - \frac{1}{3}(\rho + 1))$. *Defines for* $\Delta(\gamma) = (a_1(\gamma)^3 - 27a_3(\gamma))a_3(\gamma) \neq 0$,
The family of elliptic curves with basis $(0, 0)$ $(\gamma, \frac{1}{3}(1 - \rho)\gamma)$ *for the subgroup of point of order* 3 *on* E_γ.

4.3 Other Version of Hessian Family

The Hessian family which in homogeneous coordinate takes the form

$$H_\mu \colon u^3 + v^3 + w^3 = 3\mu uvw,$$

and in affine coordinates with $w = -1$, it has the form

$$u^3 + v^3 = 1 - 3\mu uv.$$

If we set $y = -v^3$ and $x = -uv$. We obtain $\frac{x^3}{y} - y = 1 + 3\mu x$,or

$$E_{3\mu} \colon y^2 + 3\mu xy + y = x^3$$

This change of variable defined 3-isogeny of H_μ onto $E_{3\mu}$. There are nine cross section of the family H_μ given by,
$(0, -1, 1)$, $(0, \rho, 1)$, $(0, -\rho^2, 1)$
$(1, 0, -1)$, $(\rho, 0, -\rho^2)$, $(\rho^2, 0, -\rho)$
$(-1, 1, 0)$, $(-1, \rho^2, 0)$, $(1, -\rho, 0)$.
Again ρ is the primitive third root of unity. The family H_μ is nonsingular over the line minus μ_3. Any $0 = (-1, 1, 0)$ can be chosen. These 9 points forms a subgroup of 3- division point of the family H_μ.

4.4 The Jacobi Family

Finally we consider the Jacobi family which along with the Legendre family and the Hessian family, give the three basic classcal family of elliptic curves.The Jacobi family is given by a quartic equation

and we begin by explaining how to transform a quartic equation to a cubic equation.

Remark 4.4.1. *Let $v^2 = f_4(u) = a_0u^4 + a_1u^3 + a_2u^2 + a_3u + a_4$ be a quartic equation. Let*

$$u = \frac{ax+b}{cx+d}$$

and

$$v = y\frac{ad-bc}{(cx+d)^2}$$

v acts like derivative of u, y likes derivative of x. Substituting u and v into the quartic equation we get

$$v^2 = y^2\frac{(ad-bc)^2}{(cx+d)^4} = f_4\frac{(ax+b)}{(cx+d)},$$

Or we can also write as

$$(ad-bc)^2y^2 = f_4(\frac{ax+b}{cx+d})(cx+d)^4$$

$\implies (ad-bc)^2y^2 = a_0(ax+b)^4 + a_1(ax+b)^3(cx+d) + a_2(ax+b)^2(cx+d)^2 + a_3(ax+b)^3(cx+d) + a_4(cx+d)^4$
$\implies (ad-bc)^2y^2 = \sum a_i(ax+b)^{4-i}(cx+d)^i$ *where i is from 0 to 4.*

$\implies (ad-bc)^2y^2 = c^4f_4(\frac{a}{c})x^4 + f_3(x).$
where $f_3(x)$ is a cubic polynomial and the coefficient of x^3 is $c^3f_4'(\frac{a}{c})$.
For $\frac{a}{c}$ is a simple root of f_4 and $ad-bc=1$ we reduce the equation

$$y^2 = f_3(x).$$

Definition 4.4.2 (Jacobi Family)**.** *The Jacobi family of quartic curve is given by*

$$j_\sigma\colon v^2 = (1-\sigma^2u^2)(1-\frac{u^2}{\sigma^2}) = 1 - 2\rho u^2 + u^4,$$

over any field of characteristic different from 2 and here $\rho = \frac{1}{2}(\sigma^2 + \frac{1}{\sigma^2})$ so that $\rho + 1 = \frac{1}{2}(\sigma + \frac{1}{\sigma})^2$. We take the map $j_\sigma \longrightarrow E_\lambda$ where E_λ is the Legendre family of the curve with $\lambda = \frac{1}{4}(\sigma + \frac{1}{\sigma})^2$. by the following change of variables-

$$x = \frac{\sigma^2+1}{2\sigma^2}(\frac{u-\sigma}{u-\frac{1}{\sigma}})$$

and

$$y = \frac{\sigma^4-1}{4\sigma^3}\frac{v}{(u-\frac{1}{\sigma})^2}.$$

The point on j_σ with u-coordinates

$$0, \infty, \pm\sigma, \pm\frac{1}{\sigma}, \pm 1, \pm i$$

maps to the point of order 4 on the elliptic curve E_λ.

4.5 Tate's Normal Form for a Cubic with a Torsion Point

The normal form of elliptic curve

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

. Assume that $(0,0)$ is on the the curve

$$E'\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x,$$

For $(0,0)$ lie on E $a_6 = 0$,The slope at $(0,0)$ is $y' = \dfrac{a_4}{a_3}$.
For slope to be 0, $a_4 = 0$, $a_3 \neq 0$, Since we get

$$E'\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Here, we see that $(0,0)$ is not of point of order 2, and the point $(0,0)$ is point of order 3 if and only if $a_2 = 0$, $a_3 \neq 0$.
Now we assume that $(0,0)$ is not of point of order 2 or 3,
$\implies a_2 \neq 0$, $a_3 \neq 0$
By changing x to u^2x and y to u^3y, We can make $a_3 = a_2 = -b$ and depends upon two parameter.

Definition 4.5.1. *The Tate normal form of an elliptic curve E with point $P = (0,0)$ is*

$$E = E(b,c)\colon y^2 + (1-c)xy - by = x^3 - bx^2.$$

Where b and c are the parameter from the field k.
For the discriminant $\Delta = \Delta(b,c)$ of $E(b,c)$ is

$$\Delta(b,c) = (1-c)^4b^3 - (1-c)^3b^3 - 8(1-c)^2b^4 + 36(1-c)b^4 - 27b^4 + 16b^5.$$

Remark 4.5.2. *The Tate normal form describe equation for the set of pairs (E,P) which consist a elliptic curve E together with a point P on E such that $P, 2P, 3P \neq 0$.*
This P corresponds to the pairs (b,c) with both $b \neq 0$ and $\Delta(b,c) \neq 0$.
$\longrightarrow$ In the two parameter, the Tate family $E(b,c)$, there are some cases where curve has different fibres $E(b,c)$ are isomorphic, for example $E(b,1)$ and $E(b,-1)$ are the isomorphic curves.
For $nP = 0$, for some integer $n > 3$, then the polynomial equation $f_n(b,c) = 0$ over $\mathbb{Z}$, where b and c must satisfy the polynomial equation.
$T_n\colon f_n(b,c) = 0$, $b \neq 0$ $\Delta(b,c) \neq 0$ defines an open algebraic curve with a family $E(b,c)$ of the elliptic curves over it together with a given n distinct point P. this f_n varies and can be defined explicitly.

Remark 4.5.3. *This family contains all elliptic curves with torsion point P of order n upto isomorphism. The curve T_n maps onto open curve $Y_1(n)$*
$Y_1(n)$: Parameter space for isomorphism classes of the pair (E,P) of elliptic curve together with a point P of order n.
$X_1(n)$: The curve $Y_1(n)$ has the completion $X_1(n)$ which is nonsingular where the completing points, called cusps.

Remark 4.5.4. *There is an elliptic curve E over a field k with torsion point P of order n over the field k*
$\Leftrightarrow$ *the open algebraic curve T_n has k rational points.*
$\Leftrightarrow$ *$T_n(k)$ is non empty.*
$\Leftrightarrow$ *$Y_1(n)(k)$ is non empty.*
$\Leftrightarrow$ *$X_1(n)(k)$ has noncuspidal k rational points.*

Corollary 4.5.5. *On the curve*

$$E = E(b,c)\colon y^2 + (1-c)xy - by = x^3 - bx^2.$$

we have points i.e $P = (0,0)$ then $-P = (0,b)$
For $2P = -PP = -(b,o) = (b,bc)$, $-2P = -(b,bc) = (b,0)$,$3P = (c, b-c)$,$-3P = (c,c^2)$, $4P = (d(d-1), d^2(c-d+1))$,$-4P = (d(d-1), d(d-1)^2)$, where $d = \frac{b}{c}$ in the formula for $4P$ and $-4P$. $5P = (de(e-1), d^2e(e-1)^2)$ $-5P = (de(e-1), de^2(d-e))$, where $e = \frac{c}{d-1}$.

4.6 An Explicit 2-Isogeny

Invariant of the Curve $E(a,b)$

For the curve $E(a,b)$ defined by

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

The following holds:

$$c_4 = 16(a^2 - 3b),$$

$$c_6 = 2^5(9ab - 2a^3),$$

$$\Delta = 2^4b^2(a^2 - 4b),$$

$$j = \frac{c_4^3}{\Delta} = 2^8\frac{(a^2-3b)^3}{b^2(a^2-4b)}.$$

The two basic special cases are
(1)- For $j = 12^3$ if and only if $a = 0$, and the curve is $E[0,b] = E[b] : y^2 = x^3 + bx$.
(2)- For $j = 0$ if and only if $3b = a^2 = (3c)^2$ for the characteristic unequal to 3. so the curve is $E[3c, 3c^2] : y^2 = (x+c)^3 - c^3$, and it has the form $y^2 = x^3 - c^3$ after translation of x by c.

observation-

We observe that the function,

$$h(a_1,b_1) = h(a_2,b_2).$$

$\Longrightarrow (-2a_1, a_1^2 - 4b_1) = (-2a_2, a_2^2 - 4b_2)$,
$\Longrightarrow a_1 = a_2, b_1 = b_2$,
Let $(a,b) \in k^2$, Then $\exists$ (c,d) such that $h(c,d) = (a,b)$,
$-2c = a \Longrightarrow c = \frac{-a}{2}$, $d = \frac{a^2-4b}{16}$

$$h^{-1}(a,b) = (\frac{-a}{2}, \frac{a^2-4b}{16})$$

Note-

Here $a^2 - 4b$ is the discriminant of the quadratic $x^2 + ax + b$.

Formula for the 2-Isogeny

The $2-$ Isogeny with kernel $\{0,(0,0)\}$ is given by the
$E[a,b]\colon y^2 = x^3 + ax^2 + bx$
$E[-2a, a^2-4b]\colon y^2 = x^3 - 2ax^2 + (a^2-4b)x = x^3 + \bar{a}x^2 + \bar{b}x$
Where $a' = -2a$, $b' = a^2 - 4b$,
$E[-2a, a^2-4b]\colon y^2 = x^3 - 2\bar{a}x^2 + (\bar{a}^2 - 4\bar{b})x$,
Put the value of $\bar{a}$ and $\bar{b}$ then we get
$E[-2a, a^2-4b]\colon y^2 = x^3 + 4ax^2 + 16bx$,
$E[-2a, a^2-4b] = E[4a, 16b]$.
$x \longrightarrow 4x$, $y \longrightarrow 8y$
$\phi\colon E[a,b] \longrightarrow E[-2a, a^2-4b]$
$\phi(x,y) = (\frac{y^2}{x^2}, y(1 - \frac{b}{x^2}))$.

ϕ is well-defined-

We have to check

$(\frac{y^2}{x^2}, y(1-\frac{b}{x^2}))$ lies on the $E[-2a, a^2-4b]$.

$\implies x'^3 + a'x'^2 + b'x' = x'^3 - 2ax'^2 + (a^2-4b)x'$
$\implies x'^3 + a'x'^2 + b'x' = x'[x'^2 - 2ax' + (a^2-4b)]$

$$\implies x'^3 + a'x'^2 + b'x' = \frac{y^2}{x^2}[\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2-4b)]$$

$$\implies x'^3 + a'x'^2 + b'x' = \frac{y^2}{x^6}[y^4 - 2ay^2x^2 + a^2x^4 - 4bx^4]$$

$$\implies x'^3 + a'x'^2 + b'x' = \frac{y^2}{x^6}[(y^2 - ax^2)^2 - 4bx^4]$$

$$\implies x'^3 + a'x'^2 + b'x' = \frac{y^2}{x^6}[(x^3 + bx)^2 - 4bx^4]$$

$$\implies x'^3 + a'x'^2 + b'x' = \frac{y^2}{x^6}[x^2(x^2-b)^2] = \frac{y^2(x^2-b)^2}{x^4} = y'^2$$

$\phi((0,0)) = 0$, $\phi(0) = 0$ so the kernel is $\{(0,0),0\}$

$\phi\colon E[-2a, a^2-4b] \longrightarrow E[a,b]$.

so that $\hat{\phi}(x,y) = (\frac{y^2}{4x^2}, \frac{y}{8x^2}(x^2 - (a^2 - 4b)))$,

$\hat{\phi}(x,y) = (\frac{1}{4}\frac{y^2}{x^2}, \frac{1}{8}\frac{y}{x^2}(x^2 - b'))$.

Any property which holds for ϕ will also holds for its dual.

Remark 4.6.1. *Now we check that* $\hat{\phi}\phi(P) = 2P$

$\implies \hat{\phi}\phi(x,y) = \hat{\phi}(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$

$\implies \hat{\phi}\phi(x,y) = (\frac{(x^2-b)^2}{4y^2}, \frac{x^2-b}{8x^2y^3}(y^4 - (a^2-4b)x^4))$

Consider tangent line at P *to* $E[a,b]$
$y^2 = x^3 + ax^2 + bx$
differentiating both sides with respect to x *we get*
$\implies 2yy' = 3x^2 + 2ax + b$
$\implies 2yy' = 2x^2 + 2ax + 2b + x^2 - b$
$\implies 2yy' = 3x^2 + 2ax + b$
$\implies 2yy' = 2(x^2 + ax + b) + (x^2 - b)$
$\implies 2yy' = 2\frac{y^2}{x} + (x^2 - b)$
or in other words,
$y' = \frac{y}{x} + \frac{x^2-b}{2y}$
If $2(x_1, y_1) = (x_2, y_2)$ *on* $E[a,b]$*, then the tangent line* $y = \sigma(x - x_1) + y_1$ *to* $E[a,b]$ *at* (x_1, y_1) *must intersect* $E[a,b]$ *at* $(x_2, -y_2)$.
Substitute the value of y *in* $E[a,b]$.
$y^2 = x^3 + ax^2 + bx$
$\implies [\sigma(x - x_1) + y_1]^2 = x^3 + ax^2 + bx,$
$\implies \sigma^2(x - x_1)^2 + y_1^2 + 2\sigma(x - x_1)y_1 = x^3 + ax^2 + bx,$
$\implies x^3 + (a - \sigma^2)x^2 + ... = 0$
where $a = \sigma^2 x_1^2 + y_1^2 - 2\sigma x_1 y_1$
This is repeated root x_1 *so the sum of the root is,*

$$2x_1 + x_2 = \sigma^2 - a.$$

$\implies x_2 = \sigma^2 - a - 2x_1,$

$\implies x_2 = [\frac{y_1}{x_1} + \frac{x_1^2 - b}{2y_1}]^2 - a - 2x_1,$

$\implies x_2 = \frac{(x_1^2 - b)^2}{4y_1^2}$

$y_2 = \sigma(x_2 - x_1) + y_1$

$\implies y_2 = (\frac{y_1}{x_1} + \frac{x_1^2 - b}{2y_1})(\frac{(x_1^2 - b)^2}{4y_1^2} - x_1) + y_1,$

$$\implies y_2 = (x_1^2 - b)\frac{x_1(x_1^2-b)^2 + 2x_1^2y_1^2 - 2by_1^2 - 4x_1^2y_1^2}{8x_1y_1^3},$$

$$\implies y_2 = (x_1^2 - b)\frac{x_1^2(x_1^2-b)^2 - 2y_1^2(y_1^2 - ax_1^2)}{8x_1^2y_1^3}$$

$\implies y_2 = PP$
Now, next we calculate $-PP = (x_2, -y_2)$

$$\implies -y_2 = (x_1^2 - b)\frac{2y_1^2(y_1^2 - ax_1^2) - x_1^2(x_1^2-b)^2}{8x_1^2y_1^3}.$$

Now using $x_1^3 - bx_1 = y_1^2 - ax_1^2 - 2bx_1$,
$\implies 2y_1^2(y_1^2 - ax_1^2) - (y_1^2 - ax_1^2 - 2bx_1)^2$,
Now we get,
$\implies (y_1^4 - (a^2 - 4b)x_1^4)$.
Hence we deduce that $2P = (x_2, y_2) = (\frac{(x_1^2-b)^2}{4y_1^2}, \frac{(y_1^4 - (a^2-4b)x_1^4)(x_1^2-b)}{8x_1^2y_1^3})$,
$2P = \hat{\phi}\phi$.

Proposition 4.6.2. *On the curve* $E[a, b]$ *we have*

$$(0,0) + (x,y) = (\frac{b}{x}, -\frac{by}{x^2}).$$

Proof. For $(x_1, y_1) + (0, 0) = (x_2, y_2)$
Consider the line $y = x\frac{y_1}{x_1}$ through $(0, 0)$ and (x_1, y_1). Now for the third point of interection we compute

$$x^2\frac{y_1^2}{x_1^2} = x^3 + ax^2 + bx,$$

$$\implies x^3 - (\frac{y_1^2}{x_1^2} - a)x^2 + bx = 0.$$

Sum of the root is
$x_1 + x_2 + 0 = \frac{y_1^2}{x_1^2} - a$
$\implies x_2 = \frac{y_1^2 - ax_1^2 - x_1^3}{x_1^2} = \frac{bx_1}{x_1^2} = \frac{b}{x_1}$
And $y_2 = \frac{by_1}{x_1^2}$
$PQ = (x_2, -y_2) = (\frac{b}{x_1}, \frac{-by_1}{x_1^2})$. □

Remark 4.6.3. $\phi((x, y) + (0, 0)) = \phi(x, y)$

Now $\phi((x, y) + (0, 0)) = \phi(\frac{b}{x_1}, \frac{-by_1}{x_1^2})$
$\phi((x, y) + (0, 0)) = (\frac{y_1^2}{x_1^2}, \frac{y_1}{x_1^2}(x_1^2 - b))$.

Proposition 4.6.4. *The function* $\alpha\colon E[a, b] \longrightarrow \frac{k^*}{(k^*)^2}$ *defined by* $\alpha(0) = 1$, $\alpha(0, 0) = b \mod (k^*)^2$, *and* $\alpha((x, y)) = x \mod (k^*)^2$ *is a group homomorphism.*

Proof. Let (x_1, y_1), (x_2, y_2), (x_3, y_3) on $E[a, b]$ on a line $y = \lambda x + \mu$
$\implies (\lambda x + \mu)^2 = x^3 + ax^2 + bx.$
x_1, x_2, x_3 are the roots of the above equation,
so the product of the root $x_1x_2x_3 = \mu^2$
$\alpha(x_1, y_1)\alpha(x_2, y_2)\alpha(x_3, y_3) = x_1x_2x_3 \mod (k*)^2 = 1,$
$\alpha((x, y) + (0, 0)) = \alpha(\frac{b}{x_1}, \frac{-by_1}{x_1^2}) = \frac{b}{x} \mod (k^*)^2 = bx \mod (k^*)^2 = \alpha(0, 0)\alpha(x, y)$
which shows that the α is a group homomorphism.

□

Proposition 4.6.5. *The sequence*

$$E[a, b] \longrightarrow E[-2a, a^2 - 4b] \longrightarrow \frac{k^*}{(k^*)^2}$$

is exact.

Proof. First $\alpha(\phi(x, y)) = \alpha(\frac{y^2}{x^2}, *) = \frac{y^2}{x^2} \mod (k*)^2 = y^2x^2 \mod (k*)^2 = 1$
Next, if $\alpha(x, y) = 1$,i.e.,if $\alpha^2 = t$, then we choose two points.
$(x_+, y_+) = (\frac{1}{2}(t^2 - a + \frac{y}{t}), x_+t)$ and $(x_-, y_-) = (\frac{1}{2}(t^2 - a - \frac{y}{t}), x_-t)$.
We wish to show that $(x_\pm, y_\pm)$ is on $E[a, b]$ and $\phi(x_\pm, y_\pm) = (x, y)$, Where (x, y) is on $E[-2a, a^2-4b]$.
Now,

$$x_+x_- = \frac{1}{4}[(x - a)^2 - \frac{y^2}{x^2}],$$

$$\implies x_+x_- = \frac{x^3 + a^2x - 2ax^2 - y^2}{4x},$$

$$\implies x_+x_- = b$$

since $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$
Now a point (x_i, y_i) for $i = 1, 2$ lies on $E[a, b]$ iff $\frac{(y_\pm)^2}{(x_\pm)^2} = x_\pm + a + \frac{b}{x_\pm}$,
i.e. $\frac{y_1^2}{x_1^2} = x_1 + a + x_2$, and $\frac{y_2^2}{x_2^2} = x_2 + a + x_1$.
But $x_1 + x_2 = t^2 - a$
$\implies x_1 + x_2 + a = t^2$
Now

$$\phi(x_i, y_i) = (x, y)$$

$$\phi(x_i, y_i) = ((\frac{(y_i)^2)}{(x_i)^2}, y_i(1 - \frac{b}{x_i^2})),$$

$$(x_i, y_i) = (t^2, tx_i(1 - \frac{b}{x_i^2})),$$

$$(x_i, y_i) = (x, t(x_i - \frac{b}{x_i})),$$

$$(x_i, y_i) = (x, t(x_\pm - x_\mp)),$$

$$(x_i, y_i) = (x, t(\pm(\frac{y}{t}))) = (x, \pm y).$$

This proves the proposition.

□

Chapter 5

Reduction mod p and torsion point

5.1 Reduction mod p of Projective Space and Curves

Notation

Now we will use the following notation in the next three section. Let R be a factorial ring with field of fraction of k. For each irreducible p in R we form the quotient ring $R/p = R/Rp$ and their field of fraction is to be denoted by $k(p)$.And the each element a in k can be decomposed as a quotient.

$$a = p^n \frac{u}{v},$$

Where p does not divide either u or v and n is an integer which is uniquely determined by a. Let $ord_p(a) = n$ denote the order function associated with p.
The order function satisfy the following property :

$$ord_p(ab) = ord_p(a) + ord_p(b)$$

$$ord_p(a+b) \geq min\{ord_p(a), ord_p(b)\}$$

When

$$ord_p(a) < ord_p(b)$$

$$ord_p(a+b) \geq ord_p(a)$$

$$ord_p(a+b) = ord_p(a).$$

The reduction mod p function

$$r_p \colon R_(p) \longrightarrow k(p)$$

can be defined on affine space by taking products.

$$k^n \supset R_(p)^n \longrightarrow (k(p))^n.$$

This is defined on points $x = (x_1, x_2, ..., x_n)$ such that $ord_p(x_i) > 0$, for all i.

$$r_p(x_1, x_2, ..., x_n) = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_n).$$

Definition 5.1.1. *The reduction mod p function*

$$r_p \colon \mathbb{P}_n(k) \longrightarrow \mathbb{P}_n(k(p)).$$

is defined by the relation.

$$r_p(y_0 \colon, y_1 \colon, ..., y_n) = (\bar{y}_0, \bar{y}_1, ..., \bar{y}_n).$$

where $(y_0 \colon, y_1 \colon, ... \colon y_n)$ is the homogenous coordinate of point in $\mathbb{P}_n(k)$, $y_i \in R$, for every i they don't have a common irreducible factor. Such a representatives $(y_0 \colon, y_1 \colon, ... \colon y_n)$ of a point in $\mathbb{P}_n(k)$ is called p-reduced. There p-reduced representatives are unique upto multiplication by a unit in $R_(p)$.

Remark 5.1.2. *Let $F(y_0, y_1, ..., y_n) \in k[y_0, y_1, ..., y_n]$. Multiply the polynomial F by an appropriate non zero element of k such that the polynomial f all are in R and here no common irreducible factor. Then $\bar{f}(y_0, y_1, ..., y_n)$ is a polynomial over $k(p)$ and coefficient of f are reduced modulo p. $deg\bar{f} = degF$.*

Definition 5.1.3. *Let C be an algebraic curve of degree d in $\mathbb{P}_2$ defined over k.*

$$r_p \colon \mathbb{P}_2(k) \longrightarrow \mathbb{P}_2(k(p)).$$

reduces to,

$$r_p \colon C_f(k) \longrightarrow C_f(k(p)).$$

The reason is that if $(w, x, y) \in C_f(k)$, then $f(w, x, y) = 0$ so $r_p(f(w, x, y)) = \bar{f}(\bar{w}, \bar{x}, \bar{y})$
$\Longrightarrow r_p(f(w, x, y)) = \bar{f}(r_p(w, x, y)) = 0$.

Example 5.2. *Consider the nonsingular conic defined by $wx + py^2 = 0$ reduces to singular conic equals to the union of two lines defined by $wx = 0$.*

Example 5.3. *The conic defined by the $pwx + y^2 = 0$ reduces to $y^2 = 0$ which is a double line.*

Reduction of a Cubic-

Intersection multiplicity $i(P; L, C_f)$ of P on L and C_f it is defined by the following formula,

$$\phi(t) = f(w + tw', x + tx', y + ty'),$$

where $P = (w, x, y)$ and $(w', x', y') \in L - C_f$.
The points of $L \cap C_f$ are of the form $(w + tw', x + tx', y + ty')$ where $\phi(t) = 0$, and order of zero is the intersection multiplicity. Further the order of any P on $C_f \leq i(P; L, C_f)$.
We reduce those constructions,

$$\bar{\phi}(t) = \bar{f}(\bar{w} + t\bar{w}', \bar{x} + t\bar{x}', \bar{y} + t\bar{y}')$$

We must choose (w', x', y') such that $(w', x', y') \in \bar{L} - C_{\bar{f}}$. this is only possible given $\bar{L}$ not contained in $C_{\bar{f}}$.

Remark 5.3.1. *For the above notation we have the following inequalities.*

$$i(P; L, C_f) \leq i(\bar{P}; \bar{L}, C_{\bar{f}});$$

and order of P on C_f is less than or equals to the order of $\bar{P}$ on $C_{\bar{f}}$. For $P = (1, 0, 0)$ origin $(w', x', y') = (0, a, b)$ where constant term is zero.
We get the polynomial

$$\phi(t) = f_r(ta, tb) + ... + f_d(ta, tb)$$

where r is the order of P on curve C_f.

Proposition 5.3.2. *Suppose $P, P' \in L \cap C_f$, where $P \neq P'$ and $\bar{P} = r_p(P) = r_p(P')$.If the order of P on C_f is equals the order of $\bar{P}$ on $C_{\bar{f}}$, then the reduced line $\bar{L}$ is a part of the tangent cone $C_{\bar{f}}$.if $\bar{P}$ has order 1 on $C_{\bar{f}}$, then $\bar{L}$ is tangent line to $C_{\bar{f}}$ at $\bar{P}$.*

Proof. Since $P \in L \cap C_f$ and $ord(P) \geq r$, the polynomial t^r divides $\phi(t)$. Also $P' \in L \cap C_f$
$\Longrightarrow poly.(t - t_o)|\phi(t)$, Since $t^r(t - t_o)|\phi(t)$, $r_p(P) = r_p(P')$
$\Longrightarrow \bar{t_o} mod(p)|\bar{\phi}(t)$
$\Longrightarrow t^{r+1}|\bar{\phi}(t)$ □

5.4 Minimal Normal Forms for an Elliptic Curve

Proposition 5.4.1. *Let k be a field of fraction for an integral domain R, and let E be an elliptic curve over k. Then there is a cubic equation for E in normal form with all $a_i \in R$.*

Proof. Let E be an elliptic curve over k. Choose normal form of E with coefficient $\bar{a_i}$ in variable $\bar{x}$ and $\bar{y}$. Let u be the common denominator for all $\bar{a_i}$, i.e. $u\bar{a_i} \in R$, Using the change of variable $x \longrightarrow u^2\bar{x}$ and $y \longrightarrow u^3\bar{y}$. We get the coefficient $a_i = u^i\bar{a_i}$ is in R for all i. □

Definition 5.4.2. *Let K be a field with a discrete valuation ν, and let E be an elliptic curve over K.A minimal normal form for E is in normal form with all a_j in the valuation ring R of K such that $\nu(\Delta)$ is minimal among all such equation with coefficients a_j in R.*
$\longrightarrow$ Minimal is possible as valuation is greater than 0 on discriminant on the given equation in normal form over R.

Proposition 5.4.3. *Let E and E' be two elliptic curves over K with mimimal models having coefficient a_j and a'_j, respectively. Let $f\colon E \longrightarrow E'$ be an isomorphism with $xf = u^2x' + r$; $yf = u^3y' + su^2x' + t$, Then $\nu(\Delta) = \nu(\Delta')$, $u \in R^*$ and $r, s, t \in R$, The differential ω is unique up to a unit in R.*

Proof. The equality $\nu(\Delta) = \nu(\Delta')$ by the definition of minimal, and hence
$\Longrightarrow \nu(u) = 0$
$\Longrightarrow u$ is a unit in R ($u^{12}\Delta' = \Delta$). The relation $u^8b'_8 = b_8 + 3rb_6 + 3r^2b_4 + 3r^4$,implies that $3r$ is in R, and $u^6b'_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3$ in R implies $4r$ is in R. Hence the diffrence r is in R.
$u^2a'_2 = a_2 - sa_1 + 3r - s^2$ implies s is in R
$u^6a'_6 = a_6 + sa_4 + a_2s^2 + r^3 - ta_3 - sta_1 - t^2$ implies t is in R
and the last assertion follows from the formula $\omega f = u^{-1}\omega'$.

□

Proposition 5.4.4. *If all a_j are in R, and if $0 \leq \nu(\Delta) < 12$, then the model is minimal.*

Note-

If $P^4|A$ and $P^6|B$ in R,then the equation $y^2 = x^3+Ax+B$ is not minimal. All elements of $K = j(E)$, for some E over K,implies that $j(E)$ is not in R for all E.

Proposition 5.4.5. *Let E be an elliptic curve over K and assume that characteristic of K are not equals to the 2 and 3. For a minimal model the valuation of discriminant satisfies*

$$v(\Delta) + min\{v(j), 0\} < 12 + 12v(2) + 6v(3).$$

In addition,assuming that the residue class characteristic is different from 2 and 3, it follows that a model over R is minimal iff $v(\Delta) + min\{v(j), 0\} < 12$.

Proof. We know,

$$c_4^3 = \Delta j$$

and,

$$c_6^2 = \Delta(j - 12^3)$$

We have the relation

$$v(\Delta) + v(j) = 3v(c_4)$$

and,

$$v(\Delta) + v(j - 12^3) = 2v(c_6).$$

And the equation of the cubic can be transformed into the form

$$(y)^2 = (x)^3 - x(\frac{c_4}{48}) - \frac{c_6}{864}.$$

If $48P^4|c_4$ and $864P^6|c_6$, then equation is not minimal.But as equation is minimal and since $48 = 2^4.3$ and $864 = 2^5.3^3$,
it follows that

$$v(\Delta) + v(j) = 3v(c_4) < 12 + 3v(48) = 12 + 12v(2) + 3v(3),$$

or

$$v(\Delta) + v(j - 12^3) = 6v(c_6) < 12 + 2v(864) = 12 + 10v(2) + 6v(3).$$

Since, $v(\Delta) + min\{v(j), 0\} \leq v(\Delta) + v(j)$
or, $v(\Delta) + min\{v(j), 0\} \leq v(\Delta) + v(j - 12^3)$. ,We obtain the inequality

$$v(\Delta) + min\{v(j), 0\} < 12 + 12v(2) + 6v(3).$$

Now observe that for $v(2) = v(3) = 0$
The minimal model satisfies $v(\Delta) + min\{v(j), 0\} < 12$.and the converse holds for the above proposition

$$0 < v(\Delta) + min\{v(j), 0\}.$$

Then model is minimal. □

Now suppose R-factorial ring, with field of fraction k. two normal forms for E with coefficient a_j in R are related by the admissible change of variables. $u^{12}\bar{\Delta} = \Delta$
For an irreducible element p in R, we have

$$ord_p(\Delta) = 12ord_p(u) + ord_p(\bar{\Delta}).$$

Since, by a change of variable we can always choose an equation whre $ord_p(\Delta)$ is minimal for all irreducible p in R.

Definition 5.4.6. *Let k be the field of fractions of a factorial ring R, and let E be an elliptic curve over k. A minimal normal form for E is a normal form with all $a_j \in R$ such that $ord_p(\Delta)$ is minimal among all equation in normal form with coefficient $a_j \in R$.*

5.5 Good Reduction of Elliptic Curves

Notation-

For an irreducible p a canonical reduction homomorphism $r_p \colon R_(p) \longrightarrow k(p)$ denoted by $r_p(a) = \bar{a}$.

Definition 5.5.1. *Let E be an elliptic curve over k with minimal normal form*

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

.The reduction $\bar{E}$ of E modulo p is given by

$$y^2 + \bar{a_1}xy + \bar{a_3}y = x^3 + \bar{a_2}x^2 + \bar{a_4}x + \bar{a_6}$$

.Now it is a plane cubic curve over $k(p)$.and $\bar{E}$ is also denoted by E_p.

Note-

The normal form of an equation E only has to be minimal at p.
Now observe that an admissible change of variable between two minimal normal form of E at p is given by $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ over $R_(p)$ reduced to $x = \bar{u^2}x' + \bar{r}$, $y = \bar{u^3}y' + \bar{s}\bar{u^2}x' + \bar{t}$ for $\bar{E}$ over $k(p)$.

Remark 5.5.2. *Now for the above notation the discriminant of the reduced curve $\bar{E}$ is $\bar{\Delta}$. Clearly $\bar{E}$ is nonsingular iff $\bar{\Delta} \neq 0$ or equivalently $ord_p(\Delta) = 0$.*

Definition 5.5.3. *An elliptic curve E over k has a good reduction at p given $\bar{E}$, the reduced curve at p, is nonsingular. and $\bar{E}$ is singular, we say E has a bad reduction at p.*
In general the reducttion function

$$r_p \colon \mathbb{P}_2(k) \longrightarrow \mathbb{P}_2(k(p))$$

restrict to

$$r_p \colon E(k) \longrightarrow \bar{E}(k(p)).$$

Proposition 5.5.4. *Let E be an elliptic curve over k with good reduction at p. Then the reduction function $r_p \colon E(k) \longrightarrow \bar{E}(k(p))$ is a group morphism.*

Proof. Clearly $r_p(0:0:1) = 0:0:1$ so that zero is preserved.
for $P, Q \in E(k)$ and let L be a line through P and Q when $P \neq Q$ and the tangent line to E at P when $P = Q$. then L reduces to L', the line through $r_p(P)$ and $r_p(Q)$.
Again L' is tangent to E' at $r_p(P)$ when $r_p(P) = r_p(Q)$.Now if PQ denote as usual the third intersection point of L with $\bar{E}$, then we have

$$r_p(PQ) = r_p((PQ)O) = (r_p(P)r_p(Q)r_p(O)) = r_p(P) + r_p(Q),$$

and thus r_p is a group morphism. □

Remark 5.5.5. *Since $0 = 0:0:1$ on both E and the reduced curve over $k(p)$,we see that the $p-$reduced $w:x:y$ on $E(k)$ is in $ker(r_p)$ if and only if $ord_p(y) = 0$, $ord_p(x) > 0$, and $ord_p(w) > 0$. in fact, we should divide by y and assume that the point is of the form $w:x:1$, where w and x have strictly positive ordinal at p.*

Example 5.6. *If the minimal normal form of an elliptic curve E is of the form $y^2 = f(x)$ over k , where $f(x)$ is a cubic polynomial, then E has a bad reduction at all p where $k(p)$ has characteristic 2 and at all irreducibles p which divide the discriminant $D(f)$ of the cubic $f(x)$.*

Example 5.7. *If the minimal normal form of an elliptic curve E over k is*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma),$$

then no p^2 divides the all roots α, β, and γ for any irreducible p. The elliptic curve E has good reduction at $p > 2$ if and only if p does ot divide any of the diffrence $\alpha - \beta$, $\beta - \gamma$, $\gamma - \alpha$.

5.8 The Kernel of Reduction mod p

Now In this section, we define a few results on the kernel of reduction map and the p-adic filtration. This is very useful for studying torsion points of an elliptic curves. We use some notations which we described above and the reduction map is as defined in the previous section. Now in the end the following proposition gives some result on relation between the order function valuation.

Proposition 5.8.1. *Let $(w, x, 1)$ be a point on the elliptic curve $E(k)$. If $ord_p(w) > 0$, then $ord_p(x) > 0$ and $ord_p(w) = 3ord_p(x)$ holds.*

Proof. The projective normal form for $y = 1$ for cubic equation of E is $w + a_1wx + a_3w^2 = x^3 + a_2w^2 + a_4w^2x + a_6w^3$. Let L denote the LHS of this equation and R denote the RHS. We have, $ord_p(w) > 0$. We have to prove $ord_p(x)$ is positive. We prove this by contradiction. Let if possible $ord_p(x) \leq 0$. Then $ord_p(R) = ord_p(x^3 + a_2wx^2 + a_4w^2 + a_6w^2) = ord_p(x^3) = 3ord_p(x) \leq 0$. On the other hand, $ord_p(L) = min\{ord_p(w), ord_p(a_1wx), ord_p(a_3w^2)\} = min\{ord_p(w), ord_p(a_1) + ord_p(w) + ord_p(x), ord_p(a_3) + 2ord_p(w)\}$. Since $ord_p(w) > 0$, we have $3ord_p(x) \geq ord_p(x) + ord_p(w)$. This gives $0 \geq 2ord_p(w) \geq ord_p(w)$. It follows that $ord_p(w) \leq 0$ which is a contradiction.

For the second part, $ord_p(w) = ord_p(q + a_1w + a_3w^2)$, because $ord_p(w)$ is less than $min\{ord_p(a_1w^x), ord_p(a_3w^2)\}$. Hence $ord_p(w) = ord_p(R) = 3ord_p(x)$. □

Definition 5.8.2. *(p-adic filtration on E) Let $E(k)$ be an elliptic curve defined by cubic in normal form. The p-adic filtration on E is a sequence of subgroups $E^{(n)}(k)$ which is defined as $(w : x : 1) \in E^{(n)}$ if $ord_p(w) > 0$ and $ord_p(x) \geq n$.*

Now the next proposition which gives some results on order function valuations at coordinates of some different points of intersection of a line with elliptic curve over the feild k i.e.$E(k)$.

Proposition 5.8.3. *Let $P = (w : x : 1)$, $P' = (w' : x', 1)$, $P'' = (w'' : x'' : 1)$ be three points of intersection of E with L, where E is elliptic curve defined by cubic in normal form. If $P, P' \in E^{(n)}(k)$ for $n \geq 1$, then $ord_p(x + x' + x'') \geq 2n$ and $ord_p(w'') = 3ord_p(w'') \geq 3n$.*

Proof. We take $w = cx + b$ as the equation of line L through the three points P, P', P''. We aim to calculate c and $ord_p(c)$ using equation of cubic.

First we consider the case when $P \neq P'$. Then $c = \frac{w-w'}{x-x'}$ is the slope of L. Consider the two equations $E_1 : w + a_1wx + a_3w^2 = x^3 + a_2wx^2 + a_4w^2x + a_6w^3$ and $E_2 : w' + a_1w'x' + a_3w'^2 = x'^3 + a_2w'x'^2 + a_4w'^2x' + a_6w'^3$. Consider $E_3 = E_1 - E_2 : (w - w') + a_1(wx - w'x') + a_3(w^2 - w'^2) = (x^3 - x'^3) + a_2(wx^2 - w'x'^2) + a_4(w^2x - w'^2x') + a_6(w^3 - w'^3) = (x - x')(x'^2 + xx' + x'^2) + \dots$. Each of the terms is of the form $w^a x^b - w'^a x'^b = w^a x^b - w'^a x'^b$, which we can write as $(w^a - w'^a)x^b + w'^a(x^b - x'^b)$. From the equation of E_3, we get, $(w - w')(1 + a_1x + a_3(w + w')) = (x - x')(x^2 + xx' + \dots)$. Thus, $(w - w')(1 + u) = (x - x')(x^2 + xx' + x'^2 + v)$ for $u, v \in k$, where $ord_p(u) > 0$, so, $ord_p(u + 1) = 0$. Also, each term of v is divisible by some w or w', so $ord_p(v) \geq 3n$. Since, $ord_p(x)$ and $ord_p(x') \geq n$, therefore, $ord_p(x^2 + xx' + x'^2 + v) \geq 2n$ as all the quantities are greater than or equal to $2n$. Thus we obtain $ord_p(c) = ord_p(\frac{w-w'}{x-x'}) \geq ord_p(x^2 + xx' + x'^2 - v) - ord_p(1 + u) \geq 2n$.

Next consider the case when $P = P'$, then the slope of tangent line is $c = \frac{dw}{dx}$. Differentiating E_1 with respect to x implicitly, we get $\frac{dw}{dx} + a_1(w + x\frac{dw}{dx}) + 2a_3\frac{dw}{dx}) = 3x^2 + a_2(2wx + x^2\frac{dw}{dx}) + a_4(w^2 + 2wx\frac{dw}{dx}) + 3a_6w^2(\frac{dw}{dx})$. This gives us $(1 + a_1x + 2a_3w - a_2x^2 - 2a_4wx - 3a_6w^2)\frac{dw}{dx} = 3x^2 + 2a_2wx + a_4w^2 - a_1w$. Coefficient of $\frac{dw}{dx}$ is of the form $1+u$, where $ord_p(u) > 0$, so, $ord_p(1+u) = 0$. RHS of the above equation is of the form $3x^2 + v$, where $ord_p(3x^2 + v) \geq ord_p(3x^2) \geq 2ord_p(x)$. Now since $ord_p(w) = 3n$, we have, $ord_p(c) = ord_p(\frac{dw}{dx}) = ord_p(3x^2 + v) \geq 2n$.

Therefore, in both the cases, we get $ord_p(c) \geq 2n$. From equation of line L, we have $b = w - cx$. Therefore, $ord_p(b) \geq min\{ord_p(w), ord_p(c) + ord_p(x)\} \geq 3n$.

Now to estimate the $ord_p(x + x' + x'')$, we first substitute the equation of line L through P and P' in the equation of cubic E_1. We get, $(cx + b) + a_1(cx + b)x + a_3(cx + b)^2 = x^3 + a_2(cx + b)^2 + a_4(cx + b)x + a_6(cx + b)^3$. This gives us a polynomial equation in x, and the sum of root of this polynomial equation is $x + x' + x'' = -\frac{a_2b + 2a_4bc + 3a_6bc^2 - a_1c - a_3c^2}{1 + a_2c + a_4c^2 + a_6c^3}$. Take $u = a_2c + a_4c^2 + a_6c^3$. Therefore, we get, $ord_p(1 + u) = 0$. It follows that $ord_p(x + x' + x'') \geq 2n$. We also observe that $x'' = x + x' + x'' - x - x'$, so $ord_p(x'') \geq min\{ord_p(x + x' + x''), ord_p(-x), ord_p(-x')\} \geq n$. Since $w = cx + b$, we have $ord_p(w'') \geq 3n$, and thus $(w'', x'', 1) \in E^{(n)}(k)$. This proves the proposition.

□

Remark 5.8.4. *From proposition 5.4.1 and 5.4.3, it follows that $ord_p(x + x' + x'') \geq 3n$ whenever $a_1 = 0$.*

Theorem 5.8.5. *If E is an elliptic curve in normal form over k with p-adic filtration $E^{(n)}(k)$ on $E(k)$. Then $E^{(n)}(k)$ are subgroups. Moreover, if P is a function defined from $E^{(n)}(k)$ to p^nR such that $P(w, x, 1) = x(P)$ is composed with the quotient morphism $p_nR \to p_nR/p^{2n}R$ defines*

a group morphism from $E^{(n)}(k)$ to p^nR/p^{2n} with kernel in $E^{(2n)}(k)$ induces a monomorphism $E^{(n)}R/E^{(2n)}R \to p^nR/p^{2n}R$ for $n \geq 1$.

Remark 5.8.6. *From this theorem, we conclude that if $a_1 = 0$, then we get an injective map from $\frac{E^{(n)}(k)}{E^{2n}(k)}$ to $\frac{p^nR}{p^{3n}}R$.*

5.9 Torsion in Elliptic Curve over $\mathbb{Q}$: Nagell-Lutz Theorem

Notation-

Let A_{tors} denote the torsion subgrop of an abellian group A.

Theorem 5.9.1. *(Nagell-Lutz Theorem) Let E be an elliptic curve over $\mathbb{Q}$.*
(1)- Subgroup $E(\mathbb{Q})_{tors} \cap E^1(\mathbb{Q}) = 0$ for odd prime p and the Subgroup $E(\mathbb{Q})_{tors} \cap E^2(\mathbb{Q}) = 0$ for prime $p = 2$.
(2)− The restriction of the reduction homomorphism $r_p|E(\mathbb{Q})_{tors}\colon E(\mathbb{Q})_{tors} \longrightarrow E_p(F_p)$ is injective for any odd prime p where E has a good reduction and $r_2|E(\mathbb{Q})_{tors}\colon E(\mathbb{Q})_{tors} \longrightarrow E_2(F_2)$ has kernel at most $\mathbb{Z}/2\mathbb{Z}$ when E has a good reduction at 2.

Proof. The function

$$x \longmapsto x(T)$$

defines a monomorphism and

$$E^n(\mathbb{Q})/E^{2n}(\mathbb{Q}) \longmapsto \mathbb{Z}p^n/\mathbb{Z}p^{2n} \cong \mathbb{Z}/p\mathbb{Z},$$

and this implies that there is no torsion prime to p in $E^{(1)}(\mathbb{Q})$ prime to p. Assume that $pT = 0$ where $T \in E^{(r)}(\mathbb{Q}) - E^{(r+1)}(\mathbb{Q})$ and $r > 1$
if p is odd then

$$0 = x(pT) \equiv p(xT) \mod p^{3r}$$

Hence $x(T) \in p^{3r-1}\mathbb{Z}$ and this means that $T \in E^{3r-1}\mathbb{Q}$ implies that $r \geq 3r - 1$ so that $r = 0$.
If $p = 2$ so we use

$$0 = x(2T) \equiv 2(xT) \mod 2^{2r}$$

Hence $x(T) \in 2^{2r-1}\mathbb{Z}$ and this means that $T \in E^{2r-1}\mathbb{Q}$ implies that $r = 2r - 1$ so that $r = 1$.
Hence $E(\mathbb{Q})_{tors} \cap E^1(\mathbb{Q}) = 0$ for p odd and with $E^1(\mathbb{Q})$ for $p = 2$.

For the second assertion recall that

$$ker(r_p) = E^1(\mathbb{Q}).$$

Now we use the first assertion then we get the group $E(\mathbb{Q})_{tors} \cap E^1(\mathbb{Q})/E^2(\mathbb{Q})$ injects to the $2\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$. □

Remark 5.9.2. *If C is a cubic curve defined by an equation over $\mathbb{F}_q$ in normal form, then for each x in $\mathbb{F}_q$ we have at most two possible (x, y) on the curve $C(\mathbb{F}_q)$ and so the cardinality is less than or equal to $2q + 1$.*

Corollary 5.9.3. *Let E be an elliptic curve over the set of rational numbers. if E has good reduction at an odd prime p, then the cardinality of the torsion subgroup satisfies $|E(\mathbb{Q})_{tors}| \leq 2p+1$. if E has a good reduction at 2 then $|E(\mathbb{Q})_{tors}| \leq 10$.*

Corollary 5.9.4. *For an elliptic curve E over Q, the torsion subgroup $E(\mathbb{Q})_{tors}$ of $E(\mathbb{Q})$ is finite and is either cyclic or cyclic direct sum with $\mathbb{Z}/2\mathbb{Z}$.*

5.10 Computability of Torsion Points on Elliptic Curves from Integrability and Divisibility Properties of coordinates

Theorem 5.10.1. *Let E be an elliptic curve defines over the rational numbers in normal form with integer coefficient. if $(x,y) \in \mathbb{Q}_{tors}$, then the coordinates x and y are integers.*

Proof. if $y = 0$ then the x is a solution of the cubic equation in normal form.

$$0 = x^3 + a_2x^2 + a_4x + a_6.$$

With integer coefficients. Since x is a rational number, and so it is also an integer number i.e. x is of the form $x = \frac{m}{n}$ so the equation which is of the form

$$m^3 + a_2m^2n + a_4mn^2 + a_6n^3 = 0,$$

and any prime which divides n must divide m also. Thus we have to taken an integer which is of the form $x = m$. Now we have to take the second condition.
if $y \neq 0$, then the point with homogeneous coordinate is of the form $(w : x' : 1) = (1 : x : y)$, where the $w = \frac{1}{y}$ and $x' = \frac{x}{y}$, so we have $(w : x' : 1) \in r_p^{-1}(0)$ where p is odd and $(w : x' : 1) \in E^2(\mathbb{Q})$at 2. Now in other words we have $ord_p(w) \leq 0$ for p is odd and $ord_2(w) \leq -1$ at 2. This condition becomes from the relation $ord_p(y) \geq 0$ for all p odd and $ord_2(y) \geq -1$ at 2. Now y is of the form $y = \frac{h}{2}$ for an integer h. Again take $x = \frac{m}{n}$, and x saisfies the cubic equation with the coefficient of x^3 is 1, and the coefficient of x^2 is an integer, and coeffcient of x is an integer over 2, and the constant term is an integer over 4. the change, using 2, shows $x = m$ and that $x = m$ and h is an even. This proves the theorem. □

Theorem 5.10.2. *Let E be an ellliptic curve over $\mathbb{Q}$, and let Weierstrass equation of the form $y^2 = f(x)$ for E and here $f(x)$ has an integer coefficient. if the point (x,y) is a torsion point on E, then the integer y is zero or y divides $D(f)$, where $D(f)$ is the discriminant of the cubic polynomial.*

Proof. if $y = 0$, then $(x, 0)$ is of order 2 and thus 0 divides the discriminant. Otherwise, $2(x,y) = (\bar{x}, \bar{y})$ not equals to zero on an elliptic curve over the rational numbers $E(\mathbb{Q})$. The tangent line to E has slope $f'(x)/2y$, and substituted $y = \lambda x + \beta$ into the Weierstrass form of an equation and thus we obtain the cubic equation with x has the double root and $\bar{x}$ has the single root.
Hence the sum of the root is

$$2x + \bar{x} = a - (\frac{f'(x)}{2y})^2.$$

Since x , $\bar{x}$ and a are integers , it follows that $f'(x)/2y$ is an integer, and $2y|f'(x)$.
Now, we can write the discriminant $D(f)$of $f(x)$ as a linear combination $D(f) = u(x)f(x)+v(x)f'(x)$,

where the $u(x), v(x) \in \mathbb{Z}[x]$. Since $y = f(x)$ and $y|f'(x)$ for the points (x, y) on E, Now we infer that $y|D(f)$. This proves the theorem. □

Remark 5.10.3. *For finding the $E(\mathbb{Q})_{tors}$ is to take for E a Weierstrass equation $y^2 = f(x)$ where $f(x)$ is a cubic polynomial and the coefficient of a, b and c are the integers. Consider the finite set of all divisors y_o of $D(f)$. Solve the cubic $y_o^2 = f(x)$ for the integer solution x_o. Among these (x_o, y_o) are all points of $E(Q)_{tors}$ whic are not equals to zero.*

Remark 5.10.4. *If $(x, y) \in E(\mathbb{Q})$ such that some multiple $n(x, y)$ has nonintegral coefficients, then (x, y) is not a torsion point.*

5.11 Bad Reduction and Potentially Good Reduction

Definition 5.11.1. *An elliptic curve $E(k)$ has:*
(1)− *Multiplicative reduction at p given the reduction $E_(p)$ has a double point or node.*
(2)− *Additive reduction or unstable reduction at p provided the reduction $E_(p)$ has a cusp.*

Remark 5.11.2. *Let $E(k)$ with discriminant Δ and having bad reduction at p, i.e., $ord_p(\bar{\Delta}) > 0.or$ $\bar{\Delta} = 0$ The reduction is:*
(1)− *multiplicative reduction iff $ord_p(c_4) = 0$ or, equivalently, $ord_p(b_2) = 0$.*
(2)− *additive reduction iff $ord_p(c_4) > 0$ or, equivalently, $ord_p(b_2) > 0$.*

Remark 5.11.3. *Let $E(k)$ with good reduction at p. Then the reduction modulo p of $j(E)$ is given by $r_p(j(E)) = j(E_(p))$ and $ord_p(j(E)) \geq 0$. We have two congruence relation.*

$$ord_p(j(E)) \equiv 0 \mod 3$$

and

$$ord_p(j(E) - 12^3) \equiv 0 \mod 2.$$

since $j(E) = c_4^3/\Delta$, $j(E) - 12^3 = c_6^2/\Delta$, and $12^3\Delta = c_4^3 - c_6^2$. Conversely, if $ord_p(j - 12^3) = 0 = ord_p(j)$, then the equation

$$y^2 + xy = x^3 - x\frac{12^3}{j - 12^3} - \frac{1}{j - 12^3}.$$

shows that the curve has the same j invariant which is defined over k.

Definition 5.11.4. *An elliptic curve over K has potential good reduction provided there exist a finite extension L and an extension w of v to L such that E over L has the good reduction at the valuation ψ.*

Theorem 5.11.5. *An elliptic curve E defined K has potentially good reduction iff $j(E)$ is a local integers, i.e., $\psi(j(E)) \geq 0$.*

5.12 Tate's Theorem on Good Reduction over the Rational Numbers

Theorem 5.12.1. *Every elliptic curve E over the rational numbers $\mathbb{Q}$ has bad reduction at some prime, i.e., Δ cannot be equal to ± 1.*

Proof. Assume that $\Delta = \pm 1$ such that

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 - 9b_2 b_4 b_6,$$

and

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = a_1 a_3 + 2a_4.$$

if a_1 is even, then $4|b_2$ and $2|b_4$ so that b_6 will have to be odd, and in fact, $\pm 1 = \Delta \equiv 5b_6^2 (mod 8)$. Since any square modulo 8 is congruent to 0, 1, 4 $mod(8)$, this is not possible.
If a_1 is odd, and hence b_2 is also odd. Then the coefficient $c_4 = b_2^2 - 24b_4 \equiv 1(mod 8)$. Now we write $c_4 = x \pm 12$ from the relation $c_4^3 - c_6^2 = 12^3\Delta = \pm 12^3$, and thus

$$c_6^2 = x(x^2 \pm 36x + 3.12^3) \equiv x^2(x+4) \mod 8.$$

it means that $x \equiv 5 \mod 8$. Now $3|x$, for otherwise any $p|x$ with $p > 3$, it would follow that $p^2|x$ and $\pm x$ would be a square. so this contradicts that $x \equiv 5 \mod 8$.
Let $x = 3y$ so that $y \equiv 7 \mod (8)$ and hence $c_6 = 9c$

$$3c^2 = y(y^2 \pm 12y + 4.12^3) = y((y \pm 6)^2 + 540).$$

Now $y > 0$ Since $y((y \pm 6)^2 + 540)$ is positive. if p not equal to 3 divides y, so it does so to an even power.
Also the relation for $3c^2$ shows that if $3|y$, then $27|3c^2$. In this case let $y = 3z$ and $c = 3d$ which leads to

$$d^2 = z(z^2 \pm 4z + 64)$$

From the relation for $3c^2$. if an odd prime $p|z$, then $p^2|z$ and $z|8$ is a square. But $y \equiv 7 \mod 8$ this implies that $z \equiv 5 \mod (8)$ which contradicts the facts that z is a square. □

Example 5.13. *The following curve*

$$y^2 + xy + \epsilon^2 y = x^3,$$

where $\epsilon = \dfrac{5+\sqrt{29}}{2}$ *over* $K = \mathbb{Q}\sqrt{29}$ *was shown by Tate to have good reduction at all place of* K, *and* $\Delta = -\epsilon^{10}$.

Chapter 6

Proof of Mordell-Weil Theorem

In this chapter, we see the proof of Mordell-Weil's theorem. The Mordell-Weil's Theorem is essential in the theory of elliptic curves as this results tells us that the group of elliptic curves is finitely generated. We set up a few results used in proving the theorem, and finally prove the Mordell-weil theorem.

6.1 Some Preliminary Ideas

Definition 6.1.1. *A Norm function on an abelian group A is defined as a function from $A \longrightarrow R$ such that it satisfies the following properties:*
(1) $|P| \geq 0$ $\forall P \in A$, *and for the each real numbers r such that $|P| \leq r$ is finite.*
(2) $|mP| = |m||P|$ *for all $P \in A$ and $m \in \mathbb{Z}$.*
(3) $|P + Q| \leq |P| + |Q|$ $\forall P, Q \in A$.

Proposition 6.1.2. *An abelian group G is finitely generated if and only if the index $(G : mG)$ is finite for some $m > 1$ and the group G has a norm function.*

Proof. Firstly suppose that the group G be finitely generated. And we know that if G is finitely generated, the index $(G : mG)$ is finite for all non zero m. Now the norm function can be constructed as follows. As G is finitely generated group has norm function since, $G \cong \mathbb{Z}^n \times Tors(G)$. If $P \in G$, then we can write P as $(P_1, P_2, \ldots P_n)$, where the each $P_i \in \mathbb{Z}$. The norm function on $\mathbb{Z}$ is $|.|$. Then the norm function on G can be defined as $|P| = |P_1|_1 + |P_2|_2 + \cdots + |P_n|_n$.
Conversely, Now assume that the index $(G : mG)$ is finite, i.e. it ust be equals to n and G has a norm function. And we have, $\dfrac{G}{M} = \{P + mG \mid P \in G\}$. Let $R_1, R_2, \ldots, R_n$ be the coset representatives of $\dfrac{G}{mG}$. We also let $c = \max |R_i| + 1$, $X = \{P \in A || P| \leq c\}$ and $A = \langle P_1, P_2, \ldots, P_k \rangle$, where $P_i \in X$.

Suppose if it is possible take $G - A$ is as non empty set. So, there exists a $P \in G - A$. Then by the first point of the definition of norm, P has a minimal norm. For some coset representative R_i of $G - mG$, $P \equiv R_i mod(mG)$. This means $P_i = R_i + mQ$ for some $Q \in G$. This implies $mQ = P - R_i = P + (-R_i)$. Hence, $m|Q| = |mQ| \leq |P| + |R_i| < |P| + c \leq m|P|$. Therefore, $|Q| \leq |P|$. But we know that the P has a minimal norm and that $P \in G - A$. It follows that $Q \in G$ and $P = R_i + mQ \in G$. Thus if any element is in G, it also has to be in A, which a contradiction

to the fact that $G - A$ is non empty. Therefore, $G = A = \langle X_i \rangle$, where $X_i \in X$. Thus, the group G is finitely generated by elements of X.

□

6.2 Finiteness of $(E(\mathbb{Q} : 2E(\mathbb{Q}))$ for $E[a, b]$

Here, $E[a, b]$ is defined by $y^2 = x^3 + ax^2 + bx$ for all $a, b \in k$. So our aim is to show that $(E(\mathbb{Q} : 2E(\mathbb{Q}))$ is finite for an elliptic curve of the form $y^2 = x^3 + ax^2 + bx$.
(1)- The function $\alpha : E[a, b] \longrightarrow \dfrac{k^*}{(k^*)^2}$ defined with

$$\alpha(0) = 1,$$

$$\alpha((0, 0)) = bmod(k^*)^2,$$

$$\alpha((x, y)) = xmod(k^*)^2$$

for $x \neq 0$ is a group homomorphism.
(2)− The sequence

$$E[a, b] \xrightarrow{n} E[-2a, a^2 - 4b] \xrightarrow{\alpha} \frac{k^*}{(k^*)^2}$$

is exact.

$$\phi(x, y) = (\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}).$$

For $K = \mathbb{Q}$, the field of rational numbers, The quotient group $\dfrac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$ is a vector space over $\mathbb{F}_2$ with a basis $= -1 \cup p$ where p is a prime numbers.

Proposition 6.2.1. *Let $E[a, b]$ is an be an elliptic curve over the rational numbers $\mathbb{Q}$. The homomorphism $\alpha : E[a, b] \longrightarrow \dfrac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$ has image $im(\alpha) \in W$, where W is a subspace of $\mathbb{F}_2$.*
if r distinct primes divides b,

$$|im(\alpha)| < 2^{r+1}.$$

Theorem 6.2.2. *Let $a, b \in \mathbb{Z}$, with $\Delta = 2^4 b^2(a^2 - 4b) \neq 0$, and let r is number distinct primes divisors of b and s is number of distinct primes divisor of $a^2 - 4b$. Then for $E[a, b] = E$ we have*

$$(E(\mathbb{Q} : 2E(\mathbb{Q})) \leq 2^{r+s+2}.$$

Proof. The sequence

$$E[a, b] \xrightarrow{\phi} E[-2a, a^2 - 4b] \xrightarrow{\phi'} E[a, b]$$

here α_1 and α_2 are induced isomorphisms.

$$\frac{E(\mathbb{Q})}{\phi'(E'(\mathbb{Q}))} \longrightarrow im(\alpha_1)$$

$$\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow im(\alpha_2)$$

(1)− for α_1 we take the sequence

$$E' \xrightarrow{\phi'} E \xrightarrow{\alpha_1} \frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}.$$

here $im(\phi)' = ker(\alpha_1)$ by the isomorphism theorem we have $\frac{E'}{ker(\alpha_1)} \longrightarrow im(\alpha_1)$ and $ker(\alpha) = im(\phi') = \phi'(E'(\mathbb{Q}))$.
(2)− for α_2 we take the sequence

$$E \xrightarrow{\phi} E' \xrightarrow{\alpha_2} im(\alpha_2).$$

here $im(\phi) = ker(\alpha_2)$ so by the isomorphism theorem $\frac{E'}{ker(\alpha_2)} \longrightarrow im(\alpha_2)$ and $im(\phi) = \phi(E)$. Also ϕ' induced to an isomorphism

$$\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{\phi'(E'(\mathbb{Q}))} = \frac{E(\mathbb{Q})}{2E(\mathbb{Q})}.$$

there is a 2-stage filtration

$$\phi'\phi E(\mathbb{Q}) = 2E(\mathbb{Q}) \subset \phi'(E(\mathbb{Q})) \subset E(\mathbb{Q}).$$

it follows that the index

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = |im(\alpha_1)||im(\alpha_2)| \leq 2^{r+1}.2^{s+1} = 2^{r+s+2}$$

□

6.3 Finiteness of the index $(E(k) : 2E(k))$

Theorem 6.3.1. *Suppose E be an elliptic curve over an algebraic number field k. Then index $(E(k) : 2E(k))$ is finite.*

6.4 Quasilinear and Quasiauadratic Maps

Definition 6.4.1. *For a set X a function $h : X \longrightarrow \mathbb{R}$ is proper function given $h^{-1}([-c, c])$ is finite for all $c \geq 0$.*

Definition 6.4.2. *Two function h and h' are equivalent if the map $h, h' : X \longrightarrow \mathbb{R}$,i.e. $h - h'$ is bounded. in other words, there exists $a > 0$ such that $|h(x) - h'(x)| \leq a$ for all $x \in X$.*

Definition 6.4.3. *Let A be an abellian group, a function $u : A \longrightarrow \mathbb{R}$ is quasilinear given $u(x + y)$ and $u(x) + u(y)$ are equivalent function $A \times A \longrightarrow \mathbb{R}$.*

Definition 6.4.4. *A function $\beta : A \times A \longrightarrow \mathbb{R}$ is quasibilinear given the pair of function $\beta(x + x', y)$,$\beta(x, y) + \beta(x', y)$, $\beta(x, y + y')$, and $\beta(x, y) + \beta(x, y')$ are equivalent function $A \times A \times A \longrightarrow \mathbb{R}$.*

Definition 6.4.5. *A function $q : A \longrightarrow \mathbb{R}$ is quasiquadratic given $\Delta q(x, y)$ is equivalent and $q(x) = q(-x)$. Moreover, q is positive $q(x) \geq 0$ for all $x \in A$. Again $\Delta q(x, y) = q(x + y) - q(x) - q(y)$.*

Proposition 6.4.6. *A function $q : A \longrightarrow \mathbb{R}$ is quadratic iff $q(x) = q(-x)$, $q(2x) = 4q(x)$, and q is quasiquadratic.*

Theorem 6.4.7. *If a function $q : A \longrightarrow \mathbb{R}$ is a quadratic function satisfying $q(x) = q(-x)$ then $q^*(x) = lim_{n\to\infty} 2^{-2n} q(2^n x)$ exists and the function $q^*(x)$ is quadratic.*

Proof. Since we know that q is quasiquadratic iff the weak parallelogram law holds, $q(x+y)+q(x-y) \sim 2q(x)+2q(y)$. Now we set $x = y$ then we have $q(2x) \sim 4q(x)$, i.e. $|q(2x) - 4q(x)| \leq A$ for A should be positive constant. And replacing x by $2^n x$, we get the expression

$$|2^{-2(n+1)} q(2^{n+1}x) - 2^{-2n} q(2^n x)| = 2^{-2n} A$$

For this we have following estimate for all n and p

$$|2^{-2(n+p)} q(2^{n+p}x) - 2^{-2n} q(2^n x)| = 2^{-2n}.\frac{4A}{3}.$$

so from this the sequence $q^*(x)$ is cauchy, implies it is convergent. and by the previous proposition the condition $q^*(x) = 4q^*(x)$ comes from the defining the limit and the condition that $q^*(x) = q^*(-x)$ and $q^*(x)$ is quasiquadratic are preserved in the limit. □

6.5 The General Notion of Height on Projective Space

A height on projective space is a proper, positive real valued function.

Definition 6.5.1. *Let k be a field, A k-morphism $f : \mathbb{P}_m(k) \longrightarrow \mathbb{P}_m(k)$ of degree d is a function is of the form*

$$f(y_0 : ... : y_m) = f_o(y_0 : ... : y_m) : ... : f_m(y_0 : ... : y_m),$$

Where each $f_i(y_0 : ... : y_m) \in k[y_o, y_1, ..., y_m]$ is homogeneous of degree d and not all are equals to zero at any $y_o : ... : y_m \in \mathbb{P}_m(\bar{k})$.

Definition 6.5.2. *A height h on $\mathbb{P}_m(k)$ is a proper function $h : \mathbb{P}_m(k) \longrightarrow \mathbb{R}$ such that for any k-morphism $f : \mathbb{P}_m(k) \longrightarrow \mathbb{P}_m(k)$ of degree d the composition hof is equivalent to $d.h$, i.e., there exists a constant c with*

$$|h(f(y)) - d.h(y)| \leq c$$

for all $y \in \mathbb{P}_m(k)$.

Notation-

For a point in $\mathbb{P}_m(\mathbb{Q})$ we choose a $\mathbb{Z}$-reduced representatives $y_o : ... : y_m$

$$H(y_o : ... : y_m) = max|y_o|, ..., |y_m|$$

and

$$h(P) = logH(P)$$

Where $P = y_o : ... : y_m$.This $h(P)$ is called the canonical height on $\mathbb{P}_m(\mathbb{Q})$.
In one dimensional case there is a bijection

$$u : \mathbb{Q} \cup +\infty \to \mathbb{P}_1(\mathbb{Q})$$

defined by $u(m/n) = n : m$ and $u(\infty) = 0 : 1$ and the composition

$$hu : \mathbb{Q} \cup +\infty \to \mathbb{R}$$

$$hu/\mathbb{Q} : \mathbb{Q} \to \mathbb{R}$$

Means the composition restricted to $\mathbb{Q}$ is given by $h(m/n) = logmax|m|, |n|$, where m/n is reduced to the lowest term.

$\mathbb{Z}$- Reduced-

if we take the set $(a_1/b_1, ...a_n/b_n)$ take the product of the denominator $b_1...b_n$ and

$$(a_1b_2...b_n, ..., a_nb_1...b_{n-1}) = 1$$

so the lcm of denominator is l i.e. $(a_1l_1, ..., a_nl_n)$ Then $gcd(a_1l_1, a_2l_2, ..., a_nl_n) = 1$.

Lemma 6.5.3. *Let ϕ be a form of degree d in $y_o, ..., y_m$. Then there exists a positive constant $c(\phi)$ such for $\mathbb{Z}$-Reduced $y \in \mathbb{P}_m(\mathbb{Q})$ we have $|\phi(y)| \leq c(\phi)H(y)^d$.*

Proof. Decompose $\phi(y) = \sum a_\alpha m_\alpha(y)$, where the index α counts of the monomials $m_\alpha(y)$ of degree d. Then we have

$$|\phi(y)| \leq \sum |a_\alpha||m_\alpha(y)|$$

$$|\phi(y)| \leq \sum(|a_\alpha|).(max|y_o|, ..., |y_m|)^d = c(\phi)H(y)^d,$$

Where $c(\phi) = \sum |a_\alpha|$,as upper estimate. □

Remark 6.5.4. *A sequence of forms $(f_o, f_1, ..., f_m)$ of degree d in $\mathbb{Z}[y_o, y_1, ..., y_m]$ defines a $\mathbb{Q}$-morphism.*
Means that $f_o, f_1, ..., f_m$ have no common zero in $\mathbb{P}_m(\bar{\mathbb{Q}}) \Leftrightarrow$ there exists $s \in \mathbb{Z}^+$, $b \in \mathbb{Z}$ and the polynomial $g_{ij}(y) \in \mathbb{Z}[y_o, y_1, ..., y_m]$ such that

$$\sum g_{ij}f_j = by_i^{s+d}$$

for all $i = 0, ..., m$.

Theorem 6.5.5. *If h is the canonical height on $\mathbb{P}_m\mathbb{Q}$ and $f : \mathbb{P}_m(\mathbb{Q}) \to \mathbb{P}_m(\mathbb{Q})$ is a $\mathbb{Q}$-morphism of degree d is $h(f(y)) - d.h(y)$ is bounded on $\mathbb{P}_m(\mathbb{Q}$.*

Proof. Now in this proof we use the previous lemma, and we have an upper estimate for $H(f(y)$, where $H(f(y)) = \max_i |f_i(y)| \leq \max_i cf_i(y)H(y)^d = c_2H(y)^d$. And by the previous remark, we also have a lower estimate on $H(f(y))$.
We have, $|b|.|y_i|^{s+d} = (\max_{i,j} c(g_{ij})).H(y)^s.\sum_j |f_j(y)| \leq (\max_{i,j}(c(g_{i,j})))(m+1)H(y)^s(\max_j |f_j(y)|)$.
Since common factor among $f_j(y) \mid b$. Also, by the previous remark, $\max_j |f_j(y)| \leq |b|H(f(y))$. Taking maximum over i, we get, $|b|H(y)^{s+d} \leq (\max_{i,j} c(g_{i,j}))(m+1)H(y)^s|b|H(f(y))$. This implies $c_1H(y)^d \leq H(f(y))$, for some $c_1 > 0$. Thus, $c_1H(y)^d \leq H(f(y)) \leq c_2H(y)^d$. Taking logarithm on both sides, we get $log(\frac{H(f(y))}{H(y)^d}) = h(f(y)) - d.h(y)$ is bounded on $\mathbb{P}_m(\mathbb{Q})$. Which completes the proof. □

6.6 The Canonical Height and Norm on an Elliptic curve

Lemma 6.6.1. *Let E be an elliptic curve over k defined by $y^2 = f(x)$ where $f(x)$ is a cubic polynomial. and define the function $q : E(k) \longrightarrow \mathbb{P}_1(k)$ defined by $q(x, y) = (1, x)$ and $q(0) = (0, 1)$. Then there is a k- morphism $g : \mathbb{P}_1(k) \longrightarrow \mathbb{P}_1(k)$ of degree 4 such that the diagram is commutative.*

$$\begin{array}{ccc} E(k) & \xrightarrow{2} & E(k) \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q} \\ \mathbb{P}_1(k) & \xrightarrow{g} & \mathbb{P}_1(k) \end{array}$$

Proof. First of all we take the point $(x, y) \in E(k)$. And suppose $2(x, y) = (x', y')$. So our aim to find the relation between (x, y) and $2(x, y)$. Now consider the tangent line $y = \lambda x + \beta$ to the elliptic curve E at (x, y). And we know that, $2P = P + P = -PP$. This line passing through the point $(x', -y')$. Since $y^2 = f(x)$ where $f(x)$ is a cubic polynomial, and we get, $y' = \dfrac{f'(x)}{2y} = \lambda$, which is the slope of tangent line. put $y = \lambda x + \beta$ in the equation of elliptic curve, we get the cubic equation in x i.e. $x^3 + x^2(a - \lambda^2) + x(b - 2\beta\lambda) + c - \beta^2 = 0$. Sum of roots of this polynomial $= \lambda^2 - a$. We get, $2x + x' = \lambda^2 - a = (\dfrac{3x^2 + 2ax + b}{4(x^3 + ax^2 + bx + c)})^2 - a$. Thus, $x' = \dfrac{x^4 - 2bx^2 - 8cx + (b^2 - 4ac)}{4x^3 + 4ax^2 + 4bx + 4c}$. Therefore, $g(w, x) = (g_0(w, x), g_1(w, x))$, where $g_0(w, x) = 4wx^3 + 4aw^2x^2 + 4bw^3x + 4cw^4$ and $g_1(w, x) = x^4 - 2bw^2x^2 - 8cxw^3 + (b^2 - 4ac)w^4$. Hence, the above diagram commutes.

□

Theorem 6.6.2. *Let E be an elliptic curve over a number field k in Weierstrass form $y^2 = f(x) = x^3 + bx + c$. Then there is a unique function $h_E : E(k) \longrightarrow \mathbb{R}$ such that*
(1) *$h_E(P) - (1/2)h(x(P))$ is bounded, where $x(P) = q(P)$ is the x-coordinate of P and h is the canonical height on $\mathbb{P}_1(k)$, and*
(2) *$h_E(2P) = 4h_E(P)$ and $h_E(P) = h_E(-P)$.*
furthermore, h_E is proper, positive and quadratic.

Corollary 6.6.3. *With the assumption and the notations of the above theorem, the function $|P| = \sqrt{h_E(P)}$ is a norm on $E(k)$ i.e, P satisfies all the properties of the norm-function.*

Theorem 6.6.4 (Mordell-Weil)**.** *Let E be an elliptic curve over the number field k. Then the group $E(k)$ is finitely generated.*

Proof. The proof can be seen in two separate cases. First we consider the case when E is an elliptic curve $\mathbb{Q}$. When $E = E[a, b]$, the index $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ is finite, which we proved in theorem 6.2.2. Using the corollary 6.6.3, we know about the the norm on the elliptic curve, $|P| = \sqrt{h_E(P)}$. Now we use the proposition 6.1.2, $E(\mathbb{Q})$ is a finitely generated abelian group.

Secondly, when E is any elliptic curve over any field k. Then we complete the proof as like. For if any general elliptic curve, we can extend the field k to be the field k' such that the elliptic curve breaks in the form of $y^2 = (x - a)(x - b)(x - c)$. Again,also we know the index $(E(k') : 2E(k'))$ is finite. The norm function in this case is $|P| = \sqrt{h_E(p)}$ is a norm on $E(k')$. It follows from the proposition 6.1.2 that $E(k')$ is a finitely generated abelian group. Since, $E(k)$ is a subgroup of a finitely generated abelian group $E(k')$, it is also finitely generated. This proves the theorem. □

Bibliography

[1] Husemöller, Dale. Elliptic curves. Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics, 111. Springer-Verlag, New York, 2004.

[2] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[3] Szendrői, Balázs. Cubic curves: a short survey, University of Utrecht, 2005.

[4] Belmont, Eva. Lecture notes on Elliptic Curves taught by T.A. Fisher.